Hey, Google, Turn on Wiretap: Search and Seizure in White Collar Cases

October 21, 2020

6:30 – 8 pm

Table of Contents

Hey, Google, Turn on Wiretap: Search and Seizure in White Collar Cases

October 21, 2020

6:30 – 8 pm

Timed Agenda

I. Introduction to Program and Disclaimer — 1 minute

II. Scene One (*Golden Boy's Visit to Mom's House*) — 3 minutes
- Introduction to defendant and beginning of evidentiary fact pattern

III. Scene Two (*Zoom Meeting between Golden Boy and Executive*) — 4 minutes
- Continuation of evidentiary fact pattern
- Introduction to encryption

IV. Scene Three (*DOJ Strategy Meeting*) — 14 minutes
- Discussion of elements required for an insider trading prosecution and the STOCK Act
- Background on former NY District Attorney, Thomas E. Dewey
- Introduction to prosecutorial investigative techniques including wiretapping, search warrants and subpoenas

V. Scene Four (*Golden Boy's Call with Broker*) — 4 minutes
- Continuation of evidentiary fact pattern

VI. Scene Five (*FBI Raid: Seizure of Golden Boy's Laptop and Phone*) — 4 minutes
- Continuation of evidentiary fact pattern

VII. Scene Six (*Defense Meeting: Golden Boy Meets w/ Counsel to Discuss Motion to Compel Production of Passcode*) — 3 minutes
- Introduction of the Fifth Amendment defense to compelled production of a passcode

VIII. Scene Seven (*Court Hearing on DOJ Motion to Compel Golden Boy's Production of Passcode*) — 11 minutes
- Discussion of caselaw regarding the applicability of the Fifth Amendment and the foregone conclusion exception to compelled production of a passcode

IX. Scene Eight (*Defense Meeting: Golden Boy Meets w/ Counsel to Discuss Motion to Suppress Evidence Seized from Smartphone, Laptop and Email Accounts)* — 5 minutes
- Discussion of strategy in drafting motion to suppress evidence seized from an individual's smartphone, laptop, and email accounts

X. Scene Nine (*Court Hearing on Golden Boy's Motion to Suppress Evidence Seized from Smartphone, Laptop and Email Accounts*) 13 minutes

- Discussion of caselaw regarding the applicability of the Fourth Amendment to a motion to suppress evidence seized from a smartphone, laptop and email accounts, including issues of particularity and overbreadth

XI. Panel Discussion and Audience Participation 28 minutes

- Review and discussion of important issues and caselaw raised in scenes 1-9

Commonwealth v. Gelfgatt

Supreme Judicial Court of Massachusetts

November 5, 2013, Argued; June 25, 2014, Decided

SJC-11358

Reporter
468 Mass. 512 *; 11 N.E.3d 605 **; 2014 Mass. LEXIS 416 ***; 2014 WL 2853731

COMMONWEALTH *vs.* **LEON I. GELFGATT**.

Prior History: [*1]** Suffolk. INDICTMENTS found and returned in the Superior Court Department on May 7, 2010.

A pretrial motion to compel evidence was heard by *Raymond J. Brassard*, J., and a question of law was reported by him.

The Supreme Judicial Court on its own initiative transferred the case from the Appeals Court.

Core Terms

decryption, encryption, foregone, seized, authenticity, self-incrimination, mortgage, incriminating, unencrypted, protocol, conveyed, drive, subpoena, digital, facsimile, interview, ownership, laptop, installed, exemplar, password, trigger

Case Summary

Overview

HOLDINGS: [1]-With respect to charges of forgery and related offenses, arising from defendant's alleged use of computers to improperly divert funds to himself, defendant was properly compelled pursuant to *Mass.R.Crim.P. 14(a)(2)* to decrypt the digital storage devices that were seized from him because such act was not a testimonial communication that triggered protection under the Fifth Amendment, *U.S. Const. amend. V*, or under *Mass. Const. Decl. Rights art. 12*, as the factual statements that would be conveyed were "foregone conclusions."

Outcome
Judgment reversed; matter remanded for further proceedings.

LexisNexis® Headnotes

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > Discovery

Evidence > Burdens of Proof > Allocation

Criminal Law & Procedure > Preliminary Proceedings > Discovery & Inspection > General Overview

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > General Overview

HN1[] **Abuse of Discretion, Discovery**

Generally speaking, discovery matters are committed to the sound discretion of the trial judge. An appellate court will uphold discovery rulings unless the appellant can demonstrate an abuse of discretion that resulted in prejudicial error. However, the appellate court reviews a

judge's rulings on mixed questions of fact and law de novo.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN2 **Procedural Due Process, Self-Incrimination Privilege**

See U.S. Const. amend. V.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

HN3 **Procedural Due Process, Self-Incrimination Privilege**

It is extortion of information from the accused himself that offends the sense of justice. It is well established that the Fifth Amendment, U.S. Const. amend. V, does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating. The privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN4 **Procedural Due Process, Self-Incrimination Privilege**

The United States Supreme Court held that the Fifth Amendment, U.S. Const. amend. V, privilege against self-incrimination applies to the States through the Fourteenth Amendment to the United States Constitution, U.S. Const. amend. XIV.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN5 **Procedural Due Process, Self-Incrimination Privilege**

Although the privilege under the Fifth Amendment, U.S. Const. amend. V, typically applies to oral or written statements that are deemed to be testimonial, the act of producing evidence demanded by the government may have "communicative aspects" that would render the Fifth Amendment applicable. The Fifth Amendment privilege against self-incrimination applies not only to verbal communications, but also to nonverbal acts that imply assertions. Whether an act of production is testimonial depends on whether the government compels the individual to disclose "the contents of his own mind" to explicitly or implicitly communicate some statement of fact.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN6 **Procedural Due Process, Self-Incrimination Privilege**

The act of complying with the government's demand for production could constitute a testimonial communication where it is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence. The determination whether an act of producing evidence in response to a governmental demand is sufficiently testimonial that it

renders the Fifth Amendment, U.S. Const. amend. V, applicable depends on the facts and circumstances of each particular case.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN7 **Procedural Due Process, Self-Incrimination Privilege**

It is well established that not all acts of production have communicative aspects such that they will be deemed testimonial. Significantly, the privilege of the Fifth Amendment, U.S. Const. amend. V, is not triggered where the government seeks to compel an individual to be the source of real or physical evidence by, for example, furnishing a blood sample, producing a voice exemplar, standing in a lineup, providing a handwriting exemplar, or putting on particular clothing. The Fifth Amendment privilege is not implicated in these circumstances because the individual is not required to disclose any knowledge he might have, or to speak his guilt.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN8 **Procedural Due Process, Self-Incrimination Privilege**

It is a settled proposition that a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not "compelled" within the meaning of the privilege under the Fifth Amendment, U.S. Const. amend. V.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Evidence > Burdens of Proof > Allocation

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN9 **Procedural Due Process, Self-Incrimination Privilege**

The "foregone conclusion" exception to the privilege against self-incrimination under the Fifth Amendment, U.S. Const. amend. V, provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, such that the individual adds little or nothing to the sum total of the Government's information. For the exception to apply, the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence. In those instances when the government produces evidence to satisfy the “foregone conclusion” exception, no constitutional rights are touched. The question is not of testimony but of surrender. In essence, under the "foregone conclusion" exception to the Fifth Amendment privilege, the act of production does not compel a defendant to be a witness against himself.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN10 **Procedural Due Process, Self-Incrimination Privilege**

See Mass. Const. Decl. Rights art. 12.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN11[] **Procedural Due Process, Self-Incrimination Privilege**

It is well established that *Mass. Const. Decl. Rights art. 12* affords greater protection against self-incrimination than does the Fifth Amendment, *U.S. Const. amend. V*, in circumstances that are "discrete and well defined." However, although *Mass. Const. Decl. Rights art. 12* demands a more expansive protection, it does not change the classification of evidence to which the privilege applies. Only that genre of evidence having a testimonial or communicative nature is protected under the privilege against self-incrimination. Like the federal Constitution, the protection against self-incrimination afforded by *Mass. Const. Decl. Rights art. 12* is unavailable where the government seeks to compel an individual to be the source of real or physical evidence.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

Criminal Law & Procedure > ... > Discovery & Inspection > Discovery by Government > Physical Evidence

HN12[] **Procedural Due Process, Self-Incrimination Privilege**

The Supreme Judicial Court of Massachusetts has held that, as is the case under the federal Constitution, the act of production, quite apart from the content of that which is produced, may itself be communicative. Where the information conveyed by an act of production is reflective of the knowledge, understanding, and thoughts of the witness, it is deemed to be testimonial and, therefore, within the purview of *Mass. Const. Decl. Rights art. 12*. At the same time, when it is a "foregone conclusion" that a witness has certain items, and the items themselves are not privileged, the witness has no privilege.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

Criminal Law & Procedure > ... > Defendant's Rights > Right to Remain Silent > Communicative & Testimonial Information

HN13[] **Procedural Due Process, Self-Incrimination Privilege**

Upon considering the scope of the protection against self-incrimination afforded by both the Federal Constitution and the Massachusetts Declaration of Rights, a court's analysis under *Mass. Const. Decl. Rights art. 12* need not merely duplicate the Fifth Amendment, *U.S. Const. amend. V*, analysis. Rather, a court is free to consider certain evidence, considered by the Supreme Court to be insufficiently testimonial for Fifth Amendment purposes, to be sufficiently testimonial for *Mass. Const. Decl. Rights art. 12* purposes.

Headnotes/Summary

Headnotes

Forgery > *Uttering Forged Instrument* > *Larceny* > *False Pretenses* > *Witness* > Compelling giving of evidence > Self-incrimination > *Evidence* > Information stored on computer > Testimonial statement > *Search and Seizure* > Computer > *Constitutional Law* > Self-incrimination

Counsel: *Randall E. Ravitz,* Assistant Attorney General

(*Thomas D. Ralph*, Assistant Attorney General, with him) for the Commonwealth.

Paul Joseph Davenport (*Stanley D. Helinski* with him) for the defendant.

The following submitted briefs for amici curiae:

Daniel B. Garrie, of Washington, & *Daniel K. Gelb*, for Daniel K. Gelb & others.

David H. Margolis, of Florida, for Florida Department of Law Enforcement & others.

Mark R. Gage & *Christian J. Desilets*, of West Virginia, for National White Collar Crime Center.

David W. Opderbeck, of New Jersey, for David W. Opderbeck & others.

Nathan F. Wessler, of New York, *Hanni M. Fakhoury*, of California, & *Matthew R. Segal*, *Jessie J. Rossman*, & *Kit Walsh*, for American Civil Liberties Union Foundation of Massachusetts & others.

Victoria L. Nadel, for Massachusetts Association of Criminal Defense Lawyers.

Judges: Present: Ireland, C.J., Spina, Cordy, Botsford, Gants, Duffly, & Lenk, **[***2]** JJ. Lenk, J (dissenting, with whom Duffly, J., joins).

Opinion by: SPINA

Opinion

[*513] [608]** SPINA, J. On May 5, 2010, a State grand jury returned indictments charging the defendant with seventeen counts of forgery of a document, G. L. c. 267, § 1; seventeen counts of uttering a forged instrument, G. L. c. 267, § 5; and three counts of attempting to commit the crime of larceny by false pretenses of the property of another, G. L. c. 274, § 6. The charges arose from allegations that the defendant, through his use of computers, conducted a sophisticated scheme of diverting to himself funds that were intended to be used to pay off large mortgage loans on residential properties. On November 21, 2011, the Commonwealth filed in the Superior Court a "Motion to Compel the Defendant to Enter His Password into Encryption Software He Placed on Various Digital Media Storage Devices that Are Now in the Custody of the Commonwealth" (motion to compel decryption). The Commonwealth also filed a motion to report a question of law to the Appeals Court prior to trial pursuant to Mass. R. Crim. P. 34, as amended, 442 Mass. 1501 (2004). The question concerned the lawfulness of compelling the defendant to privately enter an encryption key **[***3]** into computers seized from **[*514]** him by the Commonwealth.[1] Following a hearing on January 18, 2012, a judge denied the Commonwealth's motion to compel decryption, but he reported the following question of law:

> "Can the defendant be compelled pursuant to the Commonwealth's proposed protocol to provide his key to seized encrypted digital evidence despite the rights and protections provided by the Fifth Amendment to the United States Constitution and Article Twelve of the Massachusetts Declaration of Rights?"[2]

We transferred the case to this court on our own

[1] The parties treat as synonymous the terms "encryption key" and "password" to encryption software. For the sake of simplicity, we shall do the same.

[2] The parties have not included in the record appendix a copy of the order reporting the question of law from the Superior Court. We rely on a joint **[***4]** stipulation of the parties filed on July 19, 2012, that sets forth the language of the reported question.

motion.[3] We now conclude that the answer to the reported question is, "Yes, where the defendant's compelled decryption would not communicate facts of a testimonial nature to the Commonwealth beyond what the defendant already had admitted to investigators." Accordingly, we reverse the judge's denial of the Commonwealth's motion to compel decryption.[4]

[609]** 1. *Background*. The undisputed facts are taken from the parties' submissions to the **[***5]** motion judge.[5]

Beginning in 2009, the defendant, who is an attorney, allegedly **[*515]** orchestrated a scheme to acquire for himself funds that were intended to be used to pay off home mortgage loans. According to the Commonwealth, the defendant identified high-end properties that were listed in an online database as "under agreement." He would research each one at the applicable registry **[***6]** of deeds to determine whether there was a mortgage on the property. If there was, the defendant, purportedly using a computer, would forge an assignment of the mortgage to either "Puren Ventures, Inc." (Puren Ventures) or "Baylor Holdings, Ltd." (Baylor Holdings). He then would record the forged assignment at the applicable registry of deeds and mail a notice to the seller stating that the mortgage on the property had been assigned to one of these sham companies, which he had set up.

The defendant fostered the illusion that Puren Ventures and Baylor Holdings were actual companies by giving each one Internet-based telephone and facsimile numbers. When a closing attorney would contact one of these companies to request a statement documenting the sum necessary to pay off the reassigned mortgage, the attorney would be instructed to send the request to the facsimile number that the defendant had created. Next, the defendant would request an actual payoff figure from the true mortgage holder. The defendant would transmit this information by Internet facsimile number to the closing attorney, doing so under the guise of the sham company. The defendant would instruct the closing attorney to **[***7]** send the payoff check to a Boston address where the defendant once had practiced law. Although ultimately unsuccessful, the defendant purportedly created seventeen fraudulent assignments of mortgages, totaling over $13 million. According to the Commonwealth, the defendant relied heavily on the use of computers to conceal his identity and perpetrate his alleged scheme.

On December 17, 2009, State police troopers arrested the **[*516]** defendant immediately after he retrieved what he believed to be over $1.3 million in payoff funds from two real estate closings. They also executed search warrants for his residence in Marblehead and for his vehicle. During the search of the defendant's residence, **[**610]** troopers observed several computers that were powered on, and they photographed the computer screens.[6] The troopers seized from the defendant's residence two desktop computers, one laptop computer, and various other devices capable of storing electronic data.[7] They also

---

[3] All proceedings in the Superior Court have been stayed pending resolution of the reported question.

[4] We acknowledge the amicus briefs submitted in support of the defendant by the American Civil Liberties Union Foundation of Massachusetts, the American Civil Liberties Union Foundation, and the Electronic Frontier Foundation; by the Massachusetts Association of Criminal Defense Lawyers; and by Daniel K. Gelb, Daniel B. Garrie, and the National Association of Criminal Defense Lawyers. We also acknowledge the amicus briefs submitted in support of the Commonwealth by David W. Opderbeck, the Massachusetts Chiefs of Police Association, Inc., and NW3C, Inc., doing business as the National White Collar Crime Center; by the Florida Department of Law Enforcement, the Massachusetts Chiefs of Police Association, Inc., NW3C, Inc., doing business as the National White Collar Crime Center, and the National District Attorneys Association; and by NW3C, Inc., doing business as the National White Collar Crime Center.

[5] These submissions included an affidavit dated August 31, 2011, from David Papargiris, the director of the Attorney General's computer forensics laboratory; an affidavit dated October 19, 2011, from State police Trooper Patrick M. Johnson; and the transcript of an audio recording of a postarrest interview of the defendant conducted on December 17, 2009, by law enforcement officers. The motion judge declined to make findings of fact when ruling on the Commonwealth's motion to compel decryption, given that the only facts before him were those presented in the Commonwealth's submissions. Defense counsel did not dispute the facts set forth in the affidavits and transcript, recognizing that they spoke for themselves. He did, however, point out that he might disagree with some of the characterizations of those facts.

[6] Appearing on the computer screens were the following phrases that were visible as headings or icons: "K:\LeonDocuments\My Scans"; "Erasing Report"; "Erased area"; "Attorney Leon I. Gelfgatt"; "TrueCrypt"; and "DriveCrypt Plus Pack."

[7] Apart from the computers, troopers seized an Adaptec external hard drive, two universal serial bus (USB) thumb drives, two secure digital cards, two cellular telephones, and

seized one smaller "netbook" computer from the defendant's vehicle. Computer forensic examiners were able to view several documents and "bookmarks" to Web sites that were located on an external hard drive.[8] However, all of the data on the **[***8]** four computers were encrypted with "DriveCrypt Plus" software.[9]

According to the Commonwealth, the encryption software on **[*517]** the computers is virtually impossible to circumvent. Its manufacturer touts the fact that it does not contain a "back door" that would allow access to data by anyone other than the authorized user. Thus, the Commonwealth states, the files on the four computers cannot be accessed and viewed unless the **[***10]** authorized user first enters the correct password to unlock the encryption. The Commonwealth believes that evidence of the defendant's purported criminal activities is located on these computers.

On the day of his arrest, the defendant was interviewed by law enforcement officials after having been advised of the Miranda rights. In response to questioning, he said that he had more than one computer in his home. The defendant also informed the officials that "[e]verything is encrypted and no one is going to get to it." In order to decrypt the information, he would have to "start the program." The defendant said that he used encryption for privacy purposes, and that when law enforcement officials asked him about the type of encryption used, they essentially were asking for the defendant's help in putting him in jail. The defendant reiterated that he was able to decrypt the computers, but he refused to divulge any **[**611]** further information that would enable a forensic search.

On November 21, 2011, the Commonwealth filed its motion to compel decryption pursuant to *Mass. R. Crim. P. 14 (a) (2)*, as appearing in 442 Mass. 1518 (2004). It sought an order compelling the defendant's compliance with a **[***11]** "protocol" that the Commonwealth had established to obtain decrypted digital data.[10] As

---

fourteen compact discs.

[8] These documents included what appeared to be unsigned releases for a mortgage encumbering the defendant's residential property in Marblehead. Computer forensic examiners also were able to see an image file that appeared to contain the seal for an Arizona notary public. The "bookmarks" included a Web site where Puren Ventures was advertised for sale, and a Web site offering anonymous wire transfers.

[9] In an affidavit submitted in connection with the Commonwealth's motion to compel decryption, the director of the Attorney General's computer forensics laboratory explained the differences between encryption and decryption:

> "Encryption is the process by which 'readable' digital media, that is, digital media **[***9]** or data that can be viewed and accessed, is scrambled in such a way as to render that digital media or data 'unreadable' without decryption. Encryption can be performed both by hardware and by means of software tools.
>
> "Decryption is the process by which encrypted, scrambled data is rendered 'readable' again. In order to decrypt data, the person seeking decryption performs some action such as the entering of a password, scanning of a fingerprint or [insertion of] a USB Thumb drive with a pass code key on it. The encryption software then translates this action into a 'key,' essentially a string of numbers or characters. The encryption software then applies this key to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again."

[10] The Commonwealth's "protocol" is as follows:

> "1. The defendant, in the presence of his counsel, shall appear at the Computer Forensics Laboratory of Massachusetts Attorney General Martha Coakley within 7 days from the receipt of this Order at a time mutually agreed upon by the Commonwealth and defense counsel;
>
> "2. The Commonwealth shall provide the defendant with access to all encrypted digital storage devices that were seized from him pursuant to various search warrants issued in connection with this case;
>
> "3. The defendant shall manually enter the password or key to **[***12]** each respective digital storage device in sequence, and shall then immediately move on to the next digital storage device without entering further data or waiting for the completion of the process required for the respective devices to 'boot up';
>
> "4. The defendant shall make no effort to destroy, change, or alter any data contained on the digital storage devices;
>
> "5. The defendant is expressly ordered *not* to enter a false or 'fake' password or key, thereby causing the encryption program to generate 'fake, prepared information' as advertised by the manufacturer of the encryption program;
>
> "6. The Commonwealth shall not view or record the password or key in any way; [and]
>
> "7. The Commonwealth shall be precluded from introducing any evidence relating to this Order or the manner in which the digital media in this case was

grounds for the motion, the Commonwealth stated that compelling the defendant to enter the key to encryption **[*518]** software on various digital media storage devices that had been seized by the Commonwealth was essential to the discovery of "material" or "significant" evidence relating to the defendant's purported criminal conduct. The Commonwealth further stated that its protocol would not violate the defendant's rights under either the Fifth Amendment to the United States Constitution or art. 12 of the Massachusetts Declaration of Rights.

In denying the Commonwealth's motion to compel decryption, the judge said that, on the one hand, the Commonwealth merely was requesting a sequence of numbers and characters that would enable it to access information on the computers, but that, on the other hand, the Commonwealth was asking for the defendant's help in accessing potentially incriminating evidence that the Commonwealth had seized. In the judge's view, there was merit to the defendant's contention that production of a password to decrypt the computers constituted an admission of knowledge, ownership, and control. Further, the judge continued, the scenario presented in this case was far different from compelling **[*519]** a defendant to provide a voice exemplar, a handwriting exemplar, or a blood sample, all of which are deemed to be nontestimonial. The judge said that the defendant's refusal to disclose the encryption key during his interview with law enforcement officials could be construed as an invocation of his rights under the Fifth Amendment and art. 12. Finally, it was the judge's understanding that neither the Federal nor the State Constitution requires a defendant **[***14]** to **[**612]** assist the government in understanding evidence that it has seized from a defendant.

2. *Decryption under the Fifth Amendment*. The Commonwealth contends that compelling the defendant to enter his encryption key into the computers pursuant to the Commonwealth's protocol would not violate the defendant's Fifth Amendment right against self-incrimination. In the Commonwealth's view, the defendant's act of decryption would not communicate facts of a testimonial nature to the government beyond what the defendant already has admitted to investigators. As such, the Commonwealth continues, the defendant's act of decryption does not trigger Fifth Amendment protection. We agree.[11]

The **[***15]** Fifth Amendment provides that ***HN2***[↑] "[n]o person … shall be compelled in any criminal case to be a witness against himself."[12] See Couch v. United States, 409 U.S. 322, 328, 93 S. Ct. 611, 34 L. Ed. 2d 548 (1973) (***HN3***[↑] "It is extortion of information from the accused himself that offends our sense of justice"). It is well established that "the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a *testimonial* communication that is incriminating" (emphasis in original). **[*520]** Fisher v. United States, 425 U.S. 391, 408, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976). See United States v. Hubbell, 530 U.S. 27, 34, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000) ("The word 'witness' in the constitutional text limits the relevant category of compelled incriminating communications to those that are 'testimonial' in character"); Schmerber v. California, 384 U.S. 757, 761, 86 S. Ct. 1826, 16 L. Ed. 2d 908 (1966) ("[T]he privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature"). See also Commonwealth v. Hughes, 380 Mass. 583, 588, 404 N.E.2d 1239, cert. denied, *449 U.S. 900, 101 S. Ct. 269, 66 L. Ed. 2d 129*

---

decrypted in its case in chief. Further, the Commonwealth shall be precluded from introducing any such evidence whatsoever except to the extent necessary to cure any potentially misleading inferences created by the defendant at trial relating to this matter."

At the hearing on the motion to compel decryption, the Commonwealth stated that it "would be seeking to introduce the **[***13]** fact of encryption in order to suggest consciousness of guilt."

[11] ***HN1***[↑] Generally speaking, "discovery matters are committed to the sound discretion of the trial judge." Buster v. George W. Moore, Inc., 438 Mass. 635, 653, 783 N.E.2d 399 (2003). "We will uphold discovery rulings unless the appellant can demonstrate an abuse of discretion that resulted in prejudicial error." *Id.*, citing Solimene v. B. Grauel & Co., 399 Mass. 790, 799, 507 N.E.2d 662 (1987). However, we review a judge's rulings on mixed questions of fact and law de novo. See McCarthy v. Slade Assocs., 463 Mass. 181, 190, 972 N.E.2d 1037 (2012); Commissioner of Revenue v. Comcast Corp., 453 Mass. 293, 303, 901 N.E.2d 1185 (2009).

[12] In Malloy v. Hogan, 378 U.S. 1, 8, 84 S. Ct. 1489, 12 L. Ed. 2d 653 (1964), ***HN4***[↑] the United States **[***16]** Supreme Court held that the Fifth Amendment privilege against self-incrimination applies to the States through the Fourteenth Amendment to the United States Constitution. See Commonwealth v. Simon, 456 Mass. 280, 285 n.4, 923 N.E.2d 58, cert. denied, ***562 U.S. 874, 131 S. Ct. 181, 178 L. Ed. 2d 108 (2010)***.

(1980).

Here, the Commonwealth, through its motion, is seeking to compel the defendant to decrypt "all" of the "digital storage devices that were seized from him." Given that the Commonwealth believes that those devices contain information about the defendant's alleged mortgage payoff scheme, the entry of the encryption key or password presumably would be incriminating because "it would furnish the Government with a link in the chain of evidence leading to [the defendant's] indictment." *Doe v. United States, 487 U.S. 201, 207 n.5, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1988)*, and accompanying text. The issue on which this case turns is whether the defendant's act of decrypting the computers is a **[**613]** testimonial communication that triggers *Fifth Amendment* protection.

HN5[↑] Although the *Fifth Amendment* privilege typically applies to oral or written statements that are deemed to be testimonial, *United States v. White, 322 U.S. 694, 698, 64 S. Ct. 1248, 88 L. Ed. 1542 (1944)*, the act of producing evidence demanded by the **[***17]** government may have "communicative aspects" that would render the *Fifth Amendment* applicable. *Fisher, 425 U.S. at 410*. See *Hubbell, 530 U.S. at 36*. See also *Commonwealth v. Burgess, 426 Mass. 206, 211, 688 N.E.2d 439 (1997)* ("The *Fifth Amendment* privilege against self-incrimination applies not only to verbal communications, but … also to nonverbal acts that imply assertions"). Whether an act of production is testimonial depends on whether the government compels the individual to disclose "the contents of his own mind" to explicitly or implicitly communicate some statement of fact. *Hubbell, supra at 43*, quoting *Curcio v. United States, 354 U.S. 118, 128, 77 S. Ct. 1145, 1 L. Ed. 2d 1225 (1957)*. See *Doe v. United States, 487 U.S. at 213* (*Fifth Amendment* intended "to spare the accused from having to reveal, directly or indirectly, his knowledge of **[*521]** facts relating him to the offense or from having to share his thoughts and beliefs with the Government"). See also *Pennsylvania v. Muniz, 496 U.S. 582, 595 n.9, 110 S. Ct. 2638, 110 L. Ed. 2d 528 (1990)* (opinion of Brennan, J.) ("nonverbal conduct contains a testimonial component whenever the conduct reflects the actor's communication of his thoughts to another"). More particularly, ***HN6***[↑] the act of complying with the government's **[***18]** demand could constitute a testimonial communication where it is considered to be a tacit admission to the existence of the evidence demanded, the possession or control of such evidence by the individual, and the authenticity of the evidence. See *Hubbell, supra at 36 & n.19*; *United States v. Doe, 465 U.S. 605, 613-614, 104 S. Ct. 1237, 79 L. Ed. 2d 552 & n.11 (1984)*; *Fisher, supra.* See also *Commonwealth v. Burgess, supra*; *Commonwealth v. Hughes, 380 Mass. at 592*. The determination whether an act of producing evidence in response to a governmental demand is sufficiently testimonial that it renders the *Fifth Amendment* applicable "depend[s] on the facts and circumstances of [each] particular case[]." *Fisher, supra.* See *Doe v. United States, 487 U.S. at 214-215*.

HN7[↑] It is well established that not all acts of production have communicative aspects such that they will be deemed testimonial. See *Hubbell, 530 U.S. at 34-35*; *Doe v. United States, 487 U.S. at 210-211*. Significantly, the *Fifth Amendment* privilege is not triggered where the government seeks to compel an individual to be the source of real or physical evidence by, for example, furnishing a blood sample, *Schmerber v. California, 384 U.S. at 764-765*; producing a voice exemplar, **[***19]** *United States v. Dionisio, 410 U.S. 1, 5-7, 93 S. Ct. 764, 35 L. Ed. 2d 67 (1973)*; standing in a lineup, *United States v. Wade, 388 U.S. 218, 221-223, 87 S. Ct. 1926, 18 L. Ed. 2d 1149 (1967)*; providing a handwriting exemplar, *Gilbert v. California, 388 U.S. 263, 266-267, 87 S. Ct. 1951, 18 L. Ed. 2d 1178 (1967)*; or putting on particular clothing, *Holt v. United States, 218 U.S. 245, 252-253, 31 S. Ct. 2, 54 L. Ed. 1021 (1910)*. See *Commonwealth v. Brennan, 386 Mass. 772, 776-777, 438 N.E.2d 60 (1982)* (breathalyzer test and field sobriety tests do not produce evidence of testimonial nature). The *Fifth Amendment* privilege is not implicated in these circumstances because **[**614]** the individual is "not required 'to disclose any knowledge he might have,' or 'to speak his guilt.'" *Doe v. United States, supra at 211*, quoting *United States v. Wade, supra at 222-223*. See *Hubbell, supra at 35* ("The act of exhibiting such physical **[*522]** characteristics is not the same as a sworn communication by a witness that relates either express or implied assertions of fact or belief"); *Pennsylvania v. Muniz, 496 U.S. at 590-599* (discussing distinctions between production of "real or physical" evidence and production of "testimonial" communication for purposes of privilege against self-incrimination).

Here, the defendant's act of entering an encryption key in the **[***20]** computers seized by the Commonwealth would appear, at first blush, to be a testimonial communication that triggers *Fifth Amendment* protection. By such action, the defendant implicitly would be acknowledging that he has ownership and

control of the computers and their contents.[13] This is not simply the production of real or physical evidence like a blood sample or a handwriting exemplar. Rather, the defendant's act of entering the encryption key would be a communication of his knowledge about particular facts that would be relevant to the Commonwealth's case. Our analysis, however, does not end here. We must further determine whether the defendant's act of production loses its testimonial character because the information that would be disclosed by the defendant is a "foregone conclusion."

HN9[↑] The "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government, such that the individual "adds little or nothing to the sum total of the Government's information." Fisher, 425 U.S. at 411. For the exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of that evidence by the defendant; and (3) the authenticity of the evidence. See id. at 410-413; United States v. [*523] Bright, 596 F.3d 683, 692 (9th Cir. 2010). See also Hubbell, 530 U.S. at 40-41, 44-45 (government did not satisfy "foregone conclusion" exception where no showing of prior knowledge of existence or whereabouts of documents ultimately produced by respondent to subpoena); United States v. Doe, 465 U.S. at 613-614 & nn.11-13 **[***22]** (act of producing business records involved testimonial self-incrimination where government did not show that existence, possession, and authenticity of records were "foregone conclusion"). In those instances when the government produces evidence to satisfy the "foregone conclusion" exception, "no constitutional rights are touched. The question is not of testimony but of surrender." Fisher, supra at 411, quoting Matter [**615] of Harris, 221 U.S. 274, 279, 31 S. Ct. 557, 55 L. Ed. 732 (1911). See, e.g., United States v. Sideman & Bancroft, LLP, 704 F.3d 1197, 1202-1205 (9th Cir. 2013) (quantum of information possessed by Internal Revenue Service regarding existence and possession of summonsed documents, together with evidence of their authenticity, satisfied "foregone conclusion" exception to Fifth Amendment privilege against self-incrimination); United States v. Fricosu, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (Fifth Amendment not implicated by requiring production of unencrypted contents of computer where government knew of existence and location of files, although not specific content of documents, and knew of defendant's custody or control of computer); State v. Jancsek, 302 Or. 270, 287-288, 730 P.2d 14 (1986) (compelled **[***23]** production of letter not protected by Fifth Amendment privilege where existence, contents, and authenticity of letter already known to police). In essence, under the "foregone conclusion" exception to the Fifth Amendment privilege, the act of production does not compel a defendant to be a witness against himself.

Based on our review of the record, we conclude that the factual statements that would be conveyed by the defendant's act of entering an encryption key in the computers are "foregone conclusions" and, therefore, the act of decryption is not a testimonial communication that is protected by the Fifth Amendment. The investigation by the corruption, fraud, and computer crime division of the Attorney General's office uncovered detailed evidence that at least two mortgage assignments to Baylor Holdings were fraudulent. During his postarrest interview with State **[*524]** police Trooper Patrick M. Johnson, the defendant stated that he had performed real estate work for Baylor Holdings, which he understood to be a financial services company. He explained that his communications with this company, which purportedly was owned by Russian individuals, were highly encrypted because, according to the **[***24]** defendant, "[that] is how Russians do business." The defendant informed Trooper Johnson that he had more than one computer at his home, that the program for communicating with Baylor Holdings was installed on a laptop, and that "[e]verything is encrypted and no one is going to get to it." The defendant acknowledged that he was able to perform decryption. Further, and most significantly, the defendant said that because of encryption, the police were "not going to get to *any* of [his] computers," thereby implying that *all* of them were encrypted.

---

[13] Because the actual files and documents that are located on the defendant's computers were voluntarily created by the defendant in the course of his real estate dealings, they are not testimonial communications that enjoy Fifth Amendment protection. See United States v. Hubbell, 530 U.S. 27, 35-36, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000) (recognizing HN8[↑] "settled proposition that a person may be required to produce specific documents **[***21]** even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the [Fifth Amendment] privilege"); United States v. Doe, 465 U.S. 605, 611-612, 104 S. Ct. 1237, 79 L. Ed. 2d 552 (1984); Fisher v. United States, 425 U.S. 391, 409-410, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976).

When considering the entirety of the defendant's interview with Trooper Johnson, it is apparent that the defendant was engaged in real estate transactions involving Baylor Holdings, that he used his computers to allegedly communicate with its purported owners, that the information on all of his computers pertaining to these transactions was encrypted, and that he had the ability to decrypt the files and documents. The facts that would be conveyed by the defendant through his act of decryption — his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key — already are known **[***25]** to the government and, thus, are a "foregone conclusion."[14] The Commonwealth's **[**616]** motion to compel decryption does not violate the defendant's rights under the Fifth Amendment because the defendant is only telling the government what it already knows.

3. *Decryption under art. 12*. The Commonwealth also contends that compelling the defendant to enter his encryption key **[*525]** pursuant to the Commonwealth's protocol would not violate his privilege against self-incrimination under art. 12 of the Massachusetts Declaration of Rights. We agree.

Article 12 provides that ***HN10*** "[n]o subject shall … be compelled to accuse, **[***26]** or furnish evidence against himself." ***HN11*** It is well established that art. 12 affords greater protection against self-incrimination than does the Fifth Amendment in circumstances that are "discrete and well defined."[15] Commonwealth v. Burgess, 426 Mass. at 218. See Commonwealth v. Mavredakis, 430 Mass. 848, 858-859, 725 N.E.2d 169 (2000). However, as we have explained, "[a]lthough art. 12 demands a more expansive protection, 'it does not change the classification of evidence to which the privilege applies. Only that genre of evidence having a testimonial or communicative nature is protected under the privilege against self-incrimination.'" Commonwealth v. Burgess, supra, quoting Attorney Gen. v. Colleton, 387 Mass. 790, 796 n.6, 444 N.E.2d 915 (1982). Like the Federal Constitution, the protection against self-incrimination afforded by art. 12 is unavailable where the government seeks to compel an individual to be the source of real or physical evidence. See Commonwealth v. Burgess, supra, and cases cited.

Similarly, ***HN12*** we have held that, as is the case under the Federal Constitution, "the act of production, quite apart from the content of that which is produced, may itself be communicative." Commonwealth v. Doe, 405 Mass. 676, 679, 544 N.E.2d 860 (1989). See Commonwealth v. Hughes, 380 Mass. at 592. Where the information conveyed by an act of production "is reflective of the knowledge, understanding, and thoughts of **[***28]** the witness," it is deemed to be **[*526]** testimonial and, therefore, within the purview of art. 12. Commonwealth v. Doe, supra. At the same time, we also have recognized that "[w]hen it is a 'foregone conclusion' that a witness has certain items, and the items themselves are not privileged, the witness has no privilege." Id. at 680-681, citing Commonwealth v. Hughes, supra at 590, and Fisher v. United States, 425 U.S. at **[**617]** 411. See Commonwealth v. Diaz, 383 Mass. 73, 76 n.5, 417 N.E.2d 950 (1981) (no serious constitutional issue of self-incrimination raised by disclosure of information that is "foregone conclusion"). See also note 13, *supra*.

In Commonwealth v. Burgess, 426 Mass. at 219, when ***HN13*** the court considered the scope of the

[14] We note that compliance with an order for the production of specific documents pursuant to a subpoena may be deemed to be a testimonial communication of the fact that the documents produced are the ones demanded, thereby constituting authentication of those documents. See Fisher v. United States, 425 U.S. at 412-413 & n.12. Here, the defendant's decryption of his computers does not present an authentication issue analogous to that arising from a subpoena for specific documents because he is not selecting documents and producing them, but merely entering a password into encryption software.

[15] We have held, for example, that art. 12 of the Massachusetts Declaration of Rights does not allow a defendant's refusal to submit to a breathalyzer test to be admitted in evidence. Compare Opinion of the Justices, 412 Mass. 1201, 1209-1211, 591 N.E.2d 1073 (1992), **[***27]** with South Dakota v. Neville, 459 U.S. 553, 562-564, 103 S. Ct. 916, 74 L. Ed. 2d 748 (1983). We also have held that a custodian of corporate records may invoke his art. 12 right against self-incrimination in response to a subpoena for those records where the act of production itself would be personally incriminating. Compare Commonwealth v. Doe, 405 Mass. 676, 678, 544 N.E.2d 860 (1989), with Braswell v. United States, 487 U.S. 99, 108-110, 108 S. Ct. 2284, 101 L. Ed. 2d 98 (1988). Additionally, we have held that the type of immunity that provides the requisite degree of protection for art. 12 purposes is so-called transactional immunity, which affords broader protection that the "use and derivative use immunity" required by the Fifth Amendment. Compare Attorney Gen. v. Colleton, 387 Mass. 790, 795-801, 444 N.E.2d 915 & n.4 (1982), with Kastigar v. United States, 406 U.S. 441, 453, 92 S. Ct. 1653, 32 L. Ed. 2d 212 (1972).

protection against self-incrimination afforded by both the Federal Constitution and the Massachusetts Declaration of Rights, we pointed out that our analysis under art. 12 need not "merely duplicate our earlier Fifth Amendment analysis." Rather, "[w]e are free to consider certain evidence, considered by the Supreme Court to be insufficiently testimonial for Fifth Amendment purposes, to be sufficiently testimonial for art. 12 purposes." Id. Mindful of this pronouncement, as well as our **[***29]** jurisprudence recognizing the "foregone conclusion" principle, we are not persuaded that the circumstances presented here dictate an analytical departure from the Federal standard. Where the facts that would be conveyed by the defendant through the act of entering an encryption key into the computers seized by the Commonwealth are a "foregone conclusion," his act of production is insufficiently testimonial for art. 12 purposes.[16]

4. *Conclusion*. We answer the reported question, "Yes, where the defendant's compelled decryption would not communicate facts of a testimonial nature to the Commonwealth beyond what the defendant already had admitted to investigators." The judge's denial of the Commonwealth's motion to compel decryption is reversed, and this case is remanded to the Superior Court for further proceedings consistent with this opinion.

So ordered.

Dissent by: Lenk

Dissent

[*527] LENK, J (dissenting, with whom Duffly, J., joins). The court holds today **[***30]** that the defendant, an attorney who practices from his home, may be ordered to enter decryption keys sequentially on each and every electronic device seized from his home, his home office, and his automobile, in order to provide law enforcement officers with unencrypted access to those devices.[1] Such an order is the functional equivalent of requiring him to produce the unencrypted contents of the devices seized. The government suspects that some unspecified set of documents related to a mortgage fraud scheme may be located on one or more of these devices,[2] which the government **[**618]** thus far has been unable to read because of the encryption. I agree with the court that this act of decryption is compelled, testimonial, and potentially incriminating. Unlike the court, I conclude that this also holds true for the intrinsically linked act of thereby producing in unencrypted form any material that may be on the now encrypted devices. Further, I do not agree that the Commonwealth has shown sufficient **[*528]** knowledge of the existence, location, and authenticity of the documents it seeks such that the

[16] As properly enunciated by the Commonwealth in its protocol, see note 10, *supra*, the compelled act of computer decryption cannot be used to prove that the defendant had custody and control over the computers. Cf. Commonwealth v. Burgess, 426 Mass. 206, 220, 688 N.E.2d 439 (1997).

[1] The Commonwealth's proposed order requires the defendant to decrypt "all" of the "digital storage devices that were seized from him." These include two desktop computers and a laptop computer seized from his house; a "netbook" computer seized from his automobile; an external hard drive; two universal serial bus (USB) "thumb" drives (also known as "flash drives," "USB drives," and "sticks"); fourteen compact discs; two secure digital cards; and two cellular telephones. The devices were seized pursuant to a search warrant issued based on an affidavit by a State trooper involved in the investigation. The affidavit sought, inter alia, "[c]omputers and/or electronic storage devices capable of storing any of the below-described records and/or data"; it encompassed **[***32]** "[a]ny and all records, documents, items, and/or data, in whatever form, relating in any way to" a lengthy list of broadly defined items.

[2] A "netbook" is a smaller, more lightweight, and less powerful type of laptop computer usually used for Internet and electronic mail (e-mail) access. See Cloud Control: Copyright, Global Memes and Privacy, 10 J. Telecomm. & High Tech. L. 53, 58 & n.27 (2012) . Flash drives "are solid state memory devices that can comfortably be carried on a key chain. They can be used, usually thru a USB port, much like an external hard drive." United States v. Burgess, 576 F.3d 1078, 1090 n.12 (10th Cir.), cert. denied, *558 U.S. 1097, 130 S. Ct. 1028, 175 L. Ed. 2d 629 (2009)*. Like flash drives, secure digital cards are a type of "solid-state memory technology that stores information when not powered," but they "serve different functions and have limitations that USB flash drives do not"; secured digital cards "are thin cards used in phones or cameras that serve primarily as digital film substitutes." Sandisk Corp. v. Kingston Tech. Co., 863 F. Supp. 2d. 815, 819-820 (W.D. Wis. 2012). They are "not readily compatible with computers and often require a special adaptor to interface with a computer's USB **[***33]** port." Id. at 820.

information that would be revealed by decryption and production is a "foregone conclusion," and therefore **[***31]** that requiring the defendant to decrypt the devices would not violate his constitutional privilege against self-incrimination. Because I believe that the act of compelled entry of the codes to decrypt the seized devices, thereby producing the unencrypted contents of those devices, is protected under both the *Fifth Amendment to the United States Constitution* and *art. 12 of the Massachusetts Declaration of Rights*, I respectfully dissent.

1. *Act of production and authentication*. The court concludes that the act of decrypting the devices pursuant to the Commonwealth's proposed protocol, which necessarily would produce in unencrypted form any files stored thereon to which the encryption key would permit access, is not analogous to the act of responding to a subpoena to produce a document, where the act of production would be testimonial because it makes an assertion that, among other things, the document produced is authentic. To reach this conclusion, the court adopts the Commonwealth's contention that, by decrypting the computers and thereby producing their unencrypted contents, the defendant would be asserting only his ability to decrypt the devices. On this view, he would not be asserting that he owned them, had exclusive use and control of them, or was familiar with any of the files on them; that certain files contained the incriminating evidence sought; or that the documents were authentic. Such is far from the case.

In taking this view of the matter, the court maintains that the defendant merely would be entering a password, which he would not disclose to the Commonwealth, into the encryption program, **[***34]** and would not thereby be selecting and producing any documents. Such an artificial distinction between the act of entering the decryption key and the inevitable result of decrypting the devices,[3] and thereby producing the files for inspection, obfuscates the **[*529]** reality of what the defendant is being compelled to disclose. The Commonwealth seeks the decryption order at issue not for its own sake, but rather to enable the government to access the documents it **[**619]** sought when obtaining the search warrant permitting it to seize the devices. Here, as the United States Court of Appeals for the Eleventh Circuit concluded in similar circumstances, "the decryption and production would be tantamount to testimony by [the defendant] of his knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files." *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335, 1346 (2012)* (*In re Subpoena Duces Tecum*). Inexorably, once the decryption key is entered, the names and sizes of the files (if any) to which the defendant has access on that computer will be produced, **[***35]** the amount of unused space available to the defendant on that computer will become known, and the contents of any files will be made accessible to the Commonwealth.[4]

Moreover, the defendant has denied that there are any documents related to Baylor Holdings, Ltd. (Baylor), on that subset of the seized devices of which he has acknowledged ownership, denied that he created any documents for Baylor,[5] denied that the encrypted communication program he used to communicate with Baylor continues to be installed on those devices, and denied that **[***36]** there are any saved records of the encrypted communications he had with Baylor employees. If the defendant is compelled to decrypt the devices, and any such documents are produced thereby, the act of decryption will have resulted in a prior inconsistent statement by the defendant, which the Commonwealth may seek to use against him at trial.[6]

---

[3] That no individual file would be decrypted on the computer's disk drive until someone requested that particular file is of no moment. According to the Commonwealth's expert, the act of entering the decryption key is what would permit the decryption program to run automatically and provide readable access to an individual file upon request.

[4] The issue, of course, is not whether the decrypted contents of the computer are "testimonial," but whether the act of decrypting the computer and thereby producing decrypted information is "testimonial" under the *Fifth Amendment to the United States Constitution* and *art. 12 of the Massachusetts Declaration of Rights.*

[5] The defendant told police that he received the already-executed mortgage assignment documents from Baylor through the United States mail, and that he merely recorded those documents at the relevant registry of deeds.

[6] The Commonwealth asserts that while, according to the proposed "protocol," it will not introduce evidence of the manner in which the computers were decrypted (unless the defendant opens the door), it intends to introduce evidence of the encryption itself as evidence of "consciousness of guilt." The Commonwealth intends to make this argument even though encrypting files on computers is now a common business practice that is mandatory in many circumstances. See *In re Grand Jury Subpoena Duces Tecum Dated March*

[620]** In light of all this, I would conclude that both the acts of **[*530]** decrypting the devices and of inexorably producing thereby the unencrypted contents of the devices that the Commonwealth otherwise cannot now access are testimonial. See *United States v. Hubbell, 530 U.S. 27, 43, 120 S. Ct. 2037, 147 L. Ed. 2d 24 (2000)* (*Hubbell*); *Doe v. United States, 487 U.S. 201, 212, 108 S. Ct. 2341, 101 L. Ed. 2d 184 (1988)*.

2. *Foregone conclusion*. The court concludes that the act of entering the codes to decrypt the devices would not infringe upon the defendant's privilege against self-incrimination. The court is **[***39]** of the view that the defendant already has disclosed during an interview with State troopers anything that, absent such disclosures, might be testimonial about the act of decryption. In particular, the court concludes that the facts which might be learned through the act of decryption — ownership and control **[*531]** of the seized devices — have been revealed previously by the defendant, or are already known by the Commonwealth through other means, and therefore that the "foregone conclusion" exception applies to what otherwise would be testimonial conduct. The court does not consider whether the act of production, also in my view testimonial, is encompassed within the foregone conclusion exception.

"The touchstone of whether an act of production is testimonial is whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." *In re Subpoena Duces Tecum, 670 F.3d at 1345*, quoting *Curcio v. United States, 354 U.S. 118, 128, 77 S. Ct. 1145, 1 L. Ed. 2d 1225 (1957)*. Under the foregone conclusion doctrine, an otherwise testimonial act of production is not testimonial if the government establishes that, at the time it sought the compelled production, **[***40]** it already knew of that which would explicitly or implicitly be conveyed by the production. *Fisher v. United States, 425 U.S. 391, 410-411, 96 S. Ct. 1569, 48 L. Ed. 2d 39 (1976)* (*Fisher*). See *Hubbell, supra at 36 n.19, 43-45* (act of production testimonial if by compelled conduct "the witness would admit that the papers existed, were in his possession or control, and were authentic"; inquiry turns on extent of government's prior knowledge of existence and location of documents produced); *United States v. Ponds, 454 F.3d 313, 320-321, 372 U.S. App. D.C. 117 (D.C. Cir. 2006)*.

a. *Reasonable particularity standard*. In addressing the extent of knowledge that the government must establish in order to invoke the "foregone conclusion" doctrine, four circuit courts of the United States Court of Appeals have concluded that the government must show with "reasonable particularity" that it already knows the "location, existence, and authenticity of the purported evidence." *In re Subpoena Duces Tecum, 670 F.3d at 1344 & n.20*. See *United States v. Ponds, supra at 320-321*; *In re Grand Jury Subpoena Dated April 18, 2003, 383 F.3d 905, 910 (9th Cir. 2004)*; *In re Grand Jury Subpoena Duces Tecum Dated October 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993)*, cert denied **[***41]** sub nom. *Doe v. United States, 510 U.S. 1091, 114 S. Ct. 920, 127 L. Ed. 2d 214 (1994)*.

[621]** Treating computer files as documents, the United States Court of Appeals for the Eleventh Circuit is, to date, the only circuit court to have addressed the issue specifically in the context of **[*532]** encrypted computers. Concluding that a defendant's compelled decryption and production of the contents of computer

---

25, 2011, 670 F.3d 1335, 1347 (2012) (rejecting "the suggestion that simply because the devices were encrypted necessarily means **[***37]** that [the defendant] was trying to hide something. Just as a vault is capable of storing mountains of incriminating documents, that alone does not mean that it contains incriminating documents, or anything at all"). See also *G. L. c. 93H, § 2* (requiring adoption of regulations "relative to any person that owns or licenses personal information about a resident of the commonwealth" that are designed to "insure the security and confidentiality" of such information; "protect against anticipated threats or hazards to the security or integrity of such information; and protect against unauthorized access to or use of such information"); *201 Code Mass. Regs. §§ 17.00* (2009) (implementing *G. L. c. 93H*); G. Jacobs & K. Laurence, Professional Malpractice § 17.1 (2013) (discussing requirement, pursuant to *G. L. c. 93H* and Supreme Judicial Court Interim Guidelines for Protection of Personal Identifying Data, that attorneys "identify reasonably foreseeable risks to records containing such information, control access to it, establish policies regarding storage and secure transportation of records [e.g., in e-mail correspondence] outside of the premises, require use of up-to-date computers, firewalls, **[***38]** anti-virus software, and *secure encryption of all electronically stored and transported data*" [emphasis supplied]); John W. Sime, Selecting a Law Firm Cloud Provider, ***93 Mich. B.J. 48, 49 (2013)*** ("Data should be encrypted at two stages. The first stage is during data transmission.... [D]ata should also be encrypted while in storage at the cloud provider"). Moreover, it also seems likely, and the Commonwealth has not stated otherwise, that, should any such documents be produced on any of the seized devices, the Commonwealth will seek to characterize evidence of the defendant's earlier denials as inconsistent statements, lies, and further consciousness of guilt.

drives and external hard drives would be sufficiently testimonial to trigger *Fifth Amendment* protections, the court determined that "an act of production is not testimonial — even if the act conveys a fact regarding the existence or location, possession, or authenticity of the subpoenaed materials — if the Government can show with 'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials, thereby making any testimonial aspect a 'foregone conclusion.'" *In re Subpoena Duces Tecum, 670 F.3d at 1345-1346*. To establish a foregone conclusion, "[t]he government does not have to show that it knows specific file names," but would have to "show with some reasonable particularity that it seeks a certain file and is aware, based on other information, that (1) the file exists in **[***42]** some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *Id. at 1349 n.28*.

While the United States Court of Appeals for the First Circuit has yet to consider the issue, I would adopt, at a minimum for purposes of *art. 12*, the same reasonable particularity standard for establishing a foregone conclusion that other circuit courts have adopted, and would conclude that the Commonwealth has not met that burden here. See *id. at 1346, 1349* (no evidence "that the Government, at the time it sought to compel production, knew to any degree of particularity what, if anything, was hidden behind the encrypted wall"). Contrast *United States v. Fricosu, 841 F. Supp. 2d 1232, 1235-1237 (D. Colo. 2012)* (existence and location of files foregone conclusion where government introduced recorded conversation of defendant and third party in which she said that file sought "was on my laptop").

b. *Extent of government's knowledge in this case*. Here, the Commonwealth has made no showing that the existence, possession, and authenticity of the broad categories of items sought are foregone conclusions, under any definition of that term. The court focuses on **[***43]** the defendant's apparent access to the devices seized, and his statements that he owns a "laptop," that "everything is encrypted," and that he could decrypt at least one device ("my computer"). In so doing, it conflates the probable **[*533]** cause showing that the Commonwealth was required to make in order to seize the devices in the first instance with the showing that the Commonwealth must make when, as here, it seeks the otherwise testimonial assistance of a defendant in accessing the contents of those devices.[7] The showing that the **[**622]** Commonwealth must make as to its knowledge of the contents of those devices in order to render anything revealed by the decryption and production of that content a foregone conclusion is significantly greater than what is required to show probable cause. Hence, the "reasonable particularity" standard requires much more than government knowledge that a defendant owns or has access to a particular computer.

Even under the less specific requirements articulated in *Hubbell, supra*, moreover, the government's burden of establishing that, at the time it sought to compel decryption and production, it already knew of the documents sought, rendering any testimonial aspect of that conduct a foregone conclusion, is not met by a showing that a defendant had in his house what is essentially a locked file cabinet in which such documents might have been kept. See *In re Subpoena Duces Tecum, 670 F.3d at **[*534]** 1347 n.25* ("This

---

[7] The Commonwealth argues that the order to provide the key to decrypt the computers and thereby produce the unencrypted documents is necessary because encryption creates significant difficulties for law enforcement officers attempting to prosecute a lengthy list **[***44]** of serious crimes. In a similar vein, the Commonwealth argues explicitly that it should be able to compel the decryption of the devices and the production of their content based on the warrant affidavit, which established probable cause to seize them, as the seizure otherwise has produced no information that would be useful in prosecuting the charged offenses.

It does not follow, however, that further restrictions should be placed on fundamental protections provided by the *Fifth Amendment* and art. 12, which heretofore have been enforced by both State and Federal courts, because the prevalence of computers, in this digital age, at times may facilitate the commission of crimes. The omnipresence of electronic devices which may be monitored, tracked, and recorded has likewise afforded unparalleled opportunities to law enforcement officers in their pursuit of criminal investigations. That encryption may at times present significant difficulties to law enforcement officers does not, as the Commonwealth suggests, result in a conclusion that the *Fifth Amendment* privilege should be restricted so that enforcement is made easier. See *Blaisdell v. Commonwealth, 372 Mass. 753, 761, 364 N.E.2d 191 (1977)* ("Where **[***45]** the privilege is applicable, the constitutionally required result is that no balancing of State-defendant interests is permissible to facilitate the admittedly difficult burdens of the prosecution"). See also *Commonwealth v. Doe, 405 Mass. 676, 680, 544 N.E.2d 860 (1989)*.

situation is no different than if the Government seized a locked strongbox. Physical possession of the entire lockbox is not the issue; whether the Government has the requisite knowledge of what is contained inside the strongbox is the critical question").

i. *Existence and content of documents sought*. Aside from knowledge pertinent to the existence and nature of the encryption program itself,[8] the government has not shown that it has **[***46]** any knowledge as to the existence or content of any particular files or documents on any particular computer.[9] To the contrary, the Commonwealth's computer forensic expert's affidavit provides general information about what computers can do, but makes no specific assertions as to any files or documents expected to be found on any of the seized devices. The focus of the trooper's affidavit is on the defendant's actions away from his home, as observed by police surveillance.[10] There no **[**623]** description **[*535]** of files that are expected to be found,[11] let alone that are known to exist, on the defendant's computers,[12] the affidavit contains numerous indications of the defendant's apparent efforts to avoid downloading documents to his computers, using telephone or facsimile transmission from his house. Service providers' Web sites that the Commonwealth asserts the defendant used,[13] are described as advertising that

---

[8] David Papargiris, the director of the Attorney General's computer forensics laboratory, submitted an affidavit in support of the Commonwealth's motion to compel decryption. Papargiris stated that some of the storage devices seized from the defendant's house indicate use of an encryption program called "DriveCrypt Plus Pack." When this program is installed on a computer, the computer displays a particular screen requesting a password every time the computer is started. Nothing further can be done on that computer until the user **[***48]** enters the password. Because all of the seized computers display the same screen when they are started, Papargiris believes that the program is being used for all of the seized computers and separate storage devices.

[9] As to one external hard drive, the Commonwealth has shown knowledge of two documents related to the defendant's own home, not involving Baylor Holdings, Ltd. (Baylor), or Puren Ventures, Inc., and some links (which do not involve documents) to third-party Web sites.

[10] The trooper's affidavit details police surveillance and review of surveillance video footage of the defendant driving to various stores and post offices. Police suspect the defendant purchased money orders and gift cards at these locations, by filling out forms by hand. Additional surveillance footage shows the defendant on one occasion entering and leaving a court house that also houses a registry of deeds. Cooperating witnesses and documents obtained from third parties indicate that an unknown individual purporting to represent Baylor arranged for checks to be mailed via United States mail to the defendant's former office building in Boston.

The affidavit also recounts police observations of the defendant **[***49]** suspected to be using publicly available and "anonymous" wireless Internet services, which allow access to the Internet without identifying a particular user's Internet Protocol (IP) address, from a variety of locations, such as restaurants. These suspicions are based largely on his presence at particular times at locations where such services are available, or in nearby parking lots, and, on two occasions, because he was observed apparently using a laptop.

[11] Based on the affidavits, the Commonwealth clearly had probable cause to seize the devices themselves. In this regard, there was reason to think the defendant used some unspecified computer to connect to the Internet in communicating with the intended victims of the fraud.

[12] The search warrant affidavit states that the seized computers "are capable of storing," inter alia, information about the defendant's "contacts and activities" for a period of more than four months, "anything having do to with" his financial transactions over an approximately three-year period (although the fraudulent mortgage scheme allegedly lasted for less than one year), any Internet search, over an unlimited time frame and geographic area, for residential **[***50]** properties, and "any" document filed with "any Massachusetts Registry of Deeds," again over an unlimited period. The same information is also sought, from "[a]ny and all records, documents, items, and/or data, in whatever form," to be found at the defendant's house and in his automobile. The affidavit states further that, because "[t]ransferring data files between computers or onto storage devices such as disks is a simple task that takes little time … once a file is on one computer at a given location — particularly a home — I believe that there is probable cause to believe that it could be moved to any storage device or other computer at that same location." The court does not address whether these broad categories and date ranges meet the specificity requirements of *Commonwealth v. McDermott, 448 Mass. 750, 771-775, 864 N.E.2d 471*, cert. denied, *552 U.S. 910, 128 S. Ct. 257, 169 L. Ed. 2d 188 (2007)* (concluding that each computer file is separate, closed container, and discussing limitations necessary on searches to be conducted of computer hard drives so that warrants to conduct such searches are not constitutionally infirm). The record here also does not indicate whether the Commonwealth sought a warrant as to the search of **[***51]** each of the devices once they had been seized and transported to the police laboratory. See *id. at 774-775*.

[13] The trooper's affidavit suggests that the defendant made use of third-party services over the Internet to establish certain corporate telephone and facsimile numbers The Web sites

documents are stored **[*536]** on the third-party service providers' computers, and **[**624]** may be accessed over the Internet without downloading anything to a user's own computer. See G. Jacobs & K. Laurence, Professional Malpractice § 17.1 (2013) (discussing "cloud computing" as "in essence **[***47]** a sophisticated form of remote electronic data storage on the Internet .... Unlike traditional methods that maintain data on a computer or service at a law office or other place of business, data stored 'in the cloud' [cloud computing] is kept on large servers located elsewhere and maintained by a vendor"). The Commonwealth accordingly has not shown that it knows "with some reasonable particularity that it seeks a certain file and is aware, based on other information, that (1) the file exists in some specified location, (2) the file is possessed by the target of the subpoena, and (3) the file is authentic." *In re Subpoena Duces Tecum, 670 F.3d at 1349 n.28*.

"In *Fisher*, [*supra at 411*,] ... the act of production was not testimonial because the Government had knowledge of each fact that had the potential of being testimonial. As a contrast, the Court in *Hubbell*[, *supra at 44-45*,] found there was testimony in the production of the documents since the Government had no knowledge of the existence of documents, other than a suspicion that documents likely existed and, if they did exist, that they would fall within the broad categories requested." *In re Subpoena Duces Tecum, 670 F.3d at 1345*. Here, too, the government has no more than a suspicion that broad categories of documents, extending over periods of years, may exist on one or more of the seized devices. See *United States v. Doe, 465 U.S. 605, 613-614, 104 S. Ct. 1237, 79 L. Ed. 2d 552 & nn.11-13 (1984)*. See, e.g., *Commonwealth v. Hughes, 380 Mass. 583, 592, 404 N.E.2d 1239*, cert. denied, *449 U.S. 900, 101 S. Ct. 269, 66 L. Ed. 2d 129 (1980)* (act of producing gun by defendant charged with assault by means of dangerous weapon would not convey "merely trivial new knowledge" but would communicate "just those matters about which the Commonwealth desires but does not have solid information"). Contrast *Fisher, supra.*

[*537] The court **[***53]** notes that the defendant has admitted to engaging in real estate transactions for Baylor, communicating with Baylor over an encrypted communication program installed on his laptop, using the Internet to communicate, having more than one computer, that "everything" on his computer is encrypted, and that he knows how to decrypt it. The court points also to the fact that two of the mortgage assignments to Baylor apparently are fraudulent.[14] None of this, however, establishes anything about the government's knowledge of the documents, if any, that may be stored on the seized devices.[15] See *In re Grand Jury Subpoena dated April 18, 2003, 383 F.3d at 910* ("Although the government possessed extensive knowledge about [defendant's] price-fixing activities as a result of interviews with cooperating **[**625]** witnesses and [his] own incriminating statements ... , it is the government's knowledge of the existence and possession of the actual documents, not the information contained therein, that is central to the foregone conclusion inquiry").

Furthermore, the court misconstrues the extent of the defendant's statements concerning the encryption, thereby inferring that the defendant has asserted greater access and control than is in fact the case. The court conflates the encryption of the disk drive on one of the computers, which the defendant acknowledged, with the existence of the encrypted communication

---

described in the affidavit, however, are explicitly discussed as services which would not require placing any documents on a suspect's own computer. They are described as permitting anonymous use, storing documents on the third-party service provider's computers, and permitting access to, for instance, e-mail message attachments without downloading anything to a user's own computer. See *United States v. Falso, 544 F.3d 110, 112-114 (2d Cir. 2008)* (warrant affidavit asserting after forensic examination of computer that defendant "appeared to have gained or attempted to gain" access to Web site which distributed and sold child pornography, where e-mail address belonging to defendant was listed as subscriber to member section of Web site, defendant had Internet service from his house, and defendant had been convicted of prior misdemeanor sex offense, did not establish probable cause that images of child **[***52]** pornography would be found on defendant's computer).

[14] Police suspect the two assignments to Baylor are fraudulent based on their communication with the closing attorneys involved in the sales of the two properties **[***54]** not long after the assignments had been recorded, and with the banks that previously held the mortgages.

[15] The trooper's affidavit states, without record support, that evidence seized from the external hard drive shows that the defendant used his computers to create the forged assignments. The documents described as having been observed on the external hard drive, however, which are the only specific documents described as existing on any of the seized devices, relate to an unsigned release of a mortgage on the defendant's own property, and not to any assignment to Baylor; nothing in the affidavit indicates how the documents were created.

program[16] purportedly used to communicate with Baylor.[17] Contrary to the court's statement, the defendant has not said that the **[*538]** communication program that he ran in order to communicate **[***55]** with someone at Baylor is installed on any of his computers at this time; indeed, he stated explicitly that it *had* been installed on his "laptop" but that it might no longer be there and that the program itself "may not exist anymore."[18]

[16] As the defendant described it to police, the communication program works like an online "chat" session; one person types, and the other person sees the message displayed on his or her computer screen. The message that the user types is encrypted before it is sent to the recipient. The program as described is not intended to create and store documents, or to encrypt computer drives, but, rather, to allow users to send messages back and forth in a secure way so that someone trying to eavesdrop on the messages being sent would be unable to do so.

[17] The court points to the defendant's statement to police that, "[i]n order to decrypt the information, he would have to 'start the program'" as being a reference to the "DriveCrypt" encryption software on the computer drives that it takes as an admission of control over the drives and the ability to decrypt them. The defendant was speaking, however, of the communication program he started in order to communicate **[***56]** in a "chat" session with the Russian individuals at Baylor, not of the encryption of the computer drives themselves. According to the defendant's statement, the communication program takes up very little space on a computer drive and can be installed on any device, including a removable "flash" drive; the program requires only an Internet connection, and can be run from anywhere, by inserting a "flash" drive into a computer.

The defendant, who is a native of Russia, obtained the program at a financial conference in Europe sometime in 2004, 2005, or 2006, because he intended to develop his business in the Russian market; he believed that encrypted communication was necessary to address Russian security concerns. In response to an explicit question, the defendant answered that he did not know whether the communication program saved the contents of any conversation on a computer drive, then clarified that the communication program did not save any of the typed conversations, but, rather, deleted them at the end of a communication session, and that he thought it did not store copies of the conversations because it was intended to be secure.

[18] When asked at another point about the location **[***57]** of the "encryption device" that he used to communicate with Baylor ("Is it on your laptop? Is it on your desktop"?) the defendant replied, "At different points it was." Whether the defendant was referring to the "laptop" seized from his house or the "netbook" seized from his car is unclear. It is also unclear which of the two other computers he meant by "your desktop."

On this record, the Commonwealth does not know what is stored on any of the seized devices, or if any of them contain information relevant to the charged offenses. Notwithstanding the court's conclusion to the contrary, the affidavit in support of the search warrant and the defendant's statements to police do not give rise to a foregone conclusion that whatever would be revealed by the defendant's entry of the decryption key, and consequent production of the unencrypted contents of all of the **[*539]** seized devices, is already known to the government. See **[**626]** *Hubbell, supra at 45* ("the overbroad argument that a businessman … will always possess general business and tax records," could not "cure [the] deficiency" of government's failure to demonstrate its "prior knowledge of either the existence or the whereabouts" of requested **[***58]** documents); *In re Grand Jury Subpoena Dated April 18, 2003, 383 F.3d at 911* ("A subpoena such as this, which seeks all documents within a category but fails to describe those documents with any specificity indicates that the government needs the act of production to build its case against [the defendant]"). See also *United States v. Doe, 465 U.S. at 614 n.12*.

Even more fundamentally, to establish a foregone conclusion the government must first show that it knows any files at all exist on a particular computer. In *In re Subpoena Duces Tecum, 670 F.3d at 1346, 1349*, the United States Court of Appeals for the Eleventh Circuit reversed an order requiring a suspect to decrypt his computer, which was using the same type of encryption program that the Commonwealth's expert avers is being used to encrypt the devices here, because the court concluded that the government had not shown that any files existed on the computer, other than the encryption program itself. The encryption program at issue not only encrypts information stored on a computer, it also encrypts all unused space on the computer's hard drive, making it impossible to determine how much of the computer contains actual files and **[***59]** how much is unused or blank. Because the government could not show that any data on the computer represented actual files, the court concluded that "[t]he [g]overnment has failed to show any basis, let alone shown a basis with reasonable particularity, for its belief that encrypted files exist on the drives …"). *Id. at 1349*. Given the properties of the encryption program in place on the seized devices here, as described by the Commonwealth's expert, the Commonwealth does not know whether they

contain any documents of any kind.

ii. *Ownership, exclusive use, and control*. The court's decision also conflates access to a particular computer[19] with access to, and knowledge and control of, each of the files on that **[*540]** computer.[20] As stated, the United States Supreme Court has rejected the view that a defendant's access to a locked cabinet, whose contents are not known but that might contain the documents sought, is sufficient to establish that **[**627]** the government knows the contents of those documents, such that their compelled production by unlocking the cabinet is a foregone conclusion. *Hubbell, supra.* This distinction is even more critical in considering the issue of production or search of **[***60]** files stored on a computer. See *In re Subpoena Duces Tecum, 670 F.3d at 1346, 1349*; *United States v. Fricosu, 841 F. Supp. 2d 1232, 1235-1237 (D. Colo. 2012)*. Like many courts to have considered the issue, we have concluded that each computer file is a separate document in a closed container, requiring that searches of a computer to locate specific files must be limited and particular. See *Commonwealth v. McDermott, 448 Mass. 750, 775, 864 N.E.2d 471*, cert. denied, *552 U.S. 910, 128 S. Ct. 257, 169 L. Ed. 2d 188 (2007)*. See *United States v. Potts, 586 F.3d 823, 833 (10th Cir. 2009)* ("officers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the warrant"). See, e.g., *United States v. Mann, 592 F.3d 779, 786 (7th Cir.)*, cert. denied, *561 U.S. 1034, 130 S. Ct. 3525, 177 L. Ed. 2d 1106 (2010)*, and cases cited; *United States v. Burgess, 576 F.3d 1078, 1088-1089 (10th Cir.)*, cert. denied, *558 U.S. 1097, 130 S. Ct. 1028, 175 L. Ed. 2d 629 (2009)*; *United States v. Carey, 172 F.3d 1268, 1270-1273 (10th Cir. 1999)*; *United States v. Stierhoff, **[*541]** 477 F. Supp. 2d 423, 439 n.8 (D.R.I. 2007)*, aff'd, *549 F.3d 19 (1st Cir. 2008)*. See generally Goldfoot, The Physical Computer and the Fourth Amendment, *16 Berkeley J. Crim. L. 112 (2011)*; **[***61]** Kerr, Searches and Seizures in a Digital World, *119 Harv. L. Rev. 531 (2005)*; Trepel, Digital Searches, General Warrants, and the Case for the Courts, *10 Yale J. L. & Tech. 120 (2007)*. Therefore, the government must establish knowledge of the existence of the particular file, either by the name of the file or by knowledge of its contents, as well as the defendant's access to that portion of the encrypted drive on which the file exists. See *In re Subpoena Duces Tecum, 670 F.3d at 1346, 1349*. It has not done so here.

3. *Attorney-client privilege*. I would conclude also that the defendant cannot be compelled to enter the decryption key, and thereby produce all documents to which he has access, on each device, under the protocol as proposed by the Commonwealth, because of the possibility that the computers contain privileged information relating to the defendant's legal clients. See *Preventive Medicine Assocs. v. Commonwealth, 465 Mass. 810, 822-824, 992 N.E.2d 257 & nn.24-26 (2013)* **[***63]** ("a search, to be reasonable, must include reasonable steps designed to prevent a breach of the attorney-client privilege .... [T]he harm to the defendant could be irreparable if the Commonwealth viewed privileged materials, even if only by accident"). The issue of attorney-client privilege is not addressed in the search warrant affidavit, the protocol proffered in conjunction with the Commonwealth's motion to compel, or the court's decision.[21]

---

[19] The defendant stated that the computer in his home was in an area accessible to anyone in the house or who came to his home office, and that Baylor employees accessed his computer using the encrypted communication program. On this record, the government has not shown that the defendant had exclusive access to the computers.

[20] According to the Commonwealth's expert, the encryption program on the seized computers permits multiple users with distinct passwords, each potentially having access to a different portion of the computer drive. The government does not currently know how many user accounts exist on any of the computers, and to which portions, if any, of any particular **[***62]** computer the defendant has access. See *Trulock v. Freeh, 275 F.3d 391, 403-404 (4th Cir. 2001)* (where two individuals shared use of computer, and both had access to entire computer hard drive, other user did not have authority to consent to search of suspect's password-protected files on that drive). The ability to enter a password to start the computer does not, therefore, indicate whether the defendant has access to or control over all of the different user accounts and different sections of the computer drives that may have been established on any of the seized computers; it would, however, potentially reveal to the Commonwealth the existence of other accounts, and possibly others who use the computers, about which the Commonwealth has indicated no knowledge.

[21] The question is addressed by the defendant in his brief and by the Commonwealth in its reply brief. While the Commonwealth asserts in its reply brief, prior to a discussion on the merits, that the question of attorney-client privilege is not part of the reported question before the court, the plain language of the Commonwealth's motion to report, which was allowed, and which is presented by the Commonwealth in its initial brief as "the issue presented for review," asks, "Can the defendant be compelled *pursuant to the Commonwealth's*

The defendant told police that he ran a law office from his house, and that he had **[**628]** approximately ten active personal injury clients. He stated that he sent facsimile transmissions to his personal injury clients, when necessary, using TrustFax, an Internet **[*542]** facsimile site, from his home computer. He acknowledged that "my computer" is encrypted, but did not identify which one of the seized devices he meant, and asserted that the encryption was to protect his "privacy." The police photographs of one of the computer screens when that computer was running, showing the directory name "K:\Leon Documents\My Scans" and an icon labeled "Attorney Leon I. Gelfgatt," do not indicate that the documents, if any, on the computers relate to Baylor and not to the defendant's other clients. Nor do they show that the computers contain any documents related to Baylor. Because the proposed protocol potentially would allow the Commonwealth to view privileged information related to the defendant's other clients, I would conclude, on this basis as well, that the requested order to compel is unreasonable and impermissible.

4. *Conclusion*. Because I believe that the compelled decryption and production **[***65]** here is fundamentally testimonial, and the Commonwealth has not established a foregone conclusion that the existence, location, and authenticity of the information that would be produced is known to the government, I respectfully dissent, and would answer the reported question, "No."

End of Document

---

proposed protocol to provide his key to seized encrypted digital evidence …" (emphasis supplied)? The joint stipulation of the parties as to the wording of the reported question uses identical **[***64]** language.

KeyCite Yellow Flag - Negative Treatment
Distinguished by United States v. Oriho, 9th Cir.(Ariz.), August 10, 2020

108 S.Ct. 2341
Supreme Court of the United States

John DOE, Petitioner
v.
UNITED STATES.

No. 86–1753.
|
Argued March 2, 1988.
|
Decided June 22, 1988.

Synopsis

Target of grand jury investigation appealed from order of the United States District Court for the Southern District of Texas, finding him in civil contempt for failing to comply with order directing him to sign consent directive authorizing foreign banks to disclose records of any and all accounts over which target had right of withdrawal. The Court of Appeals affirmed in an unpublished opinion, 812 F.2d 1404, and target petitioned for certiorari. The Supreme Court, Justice Blackmun, held that court order compelling target of grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, does not violate target's Fifth Amendment privilege against self-incrimination.

Affirmed.

Justice Stevens filed dissenting opinion.

West Headnotes (8)

[1] **Witnesses** Privilege as to production of documents

Court order compelling target of grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, does not violate target's Fifth Amendment privilege against self-incrimination. U.S.C.A. Const.Amend. 5.

39 Cases that cite this headnote

[2] **Witnesses** Privilege as to production of documents

Contents of foreign bank records sought by Government are not privileged under Fifth Amendment. U.S.C.A. Const.Amend. 5.

8 Cases that cite this headnote

[3] **Witnesses** Persons entitled to claim privilege

Foreign banks cannot invoke Fifth Amendment in declining to produce bank records; privilege does not extend to such artificial entities. U.S.C.A. Const.Amend. 5.

5 Cases that cite this headnote

[4] **Witnesses** Self-Incrimination

Fifth Amendment privilege against self-incrimination protects person only against being incriminated by his own compelled testimonial communications. U.S.C.A. Const.Amend. 5.

173 Cases that cite this headnote

[5] **Witnesses** Self-Incrimination

If compelled statement is not testimonial and for that reason not protected by Fifth Amendment privilege against self-incrimination, it cannot become so because it will lead to incriminating evidence. U.S.C.A. Const.Amend. 5.

97 Cases that cite this headnote

[6] **Witnesses** Self-Incrimination

In order to be "testimonial" for purposes of Fifth Amendment privilege against self-incrimination, accused's communication must itself, explicitly or implicitly, relate factual assertion or disclose information; only then is person compelled

to be "witness" against himself. U.S.C.A. Const.Amend. 5.

240 Cases that cite this headnote

[7] **Witnesses** Self-Incrimination

Fifth Amendment privilege against self-incrimination may be asserted only to resist compelled explicit or implicit disclosures of incriminating information. U.S.C.A. Const.Amend. 5.

64 Cases that cite this headnote

[8] **Witnesses** Privilege as to production of documents

Grand jury investigation target's execution of consent directive authorizing foreign banks to disclose records of his accounts as required by foreign bank secrecy laws did not have testimonial significance, so that order compelling target to sign directive did not violate target's Fifth Amendment privilege against self-incrimination; form that target was ordered to sign did not acknowledge that account in foreign bank existed or was controlled by target, and did not indicate whether documents or any other information relating to target were present at foreign bank, assuming such account did exist. U.S.C.A. Const.Amend. 5.

64 Cases that cite this headnote

****2342** *Syllabus* *

***201** Pursuant to a subpoena, petitioner, the target of a federal grand jury investigation, produced some records as to accounts at foreign banks, but invoked his Fifth Amendment privilege against self-incrimination when questioned about the existence or location of additional bank records. After the foreign banks refused to comply with subpoenas to produce any account records because their governments' laws prohibit such disclosure without the customer's consent, the Government filed a motion with the Federal District Court for an order directing petitioner to sign a consent directive, without identifying or acknowledging the existence of any account, authorizing the banks to disclose records of any and all accounts over which he had a right of withdrawal. The court denied the motion, concluding that compelling petitioner to sign the form was prohibited by the Fifth Amendment. The Court of Appeals disagreed and reversed. On remand, the District Court ordered petitioner to execute the consent directive, and, after he refused, found him in civil contempt. The Court of Appeals affirmed.

Held: Because the consent directive here is not testimonial in nature, compelling petitioner to sign it does not violate his Fifth Amendment privilege against self-incrimination. Pp. 2345–2352.

****2343** (a) In order to be "testimonial," an accused's oral or written communication, or act, must itself, explicitly or implicitly, relate a factual assertion or disclose information. Cf. *Fisher v. United States,* 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39; *United States v. Doe,* 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552. It is consistent with the history of and the policies underlying the Self–Incrimination Clause to hold that the privilege may be asserted only to resist compelled explicit or implicit disclosures of incriminating information. Pp. 2346–2350.

(b) Petitioner's execution of the consent directive here would not have testimonial significance, because neither the form nor its execution communicates any factual assertions, implicit or explicit, or conveys any information to the Government. The form does not acknowledge that an account in a foreign bank is in existence or that it is controlled by petitioner. Nor does the form indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist. Given the consent directive's phraseology, petitioner's execution of the directive has no testimonial ***202** significance either. If the Government obtains bank records after petitioner signs the directive, the only factual statement made by anyone will be the *bank's* implicit declaration, by its act of production in response to a subpoena, that *it* believes the accounts to be petitioner's. Pp. 2350–2352.

812 F.2d 1404, (CA5 1987), affirmed.

BLACKMUN, J., delivered the opinion of the Court, in which REHNQUIST, C.J., and BRENNAN, WHITE, MARSHALL, O'CONNOR, SCALIA, and KENNEDY, JJ., joined. STEVENS, J., filed a dissenting opinion, *post*, p. ——.

Attorneys and Law Firms

Richard E. Timbie argued the cause for petitioner. With him on the briefs were *Cono R. Namorato, Scott D. Michel,* and *Jeffrey S. Lehman.*

Charles A. Rothfeld argued the cause for the United States. With him on the brief were *Solicitor General Fried, Assistant Attorney General Rose, Deputy Solicitor General Bryson, Gary R. Allen, Robert E. Lindsay,* and *Alan Hechtkopf.**

* *Rex E. Lee, Joseph B. Tompkins, Jr.,* and *Carter G. Phillips* filed a brief for the Government of the Cayman Islands as *amicus curiae.*

Opinion

Justice BLACKMUN delivered the opinion of the Court.

[1] This case presents the question whether a court order compelling a target of a grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, violates the target's Fifth Amendment privilege against self-incrimination.

I

Petitioner, named here as John Doe, is the target of a federal grand jury investigation into possible federal offenses arising from suspected fraudulent manipulation of oil cargoes and receipt of unreported income. Doe appeared before the grand jury pursuant to a subpoena that directed him to produce records of transactions in accounts at three named banks in the Cayman Islands and Bermuda. Doe produced some bank records and testified that no additional records responsive ***203** to the subpoena were in his possession or control. When questioned about the existence or location of additional records, Doe invoked the Fifth Amendment privilege against self-incrimination.

The United States branches of the three foreign banks also were served with subpoenas commanding them to produce records of accounts over which Doe had signatory authority. Citing their governments' bank-secrecy laws, which prohibit the disclosure of account records without the customer's consent, [1] the banks refused ****2344** to comply. See App. to Pet. for Cert. 17a, n. 2. The Government then filed a motion with the United States District Court for the Southern District of Texas that the court order Doe to sign 12 forms consenting to disclosure of any bank records respectively relating to 12 foreign bank accounts over which the Government knew or suspected that Doe had control. The forms indicated the account numbers and described the documents that the Government wished the banks to produce.

The District Court denied the motion, reasoning that by signing the consent forms, Doe would necessarily be admitting ***204** the existence of the accounts. The District Court believed, moreover, that if the banks delivered records pursuant to the consent forms, those forms would constitute "an admission that [Doe] exercised signatory authority over such accounts." *Id.*, at 20a. The court speculated that the Government in a subsequent proceeding then could argue that Doe must have guilty knowledge of the contents of the accounts. Thus, in the court's view, compelling Doe to sign the forms was compelling him "to perform a testimonial act that would entail admission of knowledge of the contents of potentially incriminating documents," *id.,* at 20a, n. 6, and such compulsion was prohibited by the Fifth Amendment. The District Court also noted that Doe had not been indicted, and that his signing of the forms might provide the Government with the incriminating link necessary to obtain an indictment, the kind of "fishing expedition" that the Fifth Amendment was designed to prevent. *Id.,* at 21a.

The Government sought reconsideration. Along with its motion, it submitted to the court a revised proposed consent directive that was substantially the same as that approved by the Eleventh Circuit in *United States v. Ghidoni,* 732 F.2d 814, cert. denied, 469 U.S. 932, 105 S.Ct. 328, 83 L.Ed.2d 264 (1984). The form purported to apply to any and all accounts over which Doe had a right of withdrawal, without acknowledging the existence of any such account. [2] The District Court denied this motion also, reasoning ***205** that compelling execution of the consent directive might lead to

the uncovering and linking of Doe to accounts that the grand jury did not know were in existence. The court concluded that execution of the proposed form would "admit signatory authority over the speculative accounts [and] would implicitly authenticate any records of the speculative accounts provided by the banks pursuant to the consent." App. to Pet. for Cert. 13a, n. 7.

The Court of Appeals for the Fifth Circuit reversed in an unpublished *per curiam* opinion, judgt. order reported at 775 F.2d 300 (1985). Relying on its intervening decision in *In re United States Grand Jury Proceedings (Cid),* 767 F.2d 1131 (1985), ****2345** the court held that Doe could not assert his Fifth Amendment privilege as a basis for refusing to sign the consent directive, because the form "did not have testimonial significance" and therefore its compelled execution would not violate Doe's Fifth Amendment rights. App. to Pet. for Cert. 7a. [3]

On remand, the District Court ordered petitioner to execute the consent directive. He refused. The District Court accordingly found petitioner in civil contempt and ordered ***206** that he be confined until he complied with the order. *Id.,* at 2a. The court stayed imposition of sanction pending appeal and application for writ of certiorari. *Id.,* at 2a–3a.

The Fifth Circuit affirmed the contempt order, again in an unpublished *per curiam,* concluding that its prior ruling constituted the "law of the case" and was dispositive of Doe's appeal. *Id.,* at 3a; judgt. order reported at 812 F.2d 1404 (1987). We granted certiorari, 484 U.S. 813, 108 S.Ct. 64, 98 L.Ed.2d 28 (1987), to resolve a conflict among the Courts of Appeals as to whether the compelled execution of a consent form directing the disclosure of foreign bank records is inconsistent with the Fifth Amendment. [4] We conclude that a court order compelling the execution of such a directive as is at issue here does not implicate the Amendment.

II

[2] **[3]** It is undisputed that the contents of the foreign bank records sought by the Government are not privileged under the Fifth Amendment. See *Braswell v. United States,* 487 U.S. 99, 108–110, 108 S.Ct. 2284, 2290, 101 L.Ed.2d 98 (1988); *United States v. Doe,* 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552 (1984); *Fisher v. United States,* 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). There also is no question that the foreign banks cannot invoke the Fifth Amendment in declining to produce the documents; the privilege does not extend to such artificial entities. See *Braswell v. United States,* 487 U.S., at 102–103, 108 S.Ct. at 2287; *Bellis v. United States,* 417 U.S. 85, 89–90, 94 S.Ct. 2179, 2183–2184, 40 L.Ed.2d 678 (1974). Similarly, petitioner asserts no Fifth Amendment right to prevent the banks from disclosing the account records, for the Constitution "necessarily does not proscribe incriminating statements elicited from another." ***207** *Couch v. United States,* 409 U.S. 322, 328, 93 S.Ct. 611, 616, 34 L.Ed.2d 548 (1973). Petitioner's sole claim is that his execution of the consent forms directing the banks to release records as to which the banks believe he has the right of withdrawal has independent testimonial significance that will incriminate him, and that the Fifth Amendment prohibits governmental compulsion of that act.

[4] The Self–Incrimination Clause of the Fifth Amendment reads: "No person ... shall be compelled in any criminal case to be a witness against himself." This Court has explained that "the privilege protects a person only against being incriminated by his own compelled testimonial communications." *Fisher v. United* ****2346** *States,* 425 U.S., at 409, 96 S.Ct., at 1580, citing *Schmerber v. California,* 384 U.S. 757, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966); *United States v. Wade,* 388 U.S. 218, 87 S.Ct. 1926, 18 L.Ed.2d 1149 (1967); and *Gilbert v. California,* 388 U.S. 263, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967). The execution of the consent directive at issue in this case obviously would be compelled, and we may assume that its execution would have an incriminating effect. [5] The question on which this case turns is whether the act of executing the form is a "testimonial communication." The parties disagree about both the meaning of "testimonial" and whether the consent directive fits the proposed definitions.

A

[5] Petitioner contends that a compelled statement is testimonial if the Government could use the content of the speech or writing, as opposed to its physical characteristics, to further a criminal investigation of the witness. The second half of petitioner's "testimonial" test is that the statement must be incriminating, which is, of course, already a separate requirementfor ***208** invoking the privilege. Thus, Doe contends, in essence, that every written and oral statement significant for its content is necessarily testimonial for purposes of the Fifth Amendment.[6] Under this view, the consent directive is testimonial because it is a declarative statement of consent made by Doe to the foreign banks, a statement that the Government will use to persuade the banks to produce potentially incriminating account records that would otherwise be unavailable to the grand jury.

The Government, on the other hand, suggests that a compelled statement is not testimonial for purposes of the privilege, unless it implicitly or explicitly relates a factual assertion or otherwise conveys information to the Government. It argues that, under this view, the consent directive is not testimonial because neither the directive itself nor Doe's execution of the form discloses or communicates facts or information. Petitioner disagrees.

The Government's view of the privilege, apparently accepted by the Courts of Appeals that have considered compelled consent forms,[7] is derived largely from this ****2347** Court's decisions in *Fisher* and *Doe.* The issue presented in those cases was whether the act of producing subpoenaed documents, not itself the making of a statement, might nonetheless have some protected testimonial aspects. The Court concluded that the act of production could constitute protected testimonial communication because it might entail implicit statements of fact: by producing documents in compliance with a subpoena, the witness would admit that the papers existed, were in his possession or control, and were authentic. *United States v. Doe,* 465 U.S., at 613, and n. 11, 104 S.Ct., at 1242, and n. 11; *Fisher,* 425 U.S., at 409–410, 96 S.Ct., at 1580; *id.,* at 428, 432, 96 S.Ct., at 1589, 1591 (concurring opinions). See *Braswell v. United States,* 487 U.S., at 104, 108 S.Ct., at 2288; *ante,* at 122, 108 S.Ct., at 2297 (dissenting opinion). Thus, the Court made clear that the Fifth Amendment privilege against self-incrimination applies to acts that imply assertions of fact.

[6] We reject petitioner's argument that this test does not control the determination as to when the privilege applies to oral or written statements. While the Court in *Fisher* and *Doe* did not purport to announce a universal test for determining the scope of the privilege, it also did not purport to establish a more narrow boundary applicable to acts alone. To the contrary, the Court applied basic Fifth Amendment principles.[8] An examination of the Court's application of these ***210** principles in other cases indicates the Court's recognition that, in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information.[9] Only then is a person compelled to be a "witness" against himself.

This understanding is perhaps most clearly revealed in those cases in which the Court has held that certain acts, though incriminating, are not within the privilege. Thus, a suspect may be compelled to furnish a blood sample, *Schmerber v. California,* 384 U.S., at 765, 86 S.Ct., at 1832; to provide a handwriting exemplar, *Gilbert v. California,* 388 U.S., at 266–267, 87 S.Ct., at 1953 or a voice exemplar, *United States v. Dionisio,* 410 U.S. 1, 7, 93 S.Ct. 764, 768, 35 L.Ed.2d 67 (1973); to stand in a lineup, *United States v. Wade,* 388 U.S., at 221–222, 87 S.Ct., at 1929; and to wear particular clothing, *Holt v. United States,* 218 U.S. 245, 252–253, 31 S.Ct. 2, 6, 54 L.Ed. 1021 (1910). These decisions are grounded on the proposition that "the privilege protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *Schmerber,* 384 U.S., at 761, 86 S.Ct., at 1830. The ****2348** Court accordingly held that the privilege ***211** was not implicated in each of those cases, because the suspect was not required "to disclose any knowledge he might have," or "to speak his guilt," *Wade,* 388 U.S., at 222–223, 87 S.Ct., at 1929–1930. See *Dionisio,* 410 U.S., at 7, 93 S.Ct., at 768; *Gilbert,* 388 U.S., at 266–267, 87 S.Ct., at 1953. It is the "extortion of

information from the accused," *Couch v. United States,* 409 U.S., at 328, 93 S.Ct., at 616; the attempt to force him "to disclose the contents of his own mind," *Curcio v. United States,* 354 U.S. 118, 128, 77 S.Ct. 1145, 1151, 1 L.Ed.2d 1225 (1957), that implicates the Self–Incrimination Clause. See also *Kastigar v. United States,* 406 U.S. 441, 445, 92 S.Ct. 1653, 1656, 32 L.Ed.2d 212 (1972) (the privilege "protects against any *disclosures* that the witness reasonably believes could be used in a criminal prosecution or could lead to other evidence that might be so used") (emphasis added). "Unless some attempt is made to secure a communication —written, oral or otherwise—upon which reliance is to be placed as involving [the accused's] consciousness of the facts and the operations of his mind in expressing it, the demand made upon him is not a testimonial one." 8 Wigmore § 2265, p. 386. [10]

***212** **[7]** It is consistent with the history of and the policies underlying the Self–Incrimination Clause to hold that the privilege may be asserted only to resist compelled explicit or implicit disclosures of incriminating information. Historically, the privilege was intended to prevent the use of legal compulsion to extract from the accused a sworn communication of facts which would incriminate him. Such was the process of the ecclesiastical courts and the Star Chamber—the inquisitorial method of putting the accused upon his oath and compelling him to answer questions designed to uncover uncharged offenses, without evidence from another source. See *Andresen v. Maryland,* 427 U.S. 463, 470–471, 96 S.Ct. 2737, 2743–2744, 49 L.Ed.2d 627 (1976); 8 Wigmore § 2250; E. Griswold, The Fifth Amendment Today 2–3 (1955). The major thrust of the policies undergirding the privilege is to prevent such compulsion. The Self–Incrimination Clause reflects " 'a judgment ... that the prosecution should [not] be free to build up a criminal case, in whole or in part, with the assistance of enforced *disclosures* by the accused' " (emphasis added). *Ullmann v. United States,* 350 U.S. 422, 427, 76 S.Ct. 497, 501, 100 L.Ed. 511 (1956), quoting *Maffie v. United States,* 209 F.2d 225, 227 (CA1 1954). The Court in *Murphy v. Waterfront Comm'n of New York Harbor,* 378 U.S. 52, 84 S.Ct. 1594, 12 L.Ed.2d 678 (1964), explained that the privilege is founded on

> "our unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt; our preference for an accusatorial rather than an inquisitorial system of criminal justice; our fear that self-incriminating ****2349** statements will be elicited by inhumane treatment and abuses; our sense of fair play which dictates 'a fair state-individual balance by requiring the government to leave the individual alone until good cause is shown for disturbing him and by requiring the government in its contest with the individual to shoulder the entire load,' ...; our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life,' y(3)27; ***213** our distrust of self-deprecatory statements; and our realization that the privilege, while sometimes 'a shelter to the guilty,' is often 'a protection to the innocent.' " *Id.,* at 55, 84 S.Ct., at 1596–1597 (citations omitted).

These policies are served when the privilege is asserted to spare the accused from having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share his thoughts and beliefs with the Government. [11]

We are not persuaded by petitioner's arguments that our articulation of the privilege fundamentally alters the power of the Government to compel an accused to assist in his prosecution. There are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts. The vast majority of verbal statements thus will be testimonial and, to that extent at least, will fall within ***214** the privilege. [12] Furthermore, it should be remembered that there are many restrictions on the government's prosecutorial practices in addition to the Self–Incrimination Clause. Indeed, there are other protections against governmental efforts to compel an unwilling suspect to cooperate in an investigation, including efforts to obtain ****2350** information from him. [13] We are confident that these provisions, together with the Self–Incrimination Clause, will continue to prevent abusive investigative techniques.

B

[8] The difficult question whether a compelled communication is testimonial for purposes of applying the Fifth Amendment often depends on the facts and circumstances of the particular ***215** case. *Fisher,* 425 U.S., at 410, 96 S.Ct., at 1581. This case is no exception. We turn, then, to consider whether Doe's execution of the consent directive at issue here would have testimonial significance. We agree with the Court of Appeals that it would not, because neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information to the Government.

The consent directive itself is not "testimonial." It is carefully drafted not to make reference to a specific account, but only to speak in the hypothetical. Thus, the form does not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner. Nor does the form indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist. Cf. *United States v. Ghidoni,* 732 F.2d, at 818; *In re Grand Jury Proceedings (Ranauro),* 814 F.2d 791, 793 (CA1 1987); *In re United States Grand Jury Subpoena,* 826 F.2d 1166, 1170 (CA2 1987), cert. pending, No. 87–517; *In re Grand Jury Proceedings (Cid),* 767 F.2d, at 1132. The form does not even identify the relevant bank. Although the executed form allows the Government access to a potential source of evidence, the directive itself does not point the Government toward hidden accounts or otherwise provide information that will assist the prosecution in uncovering evidence. The Government must locate that evidence " 'by the independent labor of its officers,' " *Estelle v. Smith,* 451 U.S. 454, 462, 101 S.Ct. 1866, 1872, 68 L.Ed.2d 359 (1981), quoting *Culombe v. Connecticut,* 367 U.S. 568, 582, 81 S.Ct. 1860, 1867, 6 L.Ed.2d 1037 (1961) (opinion announcing the judgment). As in *Fisher,* the Government is not relying upon the " 'truthtelling' " of Doe's directive to show the existence of, or his control over, foreign bank account records. See 425 U.S., at 411, 96 S.Ct. at 1581, quoting 8 Wigmore § 2264, p. 380.

Given the consent directive's phraseology, petitioner's compelled act of executing the form has no testimonial significance either. By signing the form, Doe makes no statement, ***216** explicit or implicit, regarding the existence of a foreign bank account or his control over any such account. Nor would his execution of the form admit the authenticity of any records produced by the bank. Cf. *United States v. Ghidoni,* 732 F.2d, at 818–819; *In re Grand Jury Subpoena,* 826 F.2d, at 1170. Not only does the directive express no view on the issue, but because petitioner did not prepare the document, any statement by Doe to the effect that it is authentic would not establish that the records are genuine. Cf. *Fisher,* 425 U.S., at 413, 96 S.Ct., at 1582. Authentication evidence would have to be provided by bank officials.

Finally, we cannot agree with petitioner's contention that his execution of the directive admits or asserts Doe's consent. The form does not state that Doe "consents" to the release of bank records. Instead, it states that the directive "shall be ****2351** construed as consent" with respect to Cayman Islands and Bermuda bank-secrecy laws. Because the directive explicitly indicates that it was signed pursuant to a court order, Doe's compelled execution of the form sheds no light on his actual intent or state of mind. [14] The form does "direct" the ***217** bank to disclose account information and release any records that "may" exist and for which Doe "may" be a relevant principal. But directing the recipient of a communication to do something is not an assertion of fact or, at least in this context, a disclosure of information. In its testimonial significance, the execution of such a directive is analogous to the production of a handwriting sample or voice exemplar: it is a nontestimonial act. In neither case is the suspect's action compelled to obtain "any knowledge he might have." *Wade,* 388 U.S., at 222, 87 S.Ct., at 1930. [15]

We read the directive as equivalent to a statement by Doe that, although he expresses no opinion about the existence ***218** of, or his control over, any such account, he is authorizing the bank to disclose information relating to accounts over which, in the bank's opinion, Doe can exercise the right of withdrawal. Cf. *Ghidoni,* 732 F.2d, at 818, n. 8 (similarly interpreting a nearly identical consent directive). When forwarded to the bank along with a subpoena, the executed directive, if effective under local law, [16] will simply make it possible ****2352** for the recipient bank to comply

with the Government's request to produce such records. As a result, if the Government obtains bank records after Doe signs the directive, the only factual statement made by anyone will be the *bank's* implicit declaration, by its act of production in response to the subpoena, that *it* believes the accounts to be petitioner's. Cf. *Fisher,* 425 U.S., at 410, 412–413, 96 S.Ct., at 1581–1582. The fact that the bank's customer has directed the disclosure of his records "would say nothing about the correctness of the bank's representations." Brief for United States 21–22. Indeed, the Second and Eleventh Circuits have concluded that consent directives virtually identical to the one here are inadmissible as an admission by the signator of either control or existence. *In re Grand Jury Subpoena,* 826 F.2d, at 1171; *Ghidoni,* 732 F.2d, at 818, and n. 9.

***219** III

Because the consent directive is not testimonial in nature, we conclude that the District Court's order compelling petitioner to sign the directive does not violate his Fifth Amendment privilege against self-incrimination. Accordingly, the judgment of the Court of Appeals is affirmed.

It is so ordered.

Justice STEVENS, dissenting.

A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe —by word or deed.

The document the Government seeks to extract from John Doe purports to order third parties to take action that will lead to the discovery of incriminating evidence. The directive itself may not betray any knowledge petitioner may have about the circumstances of the offenses being investigated by the grand jury, but it nevertheless purports to evidence a reasoned decision by Doe to authorize action by others. The forced execution of this document differs from the forced production of physical evidence just as human beings differ from other animals. [1]

***220** If John Doe can be compelled to use his mind to assist the Government in developing ****2353** its case, I think he will be forced "to be a witness against himself." The fundamental purpose of the Fifth Amendment was to mark the line between the kind of inquisition conducted by the Star Chamber and what we proudly describe as our accusatorial system of justice. It ***221** reflects "our respect for the inviolability of the human personality," *Murphy v. Waterfront Comm'n of New York Harbor,* 378 U.S. 52, 55, 84 S.Ct. 1594, 1597, 12 L.Ed.2d 678 (1964). "[I]t is an explicit right of a natural person, protecting the realm of human thought and expression." *Braswell v. United States,* 487 U.S., at 119, 108 S.Ct., at 2286 (KENNEDY, J., dissenting) [slip op. at 1]. In my opinion that protection gives John Doe the right to refuse to sign the directive authorizing access to the records of any bank account that he may control. [2] Accordingly, I respectfully dissent.

All Citations

487 U.S. 201, 108 S.Ct. 2341, 101 L.Ed.2d 184, 62 A.F.T.R.2d 88-5744, 56 USLW 4708, 88-2 USTC P 9545, 25 Fed. R. Evid. Serv. 632

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See *United States v. Detroit Lumber Co.,* 200 U.S. 321, 337, 26 S.Ct. 282, 287, 50 L.Ed. 499.

1 It is a criminal offense for a Cayman bank to divulge any confidential information with respect to a customer's account unless the customer has consented to the disclosure. See the 1976 Confidential Relationships (Preservation) Law No. 16, as amended, 1979 CAY. IS. LAWS, ch. 26, §§ 3, 4 (Cayman Islands bank-secrecy law).

Apparently, Bermuda common law has been interpreted as imposing an implied contract of confidentiality between a Bermuda bank and its customers, pursuant to which "no Bermuda bank may release information in its possession concerning its customers' affairs unless (1) it is ordered to do so by a court of competent jurisdiction in Bermuda, or (2) it receives a specific written direction from its customer requesting the bank to release such information." Letter dated August 1, 1984, from Richard A. Bradspies, Vice President–Operations, of the Bank of Bermuda International Ltd., to David Geneson, Esq., Fraud Section, Criminal Division, U.S. Dept. of Justice, Respondent's Exhibit 4; Respondent's Notice of Disclosure of 6(e) Materials, 2 Record 307.

The Government has not yet sought contempt sanctions against the banks.

2 The revised consent form reads:

"I, _____, of the State of Texas in the United States of America, do hereby direct any bank or trust company at which I may have a bank account of any kind or at which a corporation has a bank account of any kind upon which I am authorized to draw, and its officers, employees and agents, to disclose all information and deliver copies of all documents of every nature in your possession or control which relate to said bank account to Grand Jury 84–2, empaneled May 7, 1984 and sitting in the Southern District of Texas, or to any attorney of the District of Texas, or to any attorney of the United States Department of Justice assisting said Grand Jury, and to give evidence relevant thereto, in the investigation conducted by Grand Jury 84–2 in the Southern District of Texas, and this shall be irrevocable authority for so doing. This direction has been executed pursuant to that certain order of the United States District Court for the Southern District of Texas issued in connection with the aforesaid investigation, dated _____. This direction is intended to apply to the Confidential Relationships (Preservation) Law of the Cayman Islands, and to any implied contract of confidentiality between Bermuda banks and their customers which may be imposed by Bermuda common law, and shall be construed as consent with respect thereto as the same shall apply to any of the bank accounts for which I may be a relevant principal." App. to Pet. for Cert. 12a, n. 5.

3 The Court of Appeals, citing *United States v. New York Telephone Co.,* 434 U.S. 159, 174, 98 S.Ct. 364, 373, 54 L.Ed.2d 376 (1977), held that the All Writs Act, 28 U.S.C. § 1651(a), authorized the District Court to consider the Government's motion to compel Doe's execution of the consent form, since that compulsion would facilitate the enforcement of the grand jury subpoenas served on the banks. App. to Pet. for Cert. 6a–7a. Petitioner has not challenged the Court of Appeals' conclusion regarding the District Court's authority for entering its order, and we do not address that issue here.

4 The Second and Eleventh Circuits, as did the Fifth, have held that the Fifth Amendment is not implicated by a court order compelling consent to the disclosure of foreign bank records. *United States v. Ghidoni,* 732 F.2d 814 (CA11), cert. denied, 469 U.S. 932, 105 S.Ct. 328, 83 L.Ed.2d 264 (1984); *United States v. Davis,* 767 F.2d 1025, 1039–1040 (CA2 1985); accord, *In re Grand Jury Subpoena,* 826 F.2d 1166 (CA2 1987), cert. pending, No. 87–517 *sub nom. Coe v. United States.* A divided panel of the First Circuit, however, has held that such an order violates the Fifth Amendment. *In re Grand Jury Proceedings (Ranauro),* 814 F.2d 791 (1987).

5 As noted above, the District Court concluded that the consent directive was incriminating in that it would furnish the Government with a link in the chain of evidence leading to Doe's indictment. Because we ultimately find no testimonial significance in either the contents of the directive or Doe's execution of it, we need not, and do not, address the incrimination element of the privilege.

6 Petitioner's blanket assertion that a statement is testimonial for Fifth Amendment purposes if its content can be used to obtain evidence confuses the requirement that the compelled communication be "testimonial" with the separate requirement that the communication be "incriminating." If a compelled statement is "not ***209** testimonial and for that reason not protected by the privilege, it cannot become so because it will lead to incriminating evidence." *In re Grand Jury Subpoena,* 826 F.2d, at 1172, n. 2 (concurring opinion).

Petitioner's heavy reliance on this Court's decision in *Kastigar v. United States,* 406 U.S. 441, 92 S.Ct. 1653, 32 L.Ed.2d 212 (1972), for a contrary proposition is misguided. *Kastigar* affirmed the constitutionality of 18 U.S.C. §§ 6002 and 6003, which permit the Government to compel testimony as long as the witness is immunized against the use in any criminal case of the "testimony or other information" provided. In holding that the immunity provided by the statute is coextensive with the Fifth Amendment privilege, the Court implicitly concluded that the privilege prohibits "the use of compelled testimony, as well as evidence derived directly and indirectly therefrom." 406 U.S., at 453, 92 S.Ct., at 1661. The prohibition of derivative use is an implementation of the "link in the chain of evidence" theory for invocation of the privilege, pursuant to which the "compelled testimony" need not itself be incriminating if it would lead to the discovery of incriminating evidence. See *Hoffman v. United States,* 341 U.S. 479, 486, 71 S.Ct. 814, 818, 95 L.Ed. 1118 (1951). See also *Murphy v. Waterfront Comm'n of New York Harbor,* 378 U.S. 52, 79, 84 S.Ct. 1594, 1609, 12 L.Ed.2d 678 (1964); 8 J. Wigmore, Evidence § 2260 (McNaughton rev. 1961) (Wigmore). This prohibition, however, assumes that the suspect's initial compelled communication is testimonial.

7 See *In re United States Grand Jury Proceedings (Cid),* 767 F.2d 1131, 1132 (CA5 1985); *In re Grand Jury Proceedings (Ranauro),* 814 F.2d, at 793; *id.,* at 798 (dissenting opinion); *United States v. Davis,* 767 F.2d, at 1040. See also *United States v. Ghidoni,* 732 F.2d, at 816.

8 The decisions in *Fisher v. United States,* 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976), and *United States v. Doe,* 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552 (1984), rested on the understanding that " 'the Court has never on any ground ... applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which, in the Court's view, did not involve compelled testimonial self-incrimination of some sort.' " *Id.,* at 611, n. 8, 104 S.Ct., at 1241 n. 8, quoting *Fisher,* 425 U.S., at 399, 96 S.Ct. at 1575. The Court thus squarely held that the Fifth Amendment comes into play "only when the accused is compelled to make a *testimonial* communication that is incriminating." *Id.,* at 408, 96 S.Ct., at 1579 (emphasis in original); see *id.,* at 409, 96 S.Ct. at 1580; *Doe,* 465 U.S., at 611, 613, 104 S.Ct., at 1241, 1242. These principles were articulated in general terms, not as confined to acts. Petitioner has articulated no cogent argument as to why the "testimonial" requirement should have one meaning in the context of acts, and another meaning in the context of verbal statements.

9 We do not disagree with the dissent that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Post,* at 2352, n. 1. We simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. In our view, such compulsion is more like "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it is like "be[ing] compelled to reveal the combination to [petitioner's] wall safe." *Post,* at 2352.

10 Petitioner's reliance on a statement in this Court's decision in *Schmerber v. California,* 384 U.S. 757, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966), for the proposition that all verbal statements sought for their content are testimonial is misplaced. In *Schmerber,* the Court stated that the privilege extends to "an accused's communications, whatever form they might take," *id.,* at 763–764, 86 S.Ct., at 1832, but it did so in the context of clarifying that the privilege may apply not only to verbal communications, as was once thought, but also to physical communications. See *United States v. Wade,* 388 U.S. 218, 223, 87 S.Ct. 1926, 1930, 18 L.Ed.2d 1149 (1967). Contrary to petitioner's urging, the *Schmerber* line of cases does not draw a distinction between unprotected evidence sought for its physical characteristics and protected evidence sought for its content. Rather, the Court distinguished between the suspect's being compelled himself to serve as evidence and the suspect's being compelled to disclose or communicate information or facts that might serve as or lead to incriminating evidence. See, *e.g., Schmerber,* 384 U.S., at 764, 87 S.Ct., at 1832. See also *Holt v. United States,* 218 U.S. 245, 252–253, 31 S.Ct. 2, 6, 54 L.Ed. 1021 (1910); 8 Wigmore § 2265, p. 386. In order to be privileged, it is not enough that the compelled communication is sought for its content. The content itself must have testimonial significance. *Fisher,* 425 U.S., at 408, 96 S.Ct., at 1579; *Gilbert v. California,* 388 U.S. 263, 267, 87 S.Ct. 1951, 1953, 18 L.Ed.2d 1178 (1967); *Wade,* 388 U.S., at 222, 87 S.Ct., at 1929.

11 Petitioner argues that at least some of these policies would be undermined unless the Government is required to obtain evidence against an accused from sources other than his compelled statements, whether or not the statements make a factual assertion or convey information. Petitioner accordingly maintains that the policy of striking an appropriate balance between the power of the Government and the sovereignty of the individual precludes the Government from compelling an individual to utter or write words that lead to incriminating evidence. Even if some of the policies underlying the privilege might support petitioner's interpretation of the privilege, "it is clear that the scope of the privilege does not coincide with the complex of values it helps to protect. Despite the impact upon the inviolability of the human personality, and upon our belief in an adversary system of criminal justice in which the Government must produce the evidence against an accused through its own independent labors, the prosecution is allowed to obtain and use ... evidence which although compelled is generally speaking not 'testimonial,' *Schmerber v. California,* 384 U.S. 757, 761 [86 S.Ct., at 1830]." *Grosso v. United States,* 390 U.S. 62, 72–73, 88 S.Ct. 709, 715–716, 19 L.Ed.2d 906 (1968) (BRENNAN, J., concurring). See also *Schmerber,* 384 U.S., at 762–763, 86 S.Ct., at 1831. If the societal interests in privacy, fairness, and restraint of governmental power are not unconstitutionally offended by compelling the accused to have his body serve as evidence that leads to the development of highly incriminating testimony, as *Schmerber* and its progeny make clear, it is difficult to understand how compelling a suspect to make a nonfactual statement that facilitates the production of evidence by someone else offends the privilege.

12 In particular, we do not agree that our articulation cuts back on the Court's explanation in *Miranda v. Arizona,* 384 U.S. 436, 86 S.Ct. 1602, 16 L.Ed.2d 694 (1966), that "the privilege is fulfilled only when the person is guaranteed the right 'to remain silent unless he chooses to speak in the unfettered exercise of his own will.' " *Id.,* at 460, 86 S.Ct., at 1620, quoting *Malloy v. Hogan,* 378 U.S. 1, 8, 84 S.Ct. 1489, 1493, 12 L.Ed.2d 653 (1964). In *Miranda,* the Court addressed a suspect's Fifth Amendment privilege in the face of custodial interrogation by the Government. Our test for when a communication is "testimonial" does not authorize law enforcement officials to make an unwilling suspect speak in this context. It is clear that the accused in a criminal case is exempt from giving answers altogether, for (at least on the prosecution's assumption) they will disclose incriminating information that the suspect harbors.

To the extent petitioner attempts to construe *Miranda* as establishing an absolute right against being compelled to speak, that understanding is refuted by the Court's decision in *United States v. Dionisio,* 410 U.S. 1, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973), in which the Court held that a suspect may not invoke the privilege in refusing to speak for purposes of providing a voice exemplar.

13 For example, the Fourth Amendment generally prevents the government from compelling a suspect to consent to a search of his home, cf. *Schneckloth v. Bustamonte,* 412 U.S. 218, 248–249, 93 S.Ct. 2041, 2058–2059, 36 L.Ed.2d 854 (1973); the attorney-client privilege prevents the Government from compelling a suspect to direct his attorney to disclose confidential communications, see generally *Upjohn Co. v. United States,* 449 U.S. 383, 389, 101 S.Ct. 677, 682, 66 L.Ed.2d 584 (1981); 8 Wigmore § 2292; and the Due Process Clause imposes limitations on the government's ability to coerce individuals into participating in criminal prosecutions, see generally *Rochin v. California,* 342 U.S. 165, 174, 72 S.Ct. 205, 210, 96 L.Ed. 183 (1952).

14 The consent directive at issue here differs from the form at issue in *Ranauro* which suggested that the witness, in fact, had consented: "I, [witness], consent to the production to the [District Court and Grand Jury] of any and all records related to any accounts held by, or banking transactions engaged in with, [bank X], which are in the name of, or on behalf of: [witness], if any such records exist." 814 F.2d, at 796. Further, the *Ranauro* form, unlike the directive here, did not indicate that it was executed under court order. *Id.,* at 795. It is true that the First Circuit made clear that its conclusion that the *Ranauro* form was testimonial did not turn on these distinctions, *ibid.,* but we are not sanguine that the differences are irrelevant. Even if the Self–Incrimination Clause was not implicated, it might be argued that the compelled signing of such a "consent" form raises due process concerns. Cf. *In re Grand Jury Subpoena,* 826 F.2d, at 1171 (finding no due process violation where directive clearly states that witness is signing under compulsion of court order); *United States v. Ghidoni,* 732 F.2d, at 818, n. 7 (same). Neither issue, of course, is presented by this case, and we take no position on whether such compulsion in fact would violate Fifth Amendment or due process principles.

15 Petitioner apparently maintains that the performance of every compelled act carries with it an implied assertion that the act has been performed by the person who was compelled, and therefore the performance of the act is subject to the privilege. In *Wade, Gilbert,* and *Dionisio,* the Court implicitly rejected this argument. It could be said in those cases that the suspect, by providing his handwriting or voice exemplar, implicitly "acknowledged" that the writing or voice sample was his. But as the holdings make clear, this kind of simple acknowledgment—that the suspect in fact performed the compelled act—is not "sufficiently testimonial for purposes of the privilege." *Fisher,* 425 U.S., at 411, 96 S.Ct., at 1581. Similarly, the acknowledgment that Doe directed the bank to disclose any records the bank thinks are Doe's—an acknowledgment implicit in Doe's placing his signature on the consent directive—is not sufficiently testimonial for purposes of the privilege.

The dissent apparently disagrees with us on this point, although the basis for its disagreement is unclear. See *post,* at 2353–2354, n. 2. Surely, the fact that the executed form creates "a new piece of evidence that may be used against petitioner" is not relevant to whether the execution has testimonial significance, for the same could be said about the voice and writing exemplars the Court found were not testimonial in nature. Similarly irrelevant to the issue presented here is the dissent's invocation of the First Circuit's hypothetical of how the Government might use the directive to link petitioner to whatever documents the banks produce. That hypothetical, as the First Circuit indicated, *Ranauro,* 814 F.2d, at 793, goes only

to showing that the directive may be *incriminating,* an issue not presented in this case. See n. 5, *supra.* It has no bearing on whether the compelled execution of the directive is *testimonial.*

16 The Government of the Cayman Islands maintains that a compelled consent, such as the one at issue in this case, is not sufficient to authorize the release of confidential financial records protected by Cayman law. Brief for Government of Cayman Islands as *Amicus Curiae* 9–11. The Grand Court of the Cayman Islands has held expressly that a consent directive signed pursuant to an order of a United States court and at the risk of contempt sanctions, could not constitute "consent" under the Cayman confidentiality law. See *In re ABC Ltd.,* 1984 C.I.L.R. 130 (1984) (reviewing the consent directive at issue in *Ghidoni*). The United States observes that the cited decision has not been appealed and argues accordingly that Cayman law on the point has not been definitely settled.

The effectiveness of the directive under foreign law has no bearing on the constitutional issue in this case. Nevertheless, we are not unaware of the international comity questions implicated by the Government's attempts to overcome protections afforded by the laws of another nation. We are not called upon to address those questions here.

1 The forced production of physical evidence, which we have condoned, see *Gilbert v. California,* 388 U.S. 263, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967) (handwriting exemplar); *United States v. Wade,* 388 U.S. 218, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967) (voice exemplar); *Schmerber v. California,* 384 U.S. 757, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1966) (blood test); *Holt v. United States,* 218 U.S. 245, 31 S.Ct. 2, 54 L.Ed. 1021 (1910) (lineup), involves no intrusion upon the contents of the mind of the accused. See *Schmerber,* 384 U.S., at 765, 86 S.Ct., at 1832 (forced blood test permissible because it does not involve "even a shadow of testimonial compulsion upon or enforced communication by the accused"). The forced execution of a document that purports to convey the signer's authority, however, does invade the dignity of the human mind; it purports to communicate a deliberate command. The intrusion on the dignity of the individual is not diminished by the fact that the document does not reflect the true state of the signer's mind. Indeed, that the assertions petitioner is forced to utter by executing the document are false, causes an even greater violation of human dignity. For the same reason a person cannot be forced to sign a document purporting to authorize the entry of judgment against himself, cf. *Brady v. United States,* 397 U.S. 742, 748, 90 S.Ct. 1463, 25 L.Ed.2d 747 (1970), I do not believe he can be forced to sign a document purporting to authorize the disclosure of incriminating evidence. In both cases the accused is being compelled "to be a witness against himself"; indeed, here he is being compelled to bear false witness against himself.

The expression of the contents of an individual's mind falls squarely within the protection of the Fifth Amendment. *Boyd v. United States,* 116 U.S. 616, 633–635, 6 S.Ct. 524, 533–535, 29 L.Ed. 746 (1886); *Fisher v. United States,* 425 U.S. 391, 420, 96 S.Ct. 1569, 1585, 48 L.Ed.2d 39 (1976). Justice Holmes' observation that "the prohibition of compelling a man in a criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him," *Holt v. United States,* 218 U.S., at 252–253, 31 S.Ct., at 6, manifests a recognition that virtually any communication reveals the contents of the mind of the speaker. Thus the Fifth Amendment privilege is fulfilled only when the person is guaranteed the right " 'to remain silent unless he chooses to speak in the unfettered exercise of his own will.' " *Miranda v. Arizona,* 384 U.S. 436, 460, 86 S.Ct. 1602, 1620, 16 L.Ed.2d 694 (1966) (quoting *Malloy v. Hogan,* 378 U.S. 1, 8, 84 S.Ct. 1489, 1493, 12 L.Ed.2d 653 (1964)). The deviation from this principle can only lead to mischievous abuse of the dignity the Fifth Amendment commands the Government afford its citizens. Cf. *Schmerber v. California,* 384 U.S., at 764, 86 S.Ct., at 1832. The instant case is illustrative. In allowing the Government to compel petitioner to execute the directive, the

Court permits the Government to compel petitioner to speak against his will in answer to the question "Do you consent to the release of these documents?" Beyond this affront, however, the Government is being permitted also to demand that the answer be "yes."

2 The Fifth Amendment provides that no person "shall be compelled in any criminal case to be a *witness* against himself." A witness is one who "gives evidence in a cause." T. Cunningham, 2 New and Complete Law Dictionary (2d ed. 1771). The Court carefully scrutinizes the particular directive at issue here to determine whether its "form" or "execution" "communicates any factual assertions, implicit or explicit, or conveys any information to the Government." *Ante,* at 2350. But the Court's opinion errs in focusing only on whether the directive reveals historical facts, ignoring that the execution of the directive *creates new* facts and a new piece of evidence that may be used against petitioner. The Court determines that the document's form has no testimonial significance because it does not reveal the identity of any particular banks or acknowledge the existence of any particular foreign accounts. This much is true. But the document does reveal exactly what it purports to reveal, which is that petitioner "directs," see *ante,* at ——, n. 2, the release of any documents that conform to the description contained in the statement. Thus, by executing the document, petitioner admits a state of mind, a present-tense desire. That the directive asserts that it was executed "pursuant to" court order does not save petitioner from this compelled admission. Only the most sophisticated bank officer could be expected to understand the phrase "pursuant to that certain order," *ibid.,* to mean "executed involuntarily under pain of contempt." But even if the directive expressly revealed its involuntary character, it would still communicate the direction that incriminating documents be produced.

By executing the document, petitioner creates evidence that has independent significance. The Court's opinion does not foreclose the possibility that the Government will attempt to introduce the directive itself to create a link between petitioner and whatever documents the Government is able to secure through use of the directive. This danger was fully described in an example employed by the First Circuit in its analysis of a document, which, like the one at issue here, did not assert the existence of any particular bank records or accounts:

"Suppose that at trial the government were to introduce bank records produced in response to a subpoena that had been accompanied by the consent form and that it was not apparent from the face of the records or otherwise how [defendant] was linked to them. Suppose also that the government then introduced the subpoena and consent form, and a government witness testified that the bank records were received in response to the subpoena and consent form.... Would not the evidence linking [defendant] to the records be his own testimonial admission of consent?" *In re Grand Jury Proceedings (Ranauro),* 814 F.2d 791, 793 (1987).

The example reveals that the compelled execution causes the creation of evidence that did not exist before and which through the Government's artifice may become part of the prosecution's case against petitioner. The example also demonstrates that the "testimonial" significance of the directive can only be appreciated if the document is considered in its completed form from the perspective of an individual who knows no more about the circumstances of its creation than is revealed on its face. The fact that the document was produced under compulsion, which the Court relies on in asserting that the directive "sheds no light on [petitioner's] actual intent or state of mind," *ante,* at ——, is not relevant to consideration of the document's testimonial significance.

A critical issue at any trial at which the Government seeks to introduce bank records produced by a compulsory directive would be proof that the documents pertain to accounts within the control of the defendant. The directive relates the testimonial fact that the defendant ordered the production of those documents which relate to any account he has at a bank or trust company or over which he has signatory authority. Perhaps this testimony alone does not prove the fact of control, but it is certainly probative of

that fact. The defendant can no longer testify without contradiction from the face of the directive that he never authorized the production of records relating to his accounts. The directive that he was compelled to create testifies against him.

End of Document

KeyCite Yellow Flag - Negative Treatment
Disagreement Recognized by Litigation Guideline Memorandum, IRS LGM, August 1, 1994

96 S.Ct. 1569
Supreme Court of the United States

Solomon FISHER et al., Petitioners,
v.
UNITED STATES et al.
UNITED STATES et al., Petitioners,
v.
C. D. KASMIR and Jerry A. Candy.

Nos. 74-18, 74-611.
|
Argued Nov. 3, 1975.
|
Decided April 21, 1976.

Synopsis

In two cases, enforcement actions were commenced by Government to compel production of accountants' documents in possession of taxpayers' attorneys. In one case, the United States District Court for the Northern District of Texas granted enforcement and the Court of Appeals for the Fifth Circuit reversed the enforcement order, 499 F.2d 444. In a second case, the District Court for the Eastern District of Pennsylvania granted enforcement, 352 F.Supp. 731, and the Court of Appeals for the Third Circuit affirmed, 500 F.2d 683. Certiorari was granted to resolve the conflict created. The Supreme Court, Mr. Justice White, held that taxpayers' Fifth Amendment privilege was not violated by enforcement of documentary summons directed toward their attorneys, for production of accountants' documents which had been transferred to attorneys in connection with an Internal Revenue Service investigation, whether or not the Amendment would have barred a subpoena directing taxpayers to produce documents while they were in taxpayers' hands, and fact that attorneys were agents of taxpayers did not change result; and that compliance with a summons directing taxpayers to produce accountants' documents, which were not taxpayers' "private papers," would involve no incriminating testimony within protection of Fifth Amendment, and thus such documents were not, under theory of attorney-client privilege, immune from production in hands of taxpayers' attorneys to whom they had been transferred in connection with Internal Revenue Service investigation.

Judgment of Court of Appeals for Fifth Circuit in No. 74-611 reversed; judgment of Court of Appeals for Third Circuit in No. 74-18 affirmed.

Mr. Justice Brennan concurred in the judgment and filed an opinion.

Mr. Justice Marshall concurred in the judgment and filed an opinion.

West Headnotes (15)

[1] **Witnesses** Privilege as to production of documents

Enforcement of a summons to produce documents against a taxpayer's lawyer would not "compel" taxpayer to do anything and would not compel him to be a "witness" against himself within Fifth Amendment; taxpayers' personal privilege against self-incrimination was in no way decreased by transfer of documents to their attorneys, and taxpayers retained any privilege they had. U.S.C.A.Const. Amend. 5.

83 Cases that cite this headnote

[2] **Criminal Law** Compelling Self-Incrimination

Fifth Amendment is limited to prohibiting the use of physical or moral compulsion exerted on the person asserting the privilege. U.S.C.A.Const. Amend. 5.

88 Cases that cite this headnote

[3] **Witnesses** Privilege as to production of documents

Taxpayers' Fifth Amendment privilege was not violated by enforcement of documentary summonses directed toward their attorneys for

production of accountants' documents which had been transferred to attorneys in connection with an Internal Revenue Service investigation, whether or not the Amendment would have barred a subpoena directing taxpayers to produce documents while they were in taxpayers' hands, and fact that attorneys were agents of taxpayers did not change result, where constructive possession by taxpayers was not so clear nor relinquishment of possession so temporary and insignificant as to leave personal compulsion on taxpayers substantially intact. U.S.C.A.Const. Amend. 5.

154 Cases that cite this headnote

[4] **Criminal Law** Private persons in general

Under appropriate safeguards, private incriminating statements of an accused may be overheard and used in evidence, if they are not compelled at the time they were uttered.

11 Cases that cite this headnote

[5] **Criminal Law** Compelling Self-Incrimination

Disclosure of private information may be compelled if immunity removes the risk of incrimination. U.S.C.A.Const. Amend. 5.

12 Cases that cite this headnote

[6] **Criminal Law** Compelling Self-Incrimination

The Fifth Amendment's strictures, unlike the Fourth's, are not removed by showing reasonableness. U.S.C.A.Const. Amends. 4, 5.

9 Cases that cite this headnote

[7] **Witnesses** Self-Incrimination

Fifth Amendment protects against compelled self-incrimination, not the disclosure of private information. U.S.C.A.Const. Amend. 5.

194 Cases that cite this headnote

[8] **Witnesses** Privilege as to production of documents

Enforcement of documentary subpoenas directed to taxpayers' attorneys for production of accountants' documents delivered to attorneys by taxpayers was not precluded on theory that attorneys were required to respect confidences of clients who had a reasonable expectation of privacy for records in hands of attorneys and therefore did not forfeit Fifth Amendment privilege with respect to records by transferring them in order to obtain legal advice. U.S.C.A.Const. Amend. 5.

171 Cases that cite this headnote

[9] **Privileged Communications and Confidentiality** Persons entitled to assert privilege

The attorney-client privilege may be raised by the attorney.

604 Cases that cite this headnote

[10] **Privileged Communications and Confidentiality** Elements in general; definition

Privileged Communications and Confidentiality Purpose of privilege

Confidential disclosures by client to an attorney made in order to obtain legal assistance are privileged; the purpose of the privilege is to encourage clients to make full disclosure to their attorneys; however, privilege protects only those disclosures, necessary to obtain informed legal advice, which might not have been obtained absent the privilege.

946 Cases that cite this headnote

[11] **Privileged Communications and Confidentiality** Documents and records in general

Where taxpayer transferred possession of documents from himself to his attorney, in order to obtain legal assistance in tax investigations, the papers, if unobtainable by summons from the client, were unobtainable by summons directed to the attorney by reason of the attorney-client privilege.

454 Cases that cite this headnote

[12] **Criminal Law** Compelling Self-Incrimination

Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating. U.S.C.A.Const. Amend. 5.

274 Cases that cite this headnote

[13] **Witnesses** Privilege as to production of documents

Fifth Amendment privilege protects a person only against being incriminated by his own compelled testimonial communications, as opposed to compelled production of incriminating documents, even where document was written by person asserting the privilege, if he was not compelled to write it. U.S.C.A.Const. Amend. 5.

368 Cases that cite this headnote

[14] **Witnesses** Privilege as to production of documents

However incriminating the contents of accountants' work papers might be, the act of producing them, the only thing which taxpayers were compelled to do, would not itself involve testimonial self-incrimination. U.S.C.A.Const. Amend. 5.

396 Cases that cite this headnote

[15] **Privileged Communications and Confidentiality** Accountants and auditors

Compliance with a summons directing taxpayers to produce accountants' documents, which were not taxpayers' "private papers," would involve no incriminating testimony within protection of Fifth Amendment, and thus such documents were not, under theory of attorney-client privilege, immune from production in hands of taxpayers' attorneys to whom they had been transferred in connection with Internal Revenue Service investigation. U.S.C.A.Const. Amend. 5.

539 Cases that cite this headnote

****1571** Syllabus [*]

***391** In each of these cases taxpayers, who were under investigation for possible civil or criminal liability under the federal income tax laws, after having obtained from their respective accountants certain documents relating to the accountants' preparation of their tax returns, transferred the documents to their respective attorneys to assist the taxpayers in connection with the investigations. Subsequently, the Internal Revenue Service served summonses on the attorneys directing them to produce the documents, but the attorneys refused to comply. The Government then brought enforcement actions, and in each case the District Court ordered the summons enforced. In No. 74-18 the Court of Appeals affirmed, holding that the taxpayers had never acquired a possessory interest in the documents and that the documents were not immune from production in the attorney's hands. But in No. 74-611 the Court of Appeals reversed, holding that by virtue of the Fifth Amendment the documents would have been privileged from production pursuant to a summons directed to the taxpayer if he had retained possession, and that, in light of the attorney-client relationship, the taxpayer retained such privilege after transferring the documents to his attorney. Held :

1. Compelled production of the documents in question from the attorneys does not implicate whatever Fifth Amendment privilege the taxpayer-clients might have enjoyed from being themselves compelled to produce the documents. Pp. 1573-1576.

(a) Whether or not the Fifth Amendment would have barred a subpoena directing the taxpayers to produce the documents while they were in their hands, the taxpayers' privilege under that Amendment is not violated by enforcing the summonses because enforcement against a taxpayer's lawyer would not "compel" the taxpayer to do anything, and certainly would not ***392** compel him to be a "witness" against himself, and the fact that the attorneys are agents of the taxpayers does not change this result. *Couch v. United States*, 409 U.S. 322, 93 S.Ct. 611, 34 L.Ed.2d 548. Pp. 1573-1574.

(b) These cases do not present a situation where constructive possession of the documents in question is so clear or relinquishment of possession so temporary and insignificant as to leave the personal compulsion upon the taxpayer substantially intact, since the documents sought were obtainable without personal compulsion upon the taxpayers. Couch, supra. P. 1574.

****1572** (c) The taxpayers, by transferring the documents to their attorneys, did not lose any Fifth Amendment privilege they ever had not to be compelled to testify against themselves and not to be compelled themselves to produce private papers in their possession, and This personal privilege was in no way decreased by the transfer. Pp. 1574-1575.

(d) Even though the taxpayers, after transferring the documents to their attorneys, may have had a reasonable expectation of privacy with respect to the documents, the Fifth Amendment does not protect private information obtained without compelling self-incriminating testimony. Pp. 1575-1576.

2. Although the attorney-client privilege applies to documents in the hands of an attorney which would have been privileged in the hands of the client by reason of the Fifth Amendment, the taxpayer-clients in these cases would not be protected by that Amendment from producing the documents in question, because production of such documents involves no incriminating testimony and therefore the documents in the hands of the taxpayers' attorneys were not immune from production. Pp. 1576-1582.

(a) The Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial communication that is incriminating. P. 1579.

(b) Here, however incriminating the contents of the accountants' workpapers might be, the act of producing them the only thing that the taxpayers are compelled to do would not itself involve testimonial self-incrimination, and implicitly admitting the existence and possession of the papers does not rise to the level of testimony within the protection of the Fifth Amendment. Pp. 1579-1582.

No. 74-18, 500 F.2d 683, affirmed; No. 74-611, 499 F.2d 444, reversed.

Attorneys and Law Firms

Lawrce G. Wallace, Washington, D. C., for the U. S.

Robert E. Goodfriend for Kasmir et al.

***393** Richard L. Bazelon, Philadelphia, Pa., for Fisher et al.

Opinion

Mr. Justice WHITE delivered the opinion of the Court.

In these two cases we are called upon to decide whether a summons directing an attorney to produce documents delivered to him by his client in connection with the attorney-client relationship is enforceable over claims that the documents were constitutionally immune from summons in the hands of the client and retained that immunity in the hands of the attorney.

I

In each case, an Internal Revenue agent visited the taxpayer or taxpayers [1] and interviewed them in connection ***394** with an investigation of possible civil or criminal liability under the federal income tax laws. Shortly after the interviews one day

later in No. 74-611 and a week or two later in No. 74-18 the taxpayers obtained from their respective accountants certain documents relating to the preparation by the accountants of their tax returns. Shortly after obtaining the documents later the same day in No. 74-611 and a few weeks later in No. 74-18 the taxpayers transferred the documents to their lawyers respondent Kasmir and petitioner Fisher, respectively each of whom was retained to assist the taxpayer in connection with the investigation. Upon learning of the whereabouts of the documents, the Internal Revenue Service served summonses on the attorneys directing them to produce documents listed therein. In No. 74-611, the documents were described as "the following records of Tannebaum Bindler & Lewis (the accounting firm).

**1573 "1. Accountant's workpapers pertaining to Dr. E. J. Mason's books and records of 1969, 1970 and 1971. [2]

"2. Retained copies of E. J. Mason's income tax returns for 1969, 1970 and 1971.
"3. Retained copies of reports and other correspondence between Tannebaum Bindler & Lewis and Dr. E. J. Mason during 1969, 1970 and 1971."

In No. 74-18, the documents demanded were analyses by the accountant of the taxpayers' income and expenses which had been copied by the accountant from the taxpayers' canceled checks and deposit receipts. [3] In No. *395 74-611, summons was also served on the accountant directing him to appear and testify concerning the documents to be produced by the lawyer. In each case, the lawyer declined to comply with the summons directing production of the documents, and enforcement actions were commenced by the Government under 26 U.S.C. ss 7402(b) and 7604(a). In No. 74-611, the attorney raised in defense of the enforcement action the taxpayer's accountant-client privilege, his attorney-client privilege, and his Fourth and Fifth Amendment rights. In No. 74-18, the attorney claimed that enforcement would involve compulsory self-incrimination of the taxpayers in violation of their Fifth Amendment privilege, would involve a seizure of the papers without necessary compliance with the Fourth Amendment, and would violate the taxpayers' right to communicate in confidence with their attorney. In No. 74-18 the taxpayers intervened and made similar claims.

In each case the summons was ordered enforced by the District Court and its order was stayed pending appeal. In No. 74-18, 500 F.2d 683 (CA3 1974), petitioners' appeal raised, in terms, only their Fifth Amendment claim, but they argued in connection with that claim that enforcement of the summons would involve a violation of the taxpayers' reasonable expectation of privacy and particularly so in light of the confidential relationship of attorney to client. The Court of Appeals for the Third Circuit after reargument en banc affirmed the enforcement order, holding that the taxpayers had never acquired a possessory interest in the documents and that the papers were not immune in the hands of the attorney. In No. 74-611, a divided panel of the Court of Appeals for the Fifth Circuit reversed the enforcement order, 499 F.2d 444 (1974). The court reasoned that by virtue of the Fifth Amendment the documents would have been privileged *396 from production pursuant to summons directed to the taxpayer had he retained possession and, in light of the confidential nature of the attorney-client relationship, the taxpayer retained, after the transfer to his attorney, "a legitimate expectation of privacy with regard to the materials he placed in his attorney's custody, that he retained constructive possession of the evidence, and thus . . . retained Fifth Amendment protection." [4] *Id.*, at 453. We granted certiorari to resolve the conflict created. 420 U.S. 906, 95 S.Ct. 824, 42 L.Ed.2d 835 (1975). Because in our view the documents were not privileged either in the hands of the lawyers or of their clients, we affirm the judgment of the Third Circuit in No. 74-18 and reverse the judgment of the Fifth Circuit in No. 74-611.

II

[1] [2] All of the parties in these cases and the Court of Appeals for the Fifth Circuit have concurred in the proposition that if the Fifth Amendment would have excused a Taxpayer from turning over the accountant's papers had he possessed them, **1574 the Attorney to whom they are delivered for the purpose of obtaining legal advice should also be immune from subpoena. Although we agree with this proposition for the reasons set forth in Part III, Infra, we are convinced that, under our decision in Couch v. United States, 409 U.S. 322, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973),

it is not the taxpayer's Fifth Amendment privilege that would excuse the Attorney from production.

The relevant part of that Amendment provides:
"No person . . . shall be Compelled in any criminal case to be a Witness against himself." (Emphasis added.)

***397** The taxpayer's privilege under this Amendment is not violated by enforcement of the summonses involved in these cases because enforcement against a taxpayer's lawyer would not "compel" the taxpayer to do anything and certainly would not compel him to be a "witness" against himself. The Court has held repeatedly that the Fifth Amendment is limited to prohibiting the use of "physical or moral compulsion" exerted on the person asserting the privilege, Perlman v. United States, 247 U.S. 7, 15, 38 S.Ct. 417, 420, 62 L.Ed. 950, 956 (1918); Johnson v. United States, 228 U.S. 457, 458, 33 S.Ct. 572, 57 L.Ed. 919, 920 (1913); Couch v. United States, supra, 409 U.S. 322, at 328, 336, 93 S.Ct. 611, at 615, 619, 34 L.Ed.2d 548, at 554, 558. See also Holt v. United States, 218 U.S. 245, 252-253, 31 S.Ct. 2, 6, 54 L.Ed. 1021, 1030 (1910); United States v. Dionisio, 410 U.S. 1, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973); Schmerber v. California, 384 U.S. 757, 765, 86 S.Ct. 1826, 1832, 16 L.Ed.2d 908, 916 (1966); Burdeau v. McDowell, 256 U.S. 465, 476, 41 S.Ct. 574, 576, 65 L.Ed. 1048, 1051 (1921); California Bankers Assn. v. Shultz, 416 U.S. 21, 55, 94 S.Ct. 1494, 1514, 39 L.Ed.2d 812, 836 (1974). In Couch v. United States, supra, we recently ruled that the Fifth Amendment rights of a taxpayer were not violated by the enforcement of a documentary summons directed to her accountant and requiring production of the taxpayer's own records in the possession of the accountant. We did so on the ground that in such a case "the ingredient of personal compulsion against an accused is lacking." 409 U.S., at 329, 93 S.Ct., at 616, 34 L.Ed.2d, at 554.

[3] Here, the taxpayers are compelled to do no more than was the taxpayer in Couch. The taxpayers' Fifth Amendment privilege is therefore not violated by enforcement of the summonses directed toward their attorneys. This is true whether or not the Amendment would have barred a subpoena directing the taxpayer to produce the documents while they were in his hands.

The fact that the attorneys are agents of the taxpayers does not change this result. Couch held as much, since the accountant there was also the taxpayer's agent, and in this respect reflected a longstanding view. In ***398** hale v. Henkel, 201 U.S. 43, 69-70, 26 S.Ct. 370, 377, 50 L.Ed. 652, 663 (1906), the Court said that the privilege "was never intended to permit (a person) to plead the fact that some third person might be incriminated by his testimony, even though he were the agent of such person . . . . (T)he Amendment is limited to a person who shall be compelled in any criminal case to be a witness against Himself." (Emphasis in original.) "It is extortion of information from the accused himself that offends our sense of justice." Couch v. United States, supra, 409 U.S., at 328, 93 S.Ct., at 616, 34 L.Ed.2d, at 554. Agent or no, the lawyer is not the taxpayer. The taxpayer is the "accused," and nothing is being extorted from him.

Nor is this one of those situations, which Couch suggested might exist, where constructive possession is so clear or relinquishment of possession so temporary and insignificant as to leave the personal compulsion upon the taxpayer substantially intact. 409 U.S., at 333, 93 S.Ct., at 618, 34 L.Ed.2d, at 556. In this respect we see no difference between the delivery to the attorneys in these cases and delivery to the accountant in the Couch case. As was true in Couch, the documents sought were obtainable without personal compulsion on the accused.

****1575** Respondents in No. 74-611 and petitioners in No. 74-18 argue, and the Court of Appeals for the Fifth Circuit apparently agreed, that if the summons was enforced, the taxpayers' Fifth Amendment privilege would be, but should not be, lost solely because they gave their documents to their lawyers in order to obtain legal advice. But this misconceives the nature of the constitutional privilege. The Amendment protects a person from being compelled to be a witness against himself. Here, the taxpayers retained any privilege they ever had not to be compelled to testify against themselves and not to be compelled themselves to produce private papers in their possession. This personal privilege was in no way decreased by the transfer. It is simply that by ***399** reason of the transfer of the documents to the attorneys, those papers

may be subpoenaed without compulsion on the taxpayer. The protection of the Fifth Amendment is therefore not available. "A party is privileged from producing evidence but not from its production." Johnson v. United States, supra, 228 U.S., at 458, 33 S.Ct., at 572, 57 L.Ed., at 920.

The Court of Appeals for the Fifth Circuit suggested that because legally and ethically the attorney was required to respect the confidences of his client, the latter had a reasonable expectation of privacy for the records in the hands of the attorney and therefore did not forfeit his Fifth Amendment privilege with respect to the records by transferring them in order to obtain legal advice. It is true that the Court has often stated that one of the several purposes served by the constitutional privilege against compelled testimonial self-incrimination is that of protecting personal privacy. See, e. g., Murphy v. Waterfront Comm'n, 378 U.S. 52, 55, 84 S.Ct. 1594, 1596, 12 L.Ed.2d 678, 681 (1964); Couch v. United States, supra, 409 U.S. 322, at 332, 335-336, 93 S.Ct. 611, at 617, 619-620, 34 L.Ed.2d 548, at 556, 558-559; Tehan v. United States ex rel. Shott, 382 U.S. 406, 416, 86 S.Ct. 459, 465, 15 L.Ed.2d 453, 460 (1966); Davis v. United States, 328 U.S. 582, 587, 66 S.Ct. 1256, 1258, 90 L.Ed. 1453, 1456 (1946). But the Court has never suggested that every invasion of privacy violates the privilege. Within the limits imposed by the language of the Fifth Amendment, which we necessarily observe, the privilege truly serves privacy interests; but the Court has never on any ground, personal privacy included, applied the Fifth Amendment to prevent the otherwise proper acquisition or use of evidence which, in the Court's view, did not involve compelled testimonial self-incrimination of some sort. [5]

***400** [4] [5] [6] The proposition that the Fifth Amendment protects private information obtained without compelling self-incriminating testimony is contrary to the clear statements of this Court that under appropriate safeguards private incriminating statements of an accused may be overheard and used in evidence, if they are not compelled at the time they were uttered, Katz v. United States, 389 U.S. 347, 354, 88 S.Ct. 507, 512, 19 L.Ed.2d 576, 583 (1967); Osborn v. United States, 385 U.S. 323, 329-330, 87 S.Ct. 429, 432-433, 17 L.Ed.2d 394, 399-400 (1966); and Berger v. New York, 388 U.S. 41, 57, 87 S.Ct. 1873, 1882, 18 L.Ed.2d 1040, 1051 (1967); cf. ****1576** Hoffa v. United States, 385 U.S. 293, 304, 87 S.Ct. 408, 414, 17 L.Ed.2d 374, 383 (1966); and that disclosure of private information may be compelled if immunity removes the risk of incrimination. Kastigar v. United States, 406 U.S. 441, 92 S.Ct. 1653, 32 L.Ed.2d 212 (1972). If the Fifth Amendment protected generally against the obtaining of private information from a man's mouth or pen or house, its protections would presumably not be lifted by probable cause and a warrant or by immunity. The privacy invasion is not mitigated by immunity; and the Fifth Amendment's strictures, unlike the Fourth's, are not removed by showing reasonableness. The Framers addressed the subject of personal privacy directly in the Fourth Amendment. They struck a balance so that when the State's reason to believe incriminating evidence will be found becomes sufficiently great, the invasion of privacy becomes justified and a warrant to search and seize will issue. They did not seek in still another Amendment the Fifth to achieve a general protection of privacy but to deal with the more specific issue of compelled self-incrimination.

***401** [7] [8] We cannot cut the Fifth Amendment completely loose from the moorings of its language, and make it serve as a general protector of privacy a word not mentioned in its text and a concept directly addressed in the Fourth Amendment. We adhere to the view that the Fifth Amendment protects against "compelled self-incrimination, not (the disclosure of) private information." United States v. Nobles, 422 U.S. 225, 233 n. 7, 95 S.Ct. 2160, 2167, 45 L.Ed.2d 141 (1975).

Insofar as private information not obtained through compelled self-incriminating testimony is legally protected, its protection stems from other sources [6] the Fourth Amendment's protection against seizures without warrant or probable cause and against subpoenas which suffer from "too much indefiniteness or breadth in the things required to be 'particularly described,' " Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208, 66 S.Ct. 494, 505, 90 L.Ed. 614, 629 (1946); In re Horowitz, 482 F.2d 72, 75-80 (CA2 1973) (Friendly, J.); the First Amendment, see NAACP v. Alabama, 357 U.S. 449, 462, 78 S.Ct. 1163, 1171, 2 L.Ed.2d

1488, 1499 (1958); or evidentiary privileges such as the attorney-client privilege. [7]

***402** III

[9] Our above holding is that compelled production of documents from an attorney does not implicate whatever Fifth Amendment privilege the taxpayer might have enjoyed from being compelled to produce them himself. The taxpayers in these cases, however, have from the outset consistently urged that they should not be forced to expose otherwise protected documents to summons simply because they have sought legal advice and turned the papers over to their attorneys. The Government appears to agree unqualifiedly. The difficulty is that the taxpayers have erroneously relied on the Fifth Amendment without urging the attorney-client privilege in so many words. They have nevertheless invoked the relevant body of law and policies that govern the attorney-client privilege. ****1577** In this posture of the case, we feel obliged to inquire whether the attorney-client privilege applies to documents in the hands of an attorney which would have been privileged in the hands of the client by reason of the Fifth Amendment. [8]

***403** **[10]** **[11]** Confidential disclosures by a client to an attorney made in order to obtain legal assistance are privileged. 8 J. Wigmore, Evidence, s 2292 (McNaughton rev. 1961) (hereinafter Wigmore); McCormick s 87, p. 175. The purpose of the privilege is to encourage clients to make full disclosure to their attorneys. 8 Wigmore s 2291, and s 2306, p. 590; McCormick s 87, p. 175, s 92, p. 192; Baird v. Koerner, 279 F.2d 623 (CA9 1960); Modern Woodmen of America v. Watkins, 132 F.2d 352 (CA5 1942); Prichard v. United States, 181 F.2d 326 (CA6) aff'd, Per curiam, 339 U.S. 974, 70 S.Ct. 1029, 94 L.Ed. 1380 (1950); Schwimmer v. United States, 232 F.2d 855 (CA8 1956); United States v. Goldfarb, 328 F.2d 280 (CA6 1964). As a practical matter, if the client knows that damaging information could more readily be obtained from the attorney following disclosure than from himself in the absence of disclosure, the client would be reluctant to confide in his lawyer and it would be difficult to obtain fully informed legal advice. However, since the privilege has the effect of withholding relevant information from the fact-finder, it applies only where necessary to achieve its purpose. Accordingly it protects only those disclosures necessary to obtain informed legal advice which might not have been made absent the privilege. In re Horowitz, supra, 482 F.2d 72, at 81 (Friendly, J.); United States v. Goldfarb, supra, 328 F.2d 280; 8 Wigmore, s 2291, p. 554; McCormick, s 89, p. 185. This Court and the lower courts have thus uniformly held that pre-existing documents which could have been obtained by court process from the client when he was in possession may also be obtained from the attorney by similar process following transfer by the client in order ***404** to obtain more informed legal advice. *Grant v. United States*, 227 U.S. 74, 79-80, 33 S.Ct. 190, 192, 57 L.Ed. 423, 426 (1913); 8 Wigmore s 2307 and cases there cited; McCormick s 90, p. 185; *Falsone v. United States*, 205 F.2d 734 (CA5 1953); *Sovereign Camp, W.O.W. v. Reed,*, 208 Ala. 457, 94 So. 910 (1922); *Andrews v. Missisppi R. Co.*, 14 Ind. 169, 98 N.E. 49 (1860); Palatini v. Sarian, 15 N.J.Super. 34, 83 A.2d 24 (1951); Pearson v. Yoder, 39 Okl. 105, 134 P. 421 (1913); State ex rel. Sowers v. Olwell, 64 Wash.2d 828, 394 P.2d 681 (1964). The purpose of the privilege requires no broader rule. Pre-existing documents obtainable from the client are not appreciably easier to obtain from the attorney after transfer to him. Thus, even absent the attorney-client privilege, clients will not be discouraged from disclosing the documents to the attorney, and their ability to obtain informed legal advice will remain unfettered. It is otherwise if the documents are not obtainable by subpoena Duces tecum or summons while in the exclusive possession of the client, for the client will then be reluctant to transfer possession to the lawyer unless the documents are also privileged ****1578** in the latter's hands. Where the transfer is made for the purpose of obtaining legal advice, the purposes of the attorney-client privilege would be defeated unless the privilege is applicable. "It follows, then, that When the client himself would be privileged From production of the document, either as a party at common law . . . or as exempt from self-incrimination, the attorney having possession of the document is not bound to produce." 8 Wigmore s 2307, p. 592. Lower courts have so held. Id., s 2307, p. 592 n. 1, and cases there cited; United States v. Judson, 322 F.2d 460, 466 (CA9 1963); Colton v. United States, 306 F.2d 633, 639 (CA2 1962). This proposition was accepted by the Court of Appeals for the Fifth Circuit below, is asserted by petitioners ***405** in No. 74-18 and respondents in No. 74-611, and was conceded by the Government in its brief and at oral

argument. Where the transfer to the attorney is for the purpose of obtaining legal advice, we agree with it.

Since each taxpayer transferred possession of the documents in question from himself to his attorney in order to obtain legal assistance in the tax investigations in question, the papers, if unobtainable by summons from the client, are unobtainable by summons directed to the attorney by reason of the attorney-client privilege. We accordingly proceed to the question whether the documents could have been obtained by summons addressed to the taxpayer while the documents were in his possession. The only bar to enforcement of such summons asserted by the parties or the courts below is the Fifth Amendment's privilege against self-incrimination. On this question the Court of Appeals for the Fifth Circuit in No. 74-611 is at odds with the Court of Appeals for the Second Circuit in United States v. Beattie, 522 F.2d 267 (1975), cert. pending, Nos. 75-407, 75-700.

IV

The proposition that the Fifth Amendment prevents compelled production of documents over objection that such production might incriminate stems from Boyd v. United States, 116 U.S. 616, 68 S.Ct. 524, 29 L.Ed. 746 (1886). Boyd involved a civil forfeiture proceeding brought by the Government against two partners for fraudulently attempting to import 35 cases of glass without paying the prescribed duty. The partnership had contracted with the Government to furnish the glass needed in the construction of a Government building. The glass specified was foreign glass, it being understood that if part or all of the glass was furnished from the partnership's existing duty-paid inventory, ***406** it could be replaced by duty-free imports. Pursuant to this arrangement, 29 cases of glass were imported by the partnership duty free. The partners then represented that they were entitled to duty-free entry of an additional 35 cases which were soon to arrive. The forfeiture action concerned these 35 cases. The Government's position was that the partnership had replaced all of the glass used in construction of the Government building when imported the 29 cases. At trial, the Government obtained a court order directing the partners to produce an invoice the partnership had received from the shipper covering the previous 29-case shipment. The invoice was disclosed, offered in evidence, and used, over the Fifth Amendment objection of the partners, to establish that the partners were fraudulently claiming a greater exemption from duty than they were entitled to under the contract. This Court held that the invoice was inadmissible and reversed the judgment in favor of the Government. The Court ruled that the Fourth Amendment applied to court orders in the nature of subpoenas Duces tecum in the same manner in which it applies to search warrants, Id., at 622, 6 S.Ct., at 528, 29 L.Ed., at 748; and that the Government may not, consistent with the Fourth Amendment, seize a person's documents or other property as evidence unless it can claim a proprietary interest in the property superior to that of the person from whom the property is obtained. Id., at 623-624, 6 S.Ct., at 528-529, 29 L.Ed., at 748. The invoice in question was thus held to ****1579** have been obtained in violation of the Fourth Amendment. The Court went on to hold that the accused in a criminal case or the defendant in a forfeiture action could not be forced to produce evidentiary items without violating the Fifth Amendment as well as the Fourth. More specifically, the Court declared, "a compulsory production of the private books and papers of the owner of goods sought to be forfeited . . . is compelling him to be a witness against himself, ***407** within the meaning of the Fifth Amendment of the Constitution." Id., at 634-635, 6 S.Ct., at 534, 29 L.Ed., at 752. Admitting the partnership invoice into evidence had violated both the Fifth and Fourth Amendments.

Among its several pronouncements, Boyd Was understood to declare that the seizure, under warrant or otherwise, of any purely evidentiary materials violated the Fourth Amendment and that the Fifth Amendment rendered these seized materials inadmissible. Gouled v. United States, 255 U.S. 298, 41 S.Ct. 261, 65 L.Ed. 647 (1921); Agnello v. United States, 269 U.S. 20, 46 S.Ct. 4, 70 L.Ed. 145 (1925); United States v. Lefkowitz, 285 U.S. 452, 52 S.Ct. 420, 76 L.Ed. 877 (1932). That rule applied to documents as well as to other evidentiary items "(t)here is no special sanctity in papers, as distinguished from other forms of property, to render them immune from search and seizure, if only the fall within the scope of the principles of the cases in which other property may be seized. . . ." Gouled v. United States, supra, 255 U.S., at 309, 41 S.Ct., at 265, 65 L.Ed., at 652. Private papers taken from the taxpayer, like other "mere evidence," could

not be used against the accused over his Fourth and Fifth Amendment objections.

Several of Boyd's express or implicit declarations have not stood the test of time. The application of the Fourth Amendment to subpoenas was limited by Hale v. Henkel, 201 U.S. 43, 26 S.Ct. 370, 50 L.Ed. 652 (1906), and more recent cases. See, E. g., Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614 (1946). Purely evidentiary (but "nontestimonial") materials, as well as contraband and fruits and instrumentalities of crime, may now be searched for and seized under proper circumstances, Warden v. Hayden, 387 U.S. 294, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967).[9] Also, any notion that "testimonial" evidence may never be seized and used in evidence is ***408** inconsistent with *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (196; Osborn v. United States, 385 U.S. 323, 87 S.Ct. 429, 439, 17 L.Ed.2d 394 (1966); and Berger v. New York, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967), approving the seizure under appropriate circumstances of conversations of a person suspected of crime. See also Marron v. United States, 275 U.S. 192, 48 S.Ct. 74, 72 L.Ed. 231 (1927).

[12] It is also clear that the Fifth Amendment does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial Communication that is incriminating. We have, accordingly, declined to extend the protection of the privilege to the giving of blood samples, Schmerber v. California, 384 U.S. 757, 763-764, 86 S.Ct. 1826, 1831-1832, 16 L.Ed.2d 908, 915-916 (1966);[10] to the giving of handwriting exemplars, Gilbert v. California, 388 U.S. 263, 265-267, 87 S.Ct. 1951, 1952-1954, 18 L.Ed.2d 1178, 1181-1183 (1967); voice exemplars, ****1580** United States v. Wade, 388 U.S. 218, 222-223, 87 S.Ct. 1926, 1929-1930, 18 L.Ed.2d 1149, 1154-1155 (1967); or the donning of a blouse worn by the perpetrator, Holt v. United States, 218 U.S. 245, 31 S.Ct. 2, 54 L.Ed. 1021 (1910). Furthermore, despite Boyd, neither a partnership nor the individual partners are shielded from compelled production of partnership records on self-incrimination grounds. Bellis v. United States, 417 U.S. 85, 94 S.Ct. 2179, 40 L.Ed.2d 678 (1974). It would appear that under that case the precise claim sustained in Boyd would now be rejected for reasons not there considered.

The pronouncement in Boyd That a person may not be forced to produce his private papers has nonetheless often appeared as dictum in later opinions of this Court. See E. g., Wilson v. United States, 221 U.S. 361, 377, 31 S.Ct. 538, 543, 55 L.Ed. 771, 778 (1911); Wheeler v. United States, 226 U.S. 478, 489, 33 S.Ct. 158, 162, 57 L.Ed. 309, 313 (1913); ***409** United States v. White, 322 U.S. 694, 698-699, 64 S.Ct. 1248, 1251, 88 L.Ed. 1542, 1545-1546 1944); *Davis v. United States*, 328 U.S., at 587-588, 66 S.Ct., a1258-1259, 90 L.Ed., at 1456-1457; Schmerber, supra, 384 U.S., at 763-764, 86 S.Ct., at 1831-1832, 16 L.Ed.2d, at 915-916; Couch v. United States, 409 U.S., at 330, 93 S.Ct., at 616, 34 L.Ed.2d, at 555; Bellis v. United States, supra, 417 U.S., at 87, 94 S.Ct., at 2182, 40 L.Ed.2d, at 683. To the extent, however, that the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for "mere evidence," including documents, violated the Fourth Amendment and therefore also transgressed the Fifth, Gouled v. United States, supra, the foundations for the rule have been washed away. In consequence, the prohibition against forcing the production of private papers has long been a rule searching for a rationale consistent with the proscriptions of the Fifth Amendment against compelling a person to give "testimony" that incriminates him. Accordingly, we turn to the question of what, if any, incriminating testimony within the Fifth Amendment's protection, is compelled by a documentary summons.

[13] A subpoena served on a taxpayer requiring him to produce an accountant's workpapers in his possession without doubt involves substantial compulsion. But it does not compel oral testimony; nor would it ordinarily compel the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought. Therefore, the Fifth Amendment would not be violated by the fact alone that the papers on their face might incriminate the taxpayer, for the privilege protects a person only against being incriminated by his own compelled testimonial communications. Schmerber v.

California, supra ; United States v. Wade, supra, and Gilbert v. California, supra. The accountant's workpapers are not the taxpayer's. They were not prepared by the taxpayer, and they contain no testimonial declarations by him. Furthermore, as far as this record demonstrates, the preparation of all of the papers sought in these cases was wholly voluntary, and they cannot be said to contain compelled ***410** testimonial evidence, either of the taxpayers or of anyone else.[11] The taxpayer cannot avoid compliance with the subpoena merely by asserting ****1581** that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else.

[14] The act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena. Curcio v. United States, 354 U.S. 118, 125, 77 S.Ct. 1145, 1150, 1 L.Ed.2d 1225, 1231 (1957). The elements of compulsion are clearly present, but the more difficult issues are whether the tacit averments of the taxpayer are both "testimonial" and "incriminating" for purposes of applying the Fifth Amendment. These questions perhaps do not lend themselves to categorical answers; their resolution may instead depend on the facts and circumstances of particular cases or classes thereof. In light of the records now before us, we are confident that however incriminating the ***411** contents of the accountant's workpapers might be, the act of producing them the only thing which the taxpayer is compelled to do would not itself involve testimonial self-incrimination.

It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. The papers belong to the accountant, were prepared by him, and are the kind usually prepared by an accountant working on the tax returns of his client. Surely the Government is in no way relying on the "truth-telling" of the taxpayer to prove the existence of or his access to the documents. 8 Wigmore s 2264, p. 380. The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender." In re Harris, 221 U.S. 274, 279, 31 S.Ct. 557, 558, 55 L.Ed. 732, 735 (1911).

When an accused is required to submit a handwriting exemplar he admits his ability to write and impliedly asserts that the exemplar is his writing. But in common experience, the first would be a near truism and the latter self-evident. In any event, although the exemplar may be incriminating to the accused and although he is compelled to furnish it, his Fifth Amendment privilege is not violated because nothing he has said or done is deemed to be sufficiently testimonial for purposes of the privilege. This Court has also time and again allowed subpoenas against the custodian of corporate documents or those belonging to other collective entities such as unions and partnerships and those of bankrupt businesses over claims that the documents will incriminate the custodian despite the fact that producing the documents tacitly admits their existence and their location in the ***412** hands of their possessor. *E. g., Wilson v. United States*, 221 U.S. 361, 31 S.Ct. 538, 55 L.Ed. 771 (1911); *Dreier v. United States*, 221 U.S. 394, 31 S.Ct. 550, 55 L.Ed. 784 (1911); *United States v. White*, 322 U.S. 694, 64 S.Ct. 1248, 88 L.Ed. 1542 (1944); *Bellis v. United States*, 417 U.S. 85, 94 S.Ct. 2179, 40 L.Ed.2d 678 (1974); *In re Harris*, *supra*. The existence and possession or control of the subpoenaed documents being no more in issue here than in the above cases, the summons is equally enforceable.

Moreover, assuming that these aspects of producing the accountant's papers have some minimal testimonial significance, surely it is not illegal to seek accounting help in connection with one's tax returns or for the accountant to prepare workpapers and deliver them to the taxpayer. At this juncture, we are quite unprepared to hold that either the fact of existence of the papers or of their possession by the taxpayer poses any realistic threat of incrimination to the taxpayer.

****1582** As for the possibility that responding to the subpoena would authenticate[12] the workpapers, production would ***413** express nothing more than the tax payer's belief that the papers are those described in the subpoena. The taxpayer would be no more competent to authenticate the accountant's workpapers or reports[13] by producing them than

he would be to authenticate them if testifying orally. The taxpayer did not prepare the papers and could not vouch for their accuracy. The documents would not be admissible in evidence against the taxpayer without authenticating testimony. Without more, responding to the subpoena in the circumstances before us would not appear to represent a substantial threat of self-incrimination. Moreover, in Wilson v. United States, supra ; Dreier v. United States, supra ; United States v. White, supra; Bellis v. United States, supra ; and In re Harris, supra, the custodian of corporate, union, or partnership books or those of a bankrupt business was ordered to respond to a subpoena for the business' books even though doing so involved a "representation that the documents produced are those demanded by the subpoena," Curcio v. United States, 354 U.S., at 125, 77 S.Ct., at 1150, 1 L.Ed.2d, at 1231. [14]

***414** **[15]** Whether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his "private papers," see Boyd v. United States, supra, 116 U.S., at 634-635, 6 S.Ct., at 534, 29 L.Ed., at 752. We do hold that compliance with a summons directing the taxpayer to produce the accountant's documents involved in these cases would involve no incriminating testimony within the protection of the Fifth Amendment.

The judgment of the Court of Appeals for the Fifth Circuit in No. 74-611 is reversed. The judgment of the Court of Appeals for the Third Circuit in No. 74-18 is affirmed.

So ordered.

Affirmed in part; reversed in part.

Mr. Justice STEVENS took no part in the consideration or disposition of these cases.

****1583** Mr. Justice BRENNAN, concurring in the judgment.

I concur in the judgment. Given the prior access by accountants retained by the taxpayers to the papers involved in these cases and the wholly business rather than personal nature of the papers, I agree that the privilege against compelled self-incrimination did not in either of these cases protect the papers from production in response to the summonses. See Couch v. United States, 409 U.S. 322, 335-336, 93 S.Ct. 611, 619-620, 34 L.Ed.2d 548, 557-558 (1973); Id., at 337, 93 S.Ct., at 620, 34 L.Ed.2d, at 559 (Brennan, J., concurring). I do not join the Court's opinion, however, because of the portent of much of what is said of a serious crippling of the protection secured by the privilege against compelled production of one's private books and papers. Like today's decision in United States v. Miller, 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71, it is but another step in the denigration of privacy principles settled nearly 100 years ago in ***415** Boyd v. United States, 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746 1886). According to the Court, "(w)hether the Fifth Amendment would shield the taxpayer from producing his own tax records in his possession is a question not involved here; for the papers demanded here are not his 'private papers.' " Ante, at 1582. This implication that the privilege might not protect against compelled production of tax records that are his "private papers" is so contrary to settled constitutional jurisprudence that this and other like implications throughout the opinion [1] prompt me to conjecture that once again the Court is laying the groundwork for future decisions that will tell us that the question here formally reserved was actually answered against the availability of the privilege. Semble, Hudgens v. NLRB, 424 U.S. 507, 96 S.Ct. 1029, 47 L.Ed.2d 196 (1976). It is therefore appropriate to recall that history and this Court have construed the constitutional privilege to safeguard against governmental intrusions of personal privacy to compel either self-incriminating oral statements or the production of self-incriminating evidence recorded in one's private books and papers. Although as phrased in the Fifth Amendment "nor shall (any person) be compelled in any criminal case to be a witness against himself" the privilege makes no express reference, as does the Fourth Amendment, to "papers, and effects," private papers have long been held to have the protection of the privilege, designed as it is "to maintain inviolate large areas of personal privacy." Feldman v. United States, 322 U.S. 487, 490, 64 S.Ct. 1082, 1083, 88 L.Ed. 1408, 1412 (1944).

***416** I

Expressions are legion in opinions of this Court that the protection of personal privacy is a central purpose of the

privilege against compelled self-incrimination. "(I)t is the invasion of (a person's) indefeasible right of personal security, personal liberty and private property" that "constitutes the essence of the offence" that violates the privilege. Boyd v. United States, supra, 116 U.S., at 630, 6 S.Ct., at 532, 29 L.Ed., at 751. The privilege reflects "our respect for the inviolability of the human personality and of the right of each individual 'to a private enclave where he may lead a private life.' " Murphy v. Waterfront Comm'n, 378 U.S. 52, 55, 84 S.Ct. 1594, 1597, 12 L.Ed.2d 678, 681 (1964). "It respects a private inner sanctum of individual feeling and thought and proscribes state intrusion to extract self-condemnation." Couch v. United States, supra, 409 U.S., at 327, 93 S.Ct., at 615, 34 L.Ed.2d at 553. See also Tehan v. United States ex rel. Shott, 382 U.S. 406, 416, 86 S.Ct. 459, 465, 15 L.Ed.2d 453, 460 (1966); **1584 Miranda v. Arizona, 384 U.S. 436, 460, 86 S.Ct. 1602, 1620, 16 L.Ed.2d 694, 715 (1966). "The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment." Griswold v. Connecticut, 381 U.S. 479, 484, 85 S.Ct. 1678, 1681, 14 L.Ed.2d 510, 515 (1965). See also Katz v. United States, 389 U.S. 347, 350 n.5, 88 S.Ct. 507, 510, 19 L.Ed.2d 576, 581 (1967).

The Court pays lip service to this bedrock premise of privacy in the statement that "(w)ithin the limits imposed by the language of the Fifth Amendment, which we necessarily observe, the privilege truly serves privacy interests," Ante, at 1575. But this only makes explicit what elsewhere highlights the opinion, namely, the view that protection of personal privacy is merely a by product and not, as our precedents and history teach, a factor controlling in part the determination of the scope of the privilege. This cart-before-the-horse approach is fundamentally at odds with the settled principle that the scope of the privilege is not constrained by the limits of the *417 wording of the Fifth Amendment but has the reach necessary to protect the cherished value of privacy which it safeguards. See *Schmerber v. California*, 384 U.S. 757, 761-762, 86 S.Ct. 1826, 1831, 16 L.Ed.2d 908, 914 n. 6 (1966). The "Court has always construed provisions of the Constitution having regard to the principles upon which it was established. The direct operation or literal meaning of the words used do not measure the ppose or scope of its provisions. . . ." United States v. Lefkowitz, 285 U.S. 452, 467, 52 S.Ct. 420, 424, 76 L.Ed. 877, 883 (1932). "It has been repeatedly decided that (the Fifth Amendment) should receive a liberal construction, so as to prevent stealthy encroachment upon or 'gradual depreciation' of the rights secured by (it), by imperceptible practice of courts or by well-intentioned, but mistakenly overzealous executive officers." Gouled v. United States, 255 U.S. 298, 304, 41 S.Ct. 261, 263, 65 L.Ed. 647, 650 (1921). See Maness v. Meyers, 419 U.S. 449, 461, 95 S.Ct. 584, 592, 42 L.Ed.2d 574, 584 (1975). History and principle, not the mechanical application of its wording, have been the life of the Amendment. [2]

That the privilege does not protect against the production of private information where there is no compulsion, or where immunity is granted, or where there is no threat of incrimination in nowise supports the Court's argument demeaning the privilege's protection of privacy. The unavailability of the privilege in those cases only evidences that, as is the case with the First and Fourth Amendments, the protection of privacy afforded by the privilege is not absolute. The critical question then is the definition of the scope of privacy that is sheltered by the privilege.

*418 History and principle teach that the privacy protected by the Fifth Amendment extends not just to the individual's immediate declarations, oral or written, but also to his testimonial materials in the form of books and papers. [3] "The right was originally a 'right of silence' . . . only in the sense that legal process could not force incriminating statements from the defendant's **1585 own lips. Beginning in the early eighteenth century the English courts widened that right to include protection against the necessity of producing books and documents that might tend to incriminate the accused. . . .Lord Mansfield summed up the law by declaring that the defendant, in a criminal case, could not be compelled to produce any incriminating documentary evidence 'though he should hold it in his hands in Court.' " L. Levy, Origins of the Fifth Amendment 390 (1968). [4] Thus, in recognizing *419 the privilege's protection of private books and papers, Boyd v. United States, 116 U.S., at 633, 634-635, 6 S.Ct., at 533, 534-535, 29 L.Ed., at 752, 753, was faithful to this historical conception of the privilege. Boyd was reaffirmed in this respect in Ballmann v. Fagin, 200 U.S. 186, 26 S.Ct. 212, 50 L.Ed. 433 (1906), which held that

an individual could not be compelled to produce a personal cashbook containing incriminating evidence. Schmerber v. California, 384 U.S., at 761, 86 S.Ct., at 1830, 16 L.Ed.2d, at 914, most recently expressly held "that the privilege protects an accused . . . from being compelled to testify against himself, or Otherwise provide the State with evidence of a testimonial or communicative nature . . .." (Emphasis supplied.) Indeed, Boyd's holding has often been reiterated without question. E.g., Bellis v. United States, 417 U.S. 85, 87, 94 S.Ct. 2179, 2182, 40 L.Ed.2d 678, 683 (1974); United States v. Calandra, 414 U.S. 338, 346, 94 S.Ct. 613, 619, 38 L.Ed.2d 561, 570 (1974); Couch v. United States, 409 U.S. 322, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973); United States v. Wade, 388 U.S. 218, 221, 87 S.Ct. 1926, 1929, 18 L.Ed.2d 1149, 1154 (1967); Gilbert v. California, 388 U.S. 263, 266, 87 S.Ct. 1951, 1953, 18 L.Ed.2d 1178, 1182 (1967); Davis v. United States, 328 U.S. 582, 587-588, 66 S.Ct. 1256, 1257-1259, 90 L.Ed. 1453, 1456-1457 (1946); United States v. White, 322 U.S. 694, 698-699, 64 S.Ct. 1248, 1251, 88 L.Ed. 1542, 1545, 1546 (1944); Wheeler v. United States, 226 U.S. 478, 489, 33 S.Ct. 158, 162, 57 L.Ed. 309, 313 (1913); Wilson v. United States, 221 U.S. 361, 375, 31 S.Ct. 538, 542, 55 L.Ed. 771 (1911); ICC v. Baird, 194 U.S. 25, 45, 24 S.Ct. 563, 569, 48 L.Ed. 860, 869 (1904). It may therefore be emphatically stated that until today, there was no room to doubt that it is the Fifth Amendment's "historic function (to protect an individual) from compulsory incrimination through his ***420** own testimony or *personal records*." *United States v. White, supra*, 322 U.S., at 701, 64 S.Ct., at 1252, 88 L.Ed., at 1547 (emphasis supplied).

The common-law and constitutional extension of the privilege to testimonial materials, such as books and papers, was inevitable. An individual's books and papers are generally little more than an extension of his person. They reveal no less than he could reveal upon being questioned directly. Many of the matters within an individual's knowledge may as easily be retained within his head as set down on a scrap of paper. I perceive no principle which does not permit compelling one to disclose the contents of one's mind but does permit compelling the disclosure of the contents of that scrap of paper by compelling its production. Under a contrary view, the constitutional protection ****1586** would turn on fortuity, and persons would, at their peril, record their thoughts and the events of their lives. The ability to think private thoughts, facilitated as it is by pen and paper, and the ability to preserve intimate memories would be curtailed through fear that those thoughts or events of those memories would become the subjects of criminal sanctions however invalidly imposed. Indeed, it was the very reality of those fears that helped provide the historical impetus for the privilege. See Boyd v. United States, supra, 116 U.S., at 631-632, 6 S.Ct., at 532-533, 29 L.Ed., at 751-752; E. Griswold, The Fifth Amendment Today 8-9 (1955); 8 J. Wigmore, Evidence s 2250, pp. 277-281 (McNaughton rev. 1961); Id., s 2251, pp. 313-314; McKay, Self-Incrimination and the New Privacy, 1967 Supreme Court Review 193, 212. [5]

***421** ****1587** The Court's treatment of the privilege falls far short of giving it the scope required by history and our precedents. [6] It is, of course, true "that the Fifth Amendment ***422** protects against 'compelled self-incrimination, not the disclosure of) private information,' " Ante, at 1576, but it is also true that governmental compulsion to produce private information that might incriminate violates the protection of the privilege. Similarly, although it is necessary that the papers "contain no testimonial declarations by (the taxpayer)" in order for the privilege not to operate as a bar to production, Ante, at 1575, it does not follow ***423** that papers are not "testimonial" and thus producible because they contain no declarations. And while it may be that the unavailability of the privilege depends on a showing that "the preparation of all of the papers sought in these cases was wholly voluntary," Ibid., again it does not follow that the protection is necessarily unavailable if the papers were prepared voluntarily, for it is the compelled Production of testimonial evidence, not just the compelled creation of such evidence, against which the privilege protects.

Though recognizing that a subpoena served on a taxpayer involves substantial compulsion, the Court concludes that since the subpoena does not compel oral testimony or require the taxpayer to restate, repeat, or affirm the truth of the contents of the documents sought, compelled production of the documents by the taxpayer would not violate the privilege, even though the documents might incriminate the taxpayer. Ante, at 1580. This analysis is patently incomplete: the

threshold inquiry is whether the taxpayer is compelled to produce incriminating papers. That inquiry is not answered in favor of production merely because the subpoena requires neither oral testimony from nor affirmation of the papers' contents by the taxpayer. To be sure, the Court correctly observes that "(t)he taxpayer cannot avoid compliance with the subpoena Merely by asserting that the item of evidence which he is required to produce contains incriminating writing, whether his own or that of someone else." Ante, at 1580 (emphasis supplied). For it is not enough that the production of a writing, or books and papers, is compelled. Unless those materials are such as to come within the zone of privacy recognized by the Amendment, the privilege against compulsory self-incrimination does not protect against their production.

***424** We are not without guideposts for determining what books, papers, and writings come within the zone of privacy recognized by the Amendment. In Wilson v. United States, 221 U.S. 361, 31 S.Ct. 538, 58 L.Ed. 771 (1911), for example, the Court held that the Fifth Amendment did not protect against subpoenaing corporate records in the possession and control of the president of a corporation, even though the records might have incriminated him. Though the evidence was testimonial, though its production was compelled, and though it would have incriminated the party producing it, the Fifth Amendment was no bar. The Court recognized that the Amendment "(u)ndoubtedly . . . protected (the president) against the compulsory production of his private books and papers," Id., at 377, 31 S.Ct., at 543, 55 L.Ed., at 778 but with respect to corporate records, the Court held:
"(T)hey are of a character which subjects them to the scrutiny demanded . . . . This was clearly implied in the Boyd Case, where the fact that the papers involved were the Private papers of the claimant was constantly emphasized. Thus, in the case of public records and official documents, made or kept in the ****1588** administration of public office, the fact of actual possession or of lawful custody would not justify the officer in resisting inspection, even though the record was made by himself and would supply the evidence of his criminal dereliction." Id., at 380, 31 S.Ct., at 544, 55 L.Ed., at 779 (emphasis in original).

Couch v. United States, expressly held that the Fifth Amendment protected against the compelled production of testimonial evidence only if the individual resisting production had a reasonable expectation of privacy with respect to the evidence. 409 U.S., at 336, 93 S.Ct., at 619, 34 L.Ed.2d, at 558. ***425** Couch relied on Perlman v. United States, 247 U.S. 7, 38 S.C 417, 62 L.Ed. 950 (1918), where the Court permitted the use against the defendant of documentary evidence belonging to him because "there was a voluntary exposition of the articles" rather than "an invasion of the defendant's privacy." Id., at 14, 38 S.Ct., at 420, 62 L.Ed., at 955. Under Couch, therefore, one criterion is whether or not the information sought to be produced has been disclosed to or was within the knowledge of a third party. 409 U.S., at 332-333, 93 S.Ct., at 617-618, 34 L.Ed.2d, at 556-557. That is to say, one relevant consideration is the degree to which the paper holder has sought to keep private the contents of the papers he desires not to produce.

Most recently, Bellis v. United States, 417 U.S. 85, 94 S.Ct. 2179, 40 L.Ed.2d 678 (1974), followed the approach taken in Wilson. Bellis held that the partner of a small law firm could not invoke the privilege against self-incrimination to justify his refusal to comply with a subpoena requiring production of the partnership's financial records. Bellis stated: "It has long been established . . . that the Fifth Amendment privilege against compulsory self-incrimination protects an individual from compelled production of his personal papers and effects as well as compelled oral testimony. . . . The privilege applies to the business records of the sole proprietor or sole practitioner as well as to personal documents containing more intimate information about the individual's private life." 417 U.S., at 87-88, 94 S.Ct., at 2182, 40 L.Ed.2d, at 683. Bellis also recognized that the Court's "decisions holding the privilege inapplicable to the records of a collective entity also reflect . . . the protection of an individual's right to a ' "private enclave where he may lead a private life." ' . . . Protection of individual privacy was the major theme running through the Court's decision in Boyd . . . and it was on this basis that the Court in Wilson distinguished the corporate records involved in that case from the private papers at issue in Boyd." Id., at 92-92, 94 S.Ct., at 2184, 40 L.Ed.2d, at 685. "(C)orporate ***426** records do not contain the requisite element of privacy or confidentiality essential for the privilege to attach." Id., at 92, 94 S.Ct., at 2185, 40 L.Ed.2d, at 686. Bellis concluded

that the same considerations which precluded reliance upon the privilege with respect to corporate records also precluded reliance upon it with respect to partnership records in the circumstances of that case. [7]

A precise cataloguing of private papers within the ambit of the privacy protected by the privilege is probably impossible. Some papers, however, do lend themselves to classification. See generally Comment, The Search and Seizure of Private Papers: Fourth and Fifth Amendment Considerations, 6 Loyola (LA) L.Rev. 274, 300-303 (1973). Production of documentary materials created or authenticated by a State or the Federal Government, such as automobile registrations or property deeds, would seem ordinarily to fall outside the protection of the privilege. They hardly reflect an extension of the person.

**1589 Economic and business records may present difficulty in particular cases. The records of business entities generally fall without the scope of the privilege. But, as noted, the Court has recognized that the privilege extends to the business records of the sole proprietor or practitioner. Such records are at least an extension of an aspect of a person's activities, though concededly *427 not the more intimate aspects of one's life. Where the privilege would have protected one's mental notes of his business affairs in a less complicated day and age, it would seem that that protection should not fall away because the complexities of another time compel one to keep business records. Cf. *Olmstead v. United States,* 277 U.S. 438, 474, 48 S.Ct. 564, 571, 72 Ld. 944, 954 (1928) (Brandeis, J., dissenting). Nonbusiness economic records in the possession of an individual, such as canceled checks or tax records, would also seem to be protected. They may provide clear insights into a person's total lifestyle. They are, however, like business records and the papers involved in these cases, frequently, though not always, disclosed to other parties; and disclosure, in proper cases, may foreclose reliance upon the privilege. Personal letters constitute an integral aspect of a person's private enclave. And while letters, being necessarily interpersonal, are not wholly private, their peculiarly private nature and the generally narrow extent of their disclosure would seem to render them within the scope of the privilege. Papers in the nature of a personal diary are A fortiori protected under the privilege.

The Court's treatment in the instant cases of the question whether the evidence involved here is within the protection of the privilege is, with all respect, most inadequate. The gaping hole is in the omission of any reference to the taxpayer's privacy interests and to whether the subpoenas impermissibly invade those interests. The observations that the "accountant's workpapers are not the taxpayer's" and "were not prepared by the taxpayer," Ante, at 1580, touch on matters relevant to the taxpayer's expectation of privacy, but do not of themselves determine the availability of the privilege. Wilson v. United States, 221 U.S., at 378, 31 S.Ct., at 543, 55 L.Ed., at 778, stated: "(T)he mere fact that *428 the appellant himself wrote, or signed, the (documents), neither conditioned nor enlarged his privilege. Where one's private documents would tend to incriminate him, the privilege exists although they were actually written by another person." [8] Thus, although "(t)he fact that the documents may have been written by the person asserting the privilege is insufficient to trigger the privilege," Ante, at 1580 n. 11, and "the fact that it was written by him is not controlling . . .," Ibid., this is not to say that the privilege is available only as to documents written by him. For the reasons I have stated at the outset, however, I do not believe that the evidence involved in these cases falls within the scope of privacy protected by the Fifth Amendment.

II

I also question the Court's treatment of the question whether the act of producing evidence is "testimonial." I agree that the act of production implicitly admits the existence of the evidence requested and possession or control of that evidence by the party producing it. It also implicitly authenticates the evidence as that identified in the order to compel. I disagree, however, that implicit admission of the existence and possession or control of the papers in this case is not "testimonial" merely because the Government could readily have otherwise proved existence and possession or control in these cases. *429 I know of no Fifth Amendment principle which makes **1590 the testimonial nature of evidence, and therefore, one's protection against incriminating himself, turn on the strength of the Government's case against him.

Nor do I consider the taxpayers' implicit authentication an insubstantial threat of self-incrimination. Actually, authentication of the papers as those described in the

subpoenas establishes the papers as the taxpayers', thereby supplying an incriminatory link in the chain of evidence against them. It is not the less so because the taxpayers' accountants may also provide the link, since the protection against self-incrimination cannot, I repeat, turn on the strength of the Government's case.

This Court's treatment of handwriting exemplars is not supportive of its position. See Gilbert v. California, 388 U.S. 263, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967). The Court has only recognized that "(a) mere handwriting exemplar . . ., like the voice or body itself, is an identifying physical characteristic outside its protection." Id., 388 U.S., at 266-267, 87 S.Ct., at 1953, 18 L.Ed.2d, at 1183. It is because handwriting exemplars are viewed as strictly nontestimonial, not because they are insufficiently testimonial, that the Fifth Amendment does not protect against their compelled production. Also not supportive of the Court's position is the principle that the custodian of documents of a collective entity is not protected from the act of producing those documents. Nothing in the language of those cases, either expressly or impliedly, indicates that the act of production with respect to the records of business entities is insufficiently testimonial for purposes of the Fifth Amendment. At most, those issues, though considered, were disposed of on the ground, not that production was insufficiently testimonial, but that one in control of the records of an artificial organization ***430** undertakes an obligation with respect to those records foreclosing any exercise of his privilege. [9]

Mr. Justice MARSHALL, concurring in the judgment.

Today the Court adopts a wholly new approach for deciding when the Fifth Amendment privilege against self-incrimination can be asserted to bar production of documentary evidence. [1] This approach has, in various ***431** forms, been discussed by commentors for some time; nonetheless as I noted a few years ago, the theory "has an odd sound to it." Couch v. United States, 409 U.S. 322, 348, 93 S.Ct. 611, 625, 34 L.Ed.2d 548, 565 (1973) (dissenting). The Fifth Amendment basis for resisting production ****1591** of a document pursuant to subpoena, the Court tells us today, lies not in the document's contents, as we previously have suggested, but in the tacit verification inherent in the act of production itself that the document exists, is in the possession of the producer, and is the one sought by the subpoena.

This technical and somewhat esoteric focus on the testimonial elements of production rather than on the content of the evidence the investigator seeks is, as Mr. Justice BRENNAN demonstrates, contrary to the history and traditions of the privilege against self-incrimination both in this country and in England, where the privilege originated. A long line of precedents in this Court, whose rationales if not holdings are overturned by the Court today, support the notion that "any forcible and compulsory extortion of a man's . . . private papers to be used as evidence to convict him of crime" compels him to be a witness against himself within the meaning of the Fifth Amendment to the Constitution. Boyd v. United States, 116 U.S. 616, 630, 6 S.Ct. 524, 532, 29 L.Ed. 746, 751 (1886). See also Bellis v. United States, 417 U.S. 85, 87, 94 S.Ct. 2179, 2182, 40 L.Ed.2d 678, 683 (1974); Couch v. United States, supra, 409 U.S., at 330, 93 S.Ct., at 616, 34 L.Ed.2d, at 555; Schmerber v. California, 384 U.S. 757, 763-764, 86 S.Ct. 1826, 1831-1832, 16 L.Ed.2d 908, 915-916 (1966); Davis v. United States, 328 U.S. 582, 587-588, 66 S.Ct. 1256, 1258-1259, 90 L.Ed. 1453, 1456-1457 (1946); United States v. White, 322 U.S. 694, 698-699, 64 S.Ct. 1248, 1251, 88 L.Ed. 1542, 1545-1546 (1944); Wheeler v. United States, 226 U.S. 478, 489, 33 S.Ct. 158, 162, 57 L.Ed. 309, 313 (1913); Wilson v. United States, 221 U.S. 361, 377, 31 S.Ct. 538, 543, 55 L.Ed. 771, 778 (1911).

However analytically imprecise these cases may be, they represent a deeply held belief on the part of the Members of this Court throughout its history that there ***432** are certain documents no person ought to be compelled to produce at the Government's request. While I welcome the Court's attempt to provide a rationale for this longstanding rule, it is incumbent upon the Court, I believe, to fashion its theory so as to protect those documents that have always stood at the core of the Court's concern. Thus, I would have preferred it had the Court found some room in its theory for recognition of the import of the contents of the documents themselves. See Couch v. United States, supra, 409 U.S., at 350, 93 S.Ct., at 626, 34 L.Ed.2d, at 566 (Marshall, J., dissenting).

Nonetheless, I am hopeful that the Court's new theory, properly understood and applied, will provide substantially

the same protection as our prior focus on the contents of the documents. The Court recognizes, as others have argued, that the act of production can verify the authenticity of the documents produced. See, E. g., United States v. Beattie, 522 F.2d 267 (CA2 1975), cert. pending, Nos. 75-407, 75-700. But the promise of the Court's theory lies in its innovative discernment that production may also verify the documents' very existence and present possession by the producer. This expanded recognition of the kinds of testimony inherent in production not only rationalizes the cases, but seems to me to afford almost complete protection against compulsory production of our most private papers.

Thus, the Court's rationale provides a persuasive basis for distinguishing between the corporate-document cases and those involving the papers of private citizens. Since the existence of corporate record books is seldom in doubt, the verification of their existence, inherent in their production, may fairly be termed not testimonial at all. On the other hand, there is little reason to assume the present existence and possession of most private papers, and certainly not those Mr. Justice BRENNAN places at the top of his list of documents that the privilege should protect. See Ante, at 1588-1589 (concurring in judgment). ***433** Indeed, there would appear to be a precise inverse relationship between the private nature of the document and the permissibility of assuming ****1592** its existence. Therefore, under the Court's theory, the admission through production that one's diary, letters, prior tax returns, personally maintained financial records, or canceled checks exist would ordinarily provide substantial testimony. The incriminating nature of such an admission is clear, for while it may not be criminal to keep a diary, or write letters or checks, the admission that one does and that those documents are still available may quickly or simultaneously lead to incriminating evidence. If there is a "real danger" of such a result, that is enough under our cases to make such testimony subject to the claim of privilege. See Rogers v. United States, 340 U.S. 367, 71 S.Ct. 438, 95 L.Ed. 344 (1951); Brown v. Walker, 161 U.S. 591, 16 S.Ct. 644, 40 L.Ed. 819 (1896); Counselman v. Hitchcock, 142 U.S. 547, 12 S.Ct. 195, 35 L.Ed. 1110 (1892). Thus, in practice, the Court's approach should still focus upon the private nature of the papers subpoenaed and protect those about which Boyd and its progeny were most concerned.

The Court's theory will also limit the prosecution's ability to use documents secured through a grant of immunity. If authentication that the document produced is the document demanded were the only testimony inherent in production, immunity would be a useful tool for obtaining written evidence. So long as a document obtained under an immunity grant could be authenticated through other sources, as would often be possible, reliance on the immunized testimony the authentication and its fruits would not be necessary, and the document could be introduced. The Court's recognition that the act of production also involves testimony about the existence and possession of the subpoenaed documents mandates a different result. Under the Court's theory, if the document is to be obtained the ***434** immunity grant must extend to the testimony that the document is presently in existence. Such a grant will effectively shield the contents of the document, for the contents are a direct fruit of the immunized testimony that the document exists and cannot usually be obtained without reliance on that testimony.[2] Accordingly, the Court's theory offers substantially the same protection against procurement of documents under grant of immunity that our prior cases afford.

In short, while the Court sacrifices our pragmatic, if somewhat Ad hoc, content analysis for what might seem an unduly technical focus on the act of production itself, I am far less pessimistic than Mr. Justice BRENNAN that this new approach signals the end of Fifth Amendment protection for documents we have long held to be privileged. I am not ready to embrace the approach myself, but I am confident in the ability of the trial judges who must apply this difficult test in the first instance to act with sensitivity to our traditional concerns in this uncertain area.

For the reasons stated by Mr. Justice BRENNAN, I concur in the judgment of the Court.

All Citations

425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39, 37 A.F.T.R.2d 76-1244, 76-1 USTC P 9353, 1976-1 C.B. 411

Footnotes

* The syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader. See United States v. Detroit Timber & Lumber Co., 200 U.S. 321, 337, 26 S.Ct. 282, 287, 50 L.Ed. 499, 505.

1 In No. 74-18, the taxpayers are husband and wife who filed a joint return. In No. 74-611, the taxpayer filed an individual return.

2 The "books and records" concerned the taxpayer's large medical practice.

3 The husband taxpayer's checks and deposit receipts related to his textile waste business. The wife's related to her women's wear shop.

4 The respondents in No. 74-611 did not, in terms, rely on the attorney-client privilege or the Fourth Amendment before the Court of Appeals.

5 There is a line of cases in which the Court stated that the Fifth Amendment was offended by the use in evidence of documents or property seized in violation of the Fourth Amendment. Gouled v. United States, 255 U.S. 298, 306, 41 S.Ct. 261, 264, 65 L.Ed. 647, 651 (1921); Agnello v. United States, 269 U.S. 20, 33-34, 46 S.Ct. 4, 6-7, 70 L.Ed. 145, 149-150 (1925); United States v. Lefkowitz, 285 U.S. 452, 466-467, 52 S.Ct. 420, 424, 76 L.Ed. 877, 883 (1932); Mapp v. Ohio, 367 U.S. 643, 661, 81 S.Ct. 1684, 1694, 6 L.Ed.2d 1081, 1093 (1961) (Black, J., concurring). But the Court purported to find elements of compulsion in such situations. "In either case he is the unwilling source of the evidence, and the Fifth Amendment forbids that he shall be compelled to be a witness against himself in a criminal case." Gouled v. United States, supra, 255 U.S., at 306, 41 S.Ct., at 264, 65 L.Ed., at 651. In any event the predicate for those cases, lacking here, was a violation of the Fourth Amendment. Cf. Burdeau v. McDowell, supra, 256 U.S. 465, 475-476, 41 S.Ct. 574, 576, 65 L.Ed. 1048, 1050-1051 (1921).

6 In Couch v. United States, 409 U.S. 322, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973), on which taxpayers rely for their claim that the Fifth Amendment protects their "legitimate expectation of privacy," the Court differentiated between the things protected by the Fourth and Fifth Amendments. "We hold today that no Fourth or Fifth Amendment claim can prevail where, as in this case, there exists no legitimate expectation of privacy and no semblance of governmental compulsion against the person of the accused." Id., 409 U.S., at 336, 93 S.Ct., at 620, 34 L.Ed.2d, at 558.

7 The taxpayers and their attorneys have not raised arguments of a Fourth Amendment nature before this Court and could not be successful if they had. The summonses are narrowly drawn and seek only documents of unquestionable relevance to the tax investigation. Special problems of privacy which might be presented by subpoena of a personal diary, United States v. Bennett, 409 F.2d 888, 897 (CA2 1969) (Friendly, J.), are not involved here.

First Amendment values are also plainly not implicated in these cases.

8 Federal Rule Evid. 501, effective January 2, 1975, provides that with respect to privileges the United States district courts "shall be governed by the principles of the common law . . . interpreted . . . in the light of reason and experience." Thus, whether or not Rule 501 applies to this case, the attorney-client privilege issue is governed by the principles and authorities discussed and cited Infra. Fed.Rule Crim.Proc. 26.

In No. 74-611, the taxpayer did not intervene, and his rights have been asserted only through his lawyer. The parties disagree on the question whether an attorney may claim the Fifth Amendment privilege of his client. We need not resolve this question. The only privilege of the taxpayer involved here is the attorney-

client privilege, and it is universally accepted that the attorney-client privilege may be raised by the attorney, C. McCormick, Evidence s 92, p.193, s 94, p. 197 (2d ed. 1972) (hereinafter McCormick); Republic Gear Co. v. Borg-Warner Corp., 381 F.2d 551 (CA2 1967); Bouschor v. United States, 316 F.2d 451 (CA8 1963); Colton v. United States, 306 F.2d 633 (CA2 1962); Schwimmer v. United States, 232 F.2d 855 (CA8), cert. denied, 352 U.S. 833, 77 S.Ct. 48, 1 L.Ed.2d 52 (1956); Baldwin v. Commissioner, 125 F.2d 812 (CA9 1942).

9 Citing to Schmerber v. California, 384 U.S. 757, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966), Warden v. Hayden, 387 U.S., at 302-303, 87 S.Ct., at 1648, 18 L.Ed.2d, at 789, reserved the question "whether there are items of evidential value whose very nature precludes them from being the object of a reasonable search and seizure."

10 The Court's holding was: "Since the blood test evidence, although an incriminating product of compulsion, was neither petitioner's testimony nor evidence relating to some communicative act or writing by petitioner, it was not inadmissible on privilege grounds." 384 U.S., at 765, 86 S.Ct., at 1833, 16 L.Ed.2d, at 916.

11 The fact that the documents may have been written by the person asserting the privilege is insufficient to trigger the privilege, Wilson v. United States, 221 U.S. 361, 378, 31 S.Ct. 538, 543, 55 L.Ed. 771, 778 (1911). And, unless the Government has compelled the subpoenaed person to write the document, cf. Marchetti v. United States, 390 U.S. 39, 88 S.Ct. 697, 19 L.Ed.2d 889 (1968); Grosso v. United States, 390 U.S. 62, 88 S.Ct. 709, 19 L.Ed.2d 906 (1968), the fact that it was written by him is not controlling with respect to the Fifth Amendment issue. Conversations may be seized and introduced in evidence under proper safeguards, Katz v. United States, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967); Osborn v. United States, 385 U.S. 323, 87 S.Ct. 429, 439, 17 L.Ed.2d 394 (1966); Berger v. New York, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967); United States v. Bennett, 409 F.2d, at 897 n. 9, if not compelled. In the case of a documentary subpoena the only thing compelled is the act of producing the document and the compelled act is the same as the one performed when a chattel or document not authored by the producer is demanded. McCormick s 128, p. 261.

12 The "implicit authentication" rationale appears to be the prevailing justification for the Fifth Amendment's application to documentary subpoenas. Schmerber v. California, 384 U.S., at 763-764, 86 S.Ct., at 1832, 16 L.Ed.2d, at 915-916 ("the privilege reaches . . . the compulsion of responses which are also communications, for example, compliance with a subpoena to produce one's papers. Boyd v. United States, 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746"); Couch v. United States, 409 U.S., at 344, 346, 93 S.Ct., at 611, 625, 34 L.Ed.2d, at 548, 564 (Marshall, J., dissenting) (the person complying with the subpoena "implicitly testifies that the evidence he brings forth is in fact the evidence demanded"); United States v. Beattie, 522 F.2d 267, 270 (CA2 1975) (Friendly, J.) ("(a) subpoena demanding that an accused produce his own records is . . . the equivalent of requiring him to take the stand and admit their genuineness"), cert. pending, Nos. 75-407, 75-700; 8 Wigmore s 2264, p. 380 (the testimonial component involved in compliance with an order for production of documents or chattels "is the witness' assurance, compelled as an incident of the process, that the articles produced are the ones demanded"); McCormick s 126, p. 268 ("(t)his rule (applying the Fifth Amendment privilege to documentary subpoenas) is defended on the theory that one who produces documents (or other matter) described in the subpoena Duces tecum represents, by his production, that the documents produced are in fact the documents described in the subpoena"); People v. Defore, 242 N.Y. 13, 27, 150 N.E. 585, 590 (1926) (Cardozo, J.) ("A defendant is 'protected from producing his documents

in response to a Subpoena duces tecum, for his production of them in court would be his voucher of their genuineness.' There would then be 'testimonial compulsion' ").

13 In seeking the accountant's "retained copies" of correspondence with the taxpayer in No. 74-611, we assume that the summons sought only "copies" of original letters sent from the accountant to the taxpayer the truth of the contents of which could be testified to only by the accountant.

14 In these cases compliance with the subpoena is required even though the books have been kept by the person subpoenaed and his producing them would itself be sufficient authentication to permit their introduction against him.

1 For example, the Court's notation that "(s)pecial problems of privacy which might be presented by subpoena of a diary . . . are not involved here," Ante, at 1576 n. 7, is only made in the context of discussion of the Fourth Amendment and thus may readily imply that even a subpoena of a personal diary containing forthright confessions of crime may not be resisted on grounds of the privilege.

2 "The privilege against self-incrimination is a specific provision of which it is peculiarly true that 'a page of history is worth a volume of logic.' " Ullmann v. United States, 350 U.S. 422, 438, 76 S.Ct. 497, 506, 100 L.Ed. 511, 524 (1956) (Frankfurter, J.). "The previous history of the right, both in England and America, proves that it was not bound by rigid definition." L. Levy, Origins of the Fifth Amendment 428 (1968).

3 Indeed, Schmerber v. California, 384 U.S. 757, 764, 86 S.Ct. 1826, 1832, 16 L.Ed.2d 908, 916 (1966), held: "Some tests seemingly directed to obtain 'physical evidence,' for example, lie detector tests measuring changes in body function during interrogation, may actually be directed to eliciting responses which are essentially testimonial. To compel a person to submit to testing in which an effort will be made to determine his guilt or innocence on the basis of physiological responses, whether willed or not, is to evoke the spirit and history of the Fifth Amendment. Such situations call to mind the principle that the protection of the privilege 'is as broad as the mischief against which it seeks to guard.' . . ."

4 "The language of the Constitution cannot be interpreted safely except by reference to the common law and to British institutions as they were when the instrument was framed and adopted." Ex parte Grossman, 267 U.S. 87, 108-109, 45 S.Ct. 332, 333, 69 L.Ed. 527, 530 (1925). But, "the common law rule invoked shall be one not rejected by our ancestors as unsuited to their civil or political conditions." Grosjean v. American Press Co., 297 U.S. 233, 249, 56 S.Ct. 444, 449, 80 L.Ed. 660, 668 (1936). Without a doubt, the common-law privilege against self-incrimination in England extended to protection against the production of incriminating personal papers prior to the adoption of the United States Constitution. See, E.g., Roe v. Harvey, 98 Eng.Rep. 302, 305 (K.B.1769); King v. Heydon, 96 Eng.Rep. 195 (K.B.1762); King v. Purnell, 95 Eng.Rep. 595, 597 (K.B.1748); King v. Cornelius, 93 Eng.Rep. 1133, 1134 (K.B.1744); Queen v. Mead, 92 Eng.Rep. 119 (K.B.1703); King v. Worsenham, 91 Eng.Rep. 1370 (K.B.1701). The significance of this English development on the construction of our Constitution is not in any way diminished by this country's experience with the privilege prior to the Constitution's adoption. See Levy, Supra, n. 2, at 368-404.

5 "And any compulsory discovery by extorting the party's oath, or compelling the production of his private books and papers, to convict him of crime, or to forfeit his property, is contrary to the principles of a free government. It is abhorrent to the instincts of an Englishman; it is abhorrent to the instincts of an American. It may suit the purposes of despotic power; but it cannot abide the pure atmosphere of political liberty and personal freedom." Boyd v. United States, 116 U.S., at 631-632, 6 S.Ct., at 533, 29 L.Ed., at 751.
The proposition, Ante, at 1580, that Boyd's holding ultimately rested on the Fourth Amendment could not be more incorrect. Boyd did observe that the purposes to be served by the Fourth and Fifth Amendments shed light on each other, 116 U.S., at 633, 6 S.Ct., at 534, 29 L.Ed., at 752, but the holdings that the compelled production of the papers involved there violated the Fourth and Fifth Amendments were independent of each

other. In holding that "a compulsory production of the private books and papers of the owner of goods sought to be forfeited in such a suit is compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution, and is the equivalent of a search and seizure and an unreasonable search and seizure within the meaning of the Fourth Amendment," Id., at 634-635, 6 S.Ct., at 534, 29 L.Ed., at 752, the Court plainly did not make the Fourth Amendment violation a predicate, let alone an essential predicate, for its holding that there was also a Fifth Amendment violation. The Court is incorrect in suggesting that "the rule against compelling production of private papers rested on the proposition that seizures of or subpoenas for 'mere evidence,' including documents, violated the Fourth Amendment and therefore also transgressed the Fifth." Ante, at 1580. The relation of the Fourth Amendment to the Fifth Amendment violation in United States v. Lefkowitz, 285 U.S. 452, 52 S.Ct. 420, 76 L.Ed. 877 (1932); Agnello v. United States, 269 U.S. 20, 46 S.Ct. 4, 70 L.Ed. 145 (1925); and Gouled v. United States, 255 U.S. 298, 41 S.Ct. 261, 65 L.Ed. 647 (1921), was merely that the illegal searches and seizures in those cases were held to establish the element of compulsion essential to a Fifth Amendment violation. See Ante, at 1575 n. 5 Even if the Fourth Amendment violations were now held not to establish the element of Fifth Amendment compulsion, it, of course, would not follow that the Fifth Amendment's protection against compelled production of incriminating private papers is lost.

Furthermore, that purely evidentiary material may have been seized in those cases was neither relied upon to establish the Fourth Amendment violations nor, in turn, to establish the Fifth Amendment violations. Indeed, in Agnello, contraband, not mere evidence, was illegally seized. Subsequent decisions modifying the "mere evidence" rule, therefore, have left untouched the Fifth Amendment's prohibition against the compelled production of incriminating testimonial evidence. Indeed, citing Warden v. Hayden, 387 U.S. 294, 87 S.Ct. 1642, 18 L.Ed.2d 782 (1967), the Court notes, that the question is open whether the Legal search and seizure of some forms of testimonial evidence would violate the Fifth Amendment, Ante, at 1579 n. 9. Warden v. Hayden observed: "The items of clothing involved in this case are not 'testimonial' or 'communicative' in nature, and their introduction therefore did not compel respondent to become a witness against himself in violation of the Fifth Amendment. . . . This case thus does not require that we consider whether there are items of evidential value whose very nature precludes them from being the object of a reasonable search and seizure." 387 U.S., at 302-303, 87 S.Ct., at 1648, 18 L.Ed.2d, at 789. That observation was plainly addressed not to application of the Fourth Amendment but to application of the Fifth.

Contrary to the Court's intimations, Ante, at 1579, neither Katz v. United States, 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 583 (1967); Osborn v. United States, 385 U.S. 323, 87 S.Ct. 429, 17 L.Ed.2d 394 (1966); nor Berger v. New York, 388 U.S. 41, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967), all involving the Fourth Amendment, lends support to an argument that the Fifth Amendment would not protect the seizure of the private papers of a person suspected of crime. Fifth Amendment challenges to the seizure and use of private papers were not involved in those cases.

6 The grudging scope the Court today gives the privilege against self-incrimination is made evident by its observation that "(i)n the case of a documentary subpoena the only thing compelled is the act of producing the document . . .." Ante, at 1580 n. 11. Obviously disclosure or production of testimonial evidence is also compelled, and the heart of the protection of the privilege is in its safeguarding against compelled disclosure or production of that evidence.

7 With respect to a partnership invoice, it thus seems fair to say, as the Court does, Ante, at 1579, "that under (Bellis) the precise claim sustained in Boyd would now be rejected for reasons not there considered." Bellis, however, took care to point out: "We do not believe the Court in Boyd can be said to have decided the issue

presented today," 417 U.S., at 95 n. 2, 94 S.Ct., at 2187, 40 L.Ed.2d, at 688, thereby leaving unaltered Boyd's more general or "imprecise" holding protecting against the compelled production of private papers.

8 Similarly, United States v. Nobles, 422 U.S. 225, 95 S.Ct. 2160, 45 L.Ed.2d 141 (1975), held that the Fifth Amendment did not bar production of a defense investigator's summaries of interviews with witnesses. The Court carefully noted, however, that there was no indication that the summaries contained any information conveyed by the defendant to the investigator. Id., at 234, 95 S.Ct., at 2168, 45 L.Ed.2d, at 151.

9 Individuals acting as representatives of a collective group "assume the rights, duties and privileges of the artificial entity or association of which they are agents or officers, and they are bound by its obligations." United States v. White, 322 U.S. 694, 699, 64 S.Ct. 1248, 1251, 88 L.Ed. 1542, 1546 (1944). "In view of the inescapable fact that an artificial entity can only act or produce its records through its individual officers or agents, recognition of the individual's claim of privilege with respect to the financial records of the organization would substantially undermine the unchallenged rule that the organization itself is not entitled to claim any Fifth Amendment privilege, and largely frustrate legitimate governmental regulation of such organizations." Bellis v. United States, 417 U.S., at 90, 94 S.Ct., at 2184, 40 L.Ed.2d, at 685. Indeed, in one of the more recent corporate records cases, Curcio v. United States, 354 U.S. 118, 125, 77 S.Ct. 1145, 1150, 1 L.Ed.2d 1225, 1231 (1957), the Court expressly recognized that "(t)he custodian's act of producing books or records in response to a subpoena Duces tecum is itself a representation that the documents produced are those demanded by the subpoena." The Court in Curcio, however, apparently did not note any self-incrimination problem because of the undertaking by the custodian with respect to the documents. (One charged with failure to comply with an order to produce, however, may not thereafter be compelled to testify as to the existence or his control of the documents. See Curcio v. United States, supra.) In the present cases, of course, the taxpayers are not representatives of any artificial entity and have not undertaken any obligation with respect to that entity or its documents. They have stipulated, however, that the documents involved here exist and are those described in the subpoenas, thereby obviating any problem as to self-incrimination in these cases resulting from the act of production itself.

1 The Court's theory would appear to apply to real evidence as well.

2 Similarly, the Court's theory affords protection to one who possesses documents that he cannot authenticate. If authentication were the only relevant testimony inherent in the act of production, such a person would be forced to relinquish his documents, for he provides no authentication testimony of relevance by producing them in response to a subpoena. See United States v. Beattie, 522 F.2d 267 (CA2 1975) cert. pending, Nos. 75-407, 75-700. Under the Court's theory, however, if the existence of these documents were in question, the custodian would still be able to assert a claim of privilege against their production.

220 A.3d 534
Supreme Court of Pennsylvania.

COMMONWEALTH of Pennsylvania, Appellee
v.
Joseph J. DAVIS, Appellant

No. 56 MAP 2018
|
Argued: May 14, 2019
|
Decided: November 20, 2019

Synopsis

Background: Commonwealth filed pre-trial motion to compel defendant, who was charged with distribution of child pornography, to provide passcode to allow access to defendant's lawfully-seized encrypted computer. The Court of Common Pleas, Luzerne County, Criminal Division, No. CP–40–CR–0000291–2016, CP–40–MD–0000011–2016, Tina Polachek Gartley, J., granted the motion to compel, and defendant appealed. The Superior Court, No. 1243 MDA 2016, 176 A.3d 869, affirmed. Defendant appealed by allowance.

Holdings: The Supreme Court, No. 56 MAP 2018, Todd, J., held that:

[1] as matter of first impression, compelling defendant to reveal password to allow access to his lawfully-seized encrypted computer was "testimonial" in nature, triggering Fifth Amendment privilege against self-incrimination;

[2] as matter of first impression, the foregone conclusion exception to application of the Fifth Amendment privilege against self-incrimination has limited application and is inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer; and

[3] even if foregone conclusion exception to the Fifth Amendment privilege against self-incrimination could be applied to the compulsion to reveal a computer password, Commonwealth failed to satisfy requirements of exception.

Reversed and remanded.

Baer, J., filed dissenting opinion in which Dougherty and Mundy, JJ., joined.

Procedural Posture(s): Pre-Trial Hearing Motion; Appellate Review.

West Headnotes (14)

[1] **Criminal Law** Constitutional issues in general

Criminal Law Review De Novo

The Supreme Court's standard of review of an issue involving a constitutional right is de novo, and its scope of review is plenary.

1 Cases that cite this headnote

[2] **Criminal Law** Compelling Self-Incrimination

Witnesses Proceedings to which privilege applies

The Fifth Amendment privilege against self-incrimination not only applies to a defendant in a criminal trial, but in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate the speaker in future criminal proceedings. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[3] **Witnesses** Self-Incrimination

The Fifth Amendment privilege against self-incrimination protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature. U.S. Const. Amend. 5.

[4] **Witnesses** Self-Incrimination

In order to be testimonial within the meaning of the Fifth Amendment, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information; only then is a person compelled to be a witness against himself. U.S. Const. Amend. 5.

[5] **Witnesses** Self-Incrimination

In the realm of the non-physical disclosure of information, the Fifth Amendment privilege against self-incrimination is broad, as compelled testimony that communicates information that may lead to incriminating evidence is privileged even if the information itself is not inculpatory; thus, the privilege is a protection against the prosecutor's use of incriminating information derived directly or indirectly from the compelled testimony. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[6] **Witnesses** Self-Incrimination

Whenever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the "trilemma" of truth, falsity, or silence, and hence the response, whether based on truth or falsity, contains a testimonial component within the meaning of the Fifth Amendment. U.S. Const. Amend. 5.

[7] **Criminal Law** Compelling Self-Incrimination

Witnesses Self-Incrimination

To invoke the Fifth Amendment privilege against the forced provision of information, a defendant must show (1) the evidence is self-incriminating; (2) the evidence is compelled; and (3) the evidence is testimonial in nature. U.S. Const. Amend. 5.

[8] **Witnesses** Self-Incrimination

Where the government compels a physical act, such production is not testimonial, and the Fifth Amendment privilege against self-incrimination is not recognized. U.S. Const. Amend. 5.

2 Cases that cite this headnote

[9] **Witnesses** Privilege as to production of documents

An act of production may be testimonial within the meaning of the Fifth Amendment when the act expresses some explicit or implicit statement of fact that certain materials exist, are in the defendant's custody or control, or are authentic; the crux of whether an act of production is testimonial is whether the government compels the defendant to use the contents of his own mind in explicitly or implicitly communicating a fact. U.S. Const. Amend. 5.

[10] **Witnesses** Privilege as to production of documents

Compelling defendant, who was charged with distribution of child pornography, to reveal password to allow access to his lawfully-seized encrypted computer was "testimonial" in nature, triggering Fifth Amendment privilege against self-incrimination; Commonwealth was seeking electronic equivalent of combination to wall safe not as an end, but as a pathway to files being withheld, such that compelled production of the computer's password demanded recall of contents of defendant's mind and act of production carried with it the implied factual assertions that would be used to incriminate him. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[11] **Witnesses** Privilege as to production of documents

Compelling the disclosure of a password to a computer is an act of production that is testimonial within the meaning of the Fifth Amendment privilege against self-incrimination. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[12] **Witnesses** Privilege as to production of documents

For the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination to apply to the production of otherwise testimonial evidence, the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence. U.S. Const. Amend. 5.

2 Cases that cite this headnote

[13] **Witnesses** Privilege as to production of documents

The foregone conclusion exception to application of the Fifth Amendment privilege against self-incrimination has limited application and is inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer. U.S. Const. Amend. 5.

4 Cases that cite this headnote

[14] **Witnesses** Privilege as to production of documents

Even if foregone conclusion exception to the Fifth Amendment privilege against self-incrimination could be applied to the compulsion to reveal a computer password, Commonwealth failed to satisfy requirements of exception in seeking to compel defendant, charged with distribution of child pornography, to provide password to allow access to his lawfully-seized encrypted computer; while there was high probability that child pornography existed on defendant's computer, as evidenced by fact that defendant's internet address used filed sharing network to share videos depicting child pornography, compelled revelation of password could lead to trove of presently unknown number of files, given that Commonwealth would have access to all of computer's contents. U.S. Const. Amend. 5.

***537** Appeal from the Order of the Superior Court dated November 30, 2017 at No. 1243 MDA 2016, affirming the Order of the Court of Common Pleas of Luzerne County, Criminal Division, dated June 30, 2016 Nos. CP-40-CR-291-2016 and CP-40-MD-11-2016. Tina Polachek Gartley, Judge

Attorneys and Law Firms

Thomas Farrell, Esq., Farrell & Reisinger, LLC, Tyler R. Green, Esq., for Amicus Curiae.

Andrew Chapman Christy, Esq., ACLU of Pennsylvania, Demetrius Wm. Fannick, Esq., Steven M. Greenwald, Esq., Mark Alan Singer, Esq., Luzerne County Public Defenders Office, Peter David Goldberger, Esq., Law Office of Peter Goldberger, Witold J. Walczak, Esq., American Civil Liberties Union, Robert Eugene Welsh Jr., Esq., Welsh & Recker, P.C., Jennifer Stisa Granick, Esq., Brett Max Kaufman, Esq., Michael Charles Kostelaba, Esq., Amanda Marie Young, Esq., for Appellant.

Joshua D. Shapiro, Esq., William Ross Stoycos, Esq., Pennsylvania Office of Attorney General, for Appellee.

SAYLOR, C.J., BAER, TODD, DONOHUE, DOUGHERTY, WECHT, MUNDY, JJ.

OPINION

JUSTICE TODD

In this appeal by allowance, we consider an issue of first impression: Whether a defendant may be compelled to

disclose a password to allow the Commonwealth access to the defendant's lawfully-seized, but encrypted, computer. For the reasons that follow, we find that such compulsion is violative of the Fifth Amendment to the United States Constitution's prohibition against self-incrimination. Thus, we reverse the order of the Superior Court.

On July 14, 2014, agents of the Office of Attorney General ("OAG"), as part of their investigation of the electronic dissemination of child pornography, discovered that a computer at an identified Internet Protocol (IP) address [1] registered with Comcast Cable Communications ("Comcast"), repeatedly utilized a peer-to-peer file-sharing network, eMule, to share child pornography. N.T. Hearing, 1/14/16, at 6-8. Specifically, agents used a computer with software designed to make a one-to-one connection with the computer at the aforementioned IP address and downloaded a file, later confirmed to contain child pornography, which was saved to the OAG computer. *Id.* at 5-6. Based upon its transference and review of the file, the OAG obtained a court order to compel Comcast to provide subscriber information associated with the IP address. The information provided by Comcast disclosed the subscriber as Appellant Joseph Davis, as well as his address. *Id.* at 8-9.

On September 9, 2014, the OAG applied for, received, and executed a search warrant at Appellant's apartment. OAG Special Agent Justin Leri informed Appellant that he was not under arrest, but that the search involved an investigation of child pornography. *Id.* at 11. Appellant was then read his *Miranda* warnings and waived his *Miranda* rights. *Id.* Appellant acknowledged that he was the sole user of a Dell computer. [2] He admitted to having prior ***538** pornography convictions, but denied the computer contained any illegal pornographic images. Appellant then declined to answer additional questions without a lawyer. *Id.* Later examination of the computer revealed that the hard drive had been "wiped," removing data entirely or rendering it unreadable. *Id.* at 43-44.

On October 4, 2015, OAG Agent Daniel Block identified a different child pornography video that was shared with a different IP address utilizing the eMule server. An administrative subpoena to Comcast regarding this IP address again produced Appellant's name and contact information. A direct connection was made from OAG computers to this IP address, and one electronic file containing child pornography was transferred to the OAG computer. *Id.* at 19.

On October 20, 2015, the OAG executed another search warrant at Appellant's apartment based upon this video. At Appellant's apartment, the agents discovered a single computer, an HP Envy 700 desktop. After being *Mirandized*, Appellant informed the agents that he lived alone, that he was the sole user of the computer, and that he used hardwired Internet services which are password protected, and, thus, not accessible by the public, such as through Wifi. *Id.* at 26. Appellant offered that only he knew the password to his computer. *Id.* Appellant also informed the agents, *inter alia*, that he watched pornography on the computer which he believed was legal; that he had previously been arrested for child pornography; and that child pornography was legal in other countries so he did not understand why it was illegal in the United States. *Id.* at 27-28. The agents arrested Appellant for the eMule distributions and seized his computer. Agent Block asked Appellant for the password to this computer and Appellant refused. *Id.* at 28. Subsequently, when in transit to his arraignment, Appellant spoke openly about watching various pornographic movies, indicating that he particularly liked watching 10, 11, 12, and 13-year olds. *Id.* at 30. Agent Block again requested that Appellant provide him with the password to the computer. Appellant responded: "It's 64 characters and why would I give that to you? We both know what's on there. It's only going to hurt me. No f*cking way I'm going to give it to you." *Id.*

Later, in a holding cell, Agent Leri conversed with Appellant who, *inter alia*, offered that he believes the "government continuously spies on individuals," and questioned "why it's illegal to ... view movies in the privacy of [his] own home." *Id.* at 35. In a later conversation, Agent Leri asked Appellant if he could remember the password. Appellant replied that he could not remember it, and that, even if he could, it would be like "putting a gun to his head and pulling the trigger." *Id.* at 35-36. In a subsequent visit, when asked again about the password, Appellant offered that "he would die in jail before he could ever remember the password." *Id.* at 37.

A supervisory agent in computer forensics, Special Agent Braden Cook, testified that a portion of Appellant's HP 700 Envy computer's hard drive was encrypted with a program called TrueCrypt Version 7.1. *Id.* at 42. The entire hard drive of the computer was encrypted and "there was no data

that could be read without opening the TrueCrypt volume." *Id.* at 46. Agent Cook could only confirm that there was "Windows on the computer and the TrueCrypt," and he had no knowledge of any specific files other than the operating system files. *Id.* at 50-51.

***539** Appellant was charged with two counts of disseminating child pornography in violation of 18 Pa.C.S. § 6312(c), and two counts of criminal use of a communication facility in violation of 18 Pa.C.S. § 7512(a), which arose from the July 2014 and October 2015 detections.

On December 17, 2015, the Commonwealth filed with the Luzerne County Court of Common Pleas a pre-trial motion to compel Appellant to divulge the password to his HP 700 computer. Appellant responded by invoking his right against self-incrimination. On January 14, 2016, the trial court conducted an evidentiary hearing at which several OAG agents testified, as set forth above, about the investigation supporting the seizure of the computer.

The trial court focused on the question of whether the encryption was testimonial in nature, and, thus, protected by the Fifth Amendment. The trial court opined that "[t]he touchstone of whether an act of production is testimonial is whether the government compels the individual to use 'the contents of his own mind' to explicitly or implicitly communicate some statement of fact." Trial Court Opinion, 6/30/2016, at 8-9 (citation omitted). As part of its analysis, the trial court looked to the "foregone conclusion" exception to the Fifth Amendment privilege against self-incrimination as articulated by the United States Supreme Court in *Fisher v. United States*, 425 U.S. 391, 409, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). The court noted the rationale underlying this doctrine is that an act of production does not involve testimonial communication if the facts conveyed are already known to the government, such that the individual " 'adds little or nothing to the sum total of the government's information.' " Trial Court Opinion, 6/30/2016, at 9 (quoting *Fisher*, 425 U.S. at 409, 96 S.Ct. 1569). The trial court offered that for this exception to apply, the government must establish its knowledge of (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence. *Id.* at 9.

Applying the foregone conclusion exception, the trial court found that, in the case at bar, the computer located in Appellant's residence had hard-wired Internet access only; Appellant admitted it was TrueCrypt encrypted; that he was the only user, and he was the only one who knew the password; Appellant indicated to the agents that "we both know what is on there," and stated that he would "die in prison before giving up the password;" and that the Commonwealth knew with a reasonable degree of certainty that child pornography was on the computer. *Id.* at 11. Based upon these facts, the trial court determined that the information the Commonwealth sought from Appellant was a foregone conclusion, in that the facts to be conveyed by Appellant's act of production of his password already were known to the government. As, according to the trial court, Appellant's revealing his password would not provide the Commonwealth with any new evidence, and would simply be an act that permitted the Commonwealth to retrieve what was already known to them, the foregone conclusion exception was satisfied. Thus, on June 30, 2016, the trial court granted the Commonwealth's motion and directed Appellant to supply the Commonwealth with any passwords used to access the computer within 30 days. Appellant filed an interlocutory appeal.

A three-judge panel of the Superior Court affirmed. *Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. 2017).[3] Like the ***540** trial court, the Superior Court found that, to qualify for the Fifth Amendment privilege, a communication must be testimonial. The Superior Court observed that the question of whether compelling an individual to provide a digital password was testimonial in nature was an issue of first impression for the court. Building upon the trial court's analysis, the Superior Court explained that the Fifth Amendment right against self-incrimination is not violated when the information communicated to the government by way of a compelled act of production is a foregone conclusion. The court reasoned that the foregone conclusion exception provides that an act of production does not involve testimonial communication where the facts conveyed already are known to the government and set forth the applicable three-prong test. *Id.* at 874-75 (citing *Fisher*, 425 U.S. at 410-13, 96 S.Ct. 1569).

Applying the foregone conclusion exception, the Superior Court, contrary to the trial court, focused on the password itself, and reasoned that the Commonwealth established the computer could not be opened without the password, that the computer belonged to Appellant and the password was in his possession, and that this information was "self-authenticating" — *i.e.*, if the computer was accessible upon entry of the password, the password was authentic. *Id.* at 876. Further, the court noted that multiple jurisdictions have held that the government's knowledge of the encrypted documents or evidence that it sought to compel did not need to be exact, and determined that, based on the agents' forensic investigation, as well as Appellant's own statements to the agents while in custody, there was a high probability that child pornography existed on his computer. Thus, the Superior Court concluded that the trial court did not err in holding that the act of providing the password in question was not testimonial in nature and that Appellant's Fifth Amendment right against self-incrimination would not be violated by compelling him to disclose the password.

[1] Our Court granted allocatur to consider the following issue, as framed by Appellant:

> May [Appellant] be compelled to disclose orally the memorized password to a computer over his invocation of privilege under the Fifth Amendment to the Constitution of the United States, and Article I, [S]ection 9 of the Pennsylvania Constitution?

Commonwealth v. Davis, —— Pa. ——, 195 A.3d 557 (2018) (order). The parameters of our review of an issue involving a constitutional right is well settled. Our standard of review is *de novo*, and our scope of review is plenary. *Commonwealth v. Baldwin*, 619 Pa. 178, 58 A.3d 754, 762 (2012).

Appellant argues the Fifth Amendment prohibits government compulsion to disclose a computer password against one's will, reasoning that requiring an individual to recall and disclose the memorized password is quintessentially testimonial, *i.e.*, revealing the contents of one's own mind. Indeed, according to Appellant, the privilege is not just about information, but is "about a core of individual autonomy into which the state may not encroach." Appellant's Brief at 16. Appellant maintains that, ***541** as his password exists in his mind, he cannot be compelled to remember the password or reveal it, as a person's thoughts and knowledge are at the core of the Fifth Amendment.

According to Appellant, the Fifth Amendment protects against not only compelled written and oral testimony, but nonverbal acts as well. Appellant continues that, while not at issue in this appeal, even if the Commonwealth had obtained an order compelling Appellant to physically enter his password into his computer — rather than forcing him to speak or write down his password — this would still constitute a form of written testimony and, in any event, such a demand for action still requires using the contents of his mind to enter his password. Appellant contrasts such compulsion with one requiring merely physical acts, such as being required to wear a particular shirt, provide a blood sample, or provide a handwriting exemplar, which are not testimonial in nature, as they do not rely on the contents of one's mind. *See* *Holt v. United States*, 218 U.S. 245, 252-53, 31 S.Ct. 2, 54 L.Ed. 1021 (1910); *Schmerber v. California*, 384 U.S. 757, 761, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966); *Gilbert v. California*, 388 U.S. 263, 266-67, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967). Appellant offers that providing a password that will unlock data on a computer is no different from providing a combination that unlocks a briefcase or a safe, which has been held to be testimonial in nature.

Appellant further asserts that the Supreme Court's " 'foregone conclusion' rationale," as set forth in *Fisher*, does not apply to computer passwords. Appellant's Brief at 24. Appellant suggests that the holding in *Fisher* was limited to its facts and merely involved the question of whether the disclosure of certain tax documents known to be in the possession of the defendants' attorneys, as agents of the defendants, could be compelled by the government. In distinguishing *Fisher*, Appellant not only emphasizes that in that case the request did not compel oral testimony, or require restating, repeating, or affirming the truth of the contents of the documents, but explains that, because accountants prepared the papers which were ultimately

possessed by defendants' attorneys, and could independently authenticate them, the Government was not relying upon the "truth-telling" of the defendants. *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569.

Appellant submits that, regardless of the scope of the foregone conclusion rationale, it is limited to the act of producing documents and that, as discussed below, the United States Supreme Court has applied the foregone conclusion exception only once since *Fisher*, rejecting its usage in the context of the compelled production of business records. *United States v. Hubbell*, 530 U.S. 27, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) (dismissing government's reliance on foregone conclusion exception, finding that compulsion to produce papers that would require defendant to make use of his own mind to identify hundreds of documents responsive to the request did not fall within the exception).

Appellant asserts that, even if the foregone conclusion rationale could apply to the compelled decryption of a computer, it cannot be satisfied in this matter. Specifically, as to the password itself, Appellant contends that it is not a foregone conclusion that he even knows the password at this time. Likewise, if the rationale goes to the presence of contraband on Appellant's computer, which Appellant maintains that it does, here, the OAG agents noted that they could not tell what might be on the confiscated computer, and, as the computer was not connected to the Internet when it was seized, there is no proof that it was ***542** the one used to share pornography on eMule.[4] Finally, Appellant adds that the relatively few states that have considered the decryption password issue have reached divergent conclusions, and stresses that the national trend is toward greater protections.

The Commonwealth explains that the Fifth Amendment, by its terms, provides that no person shall be compelled in any criminal case to be a witness against himself; thus, according to the Commonwealth, this Amendment covers only communications that are testimonial, and the compulsion to produce physical evidence is not protected. The Commonwealth relies almost exclusively on what it describes as the foregone conclusion "doctrine," as articulated in *Fisher* and other decisional law. The Commonwealth surveys various decisions and submits that the majority of cases find it logical and sound to extend the foregone conclusion exception to providing the password to an encrypted device. Here, according to the Commonwealth, the compelled act is the surrendering of the password, and the "testimony" inherent in Appellant's production of the password — the existence, location, and authenticity, *of the password* — is a foregone conclusion. In short, the Commonwealth contends that revealing the password will add nothing communicative to the government's information as it does not disclose information about the computer or its contents. Thus, the Commonwealth asserts it has met its burden in this regard.[5]

[2] **[3]** **[4]** Our analysis begins with the United States Constitution. The Self-Incrimination Clause of the Fifth Amendment provides "[n]o person ... shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. This privilege not only applies to a defendant in a criminal trial, but "in any other proceeding, civil or criminal, formal or informal, where the answers might incriminate [the speaker] in future criminal proceedings." *Minnesota v. Murphy*, 465 U.S. 420, 426, 104 S.Ct. 1136, 79 L.Ed.2d 409 (1984) (citation omitted). "Although the text does not delineate the ways in which a person might be made a 'witness against himself,' we have long held that the privilege does not protect a suspect from being compelled by the State to produce 'real or physical evidence.' ***543** Rather, the privilege 'protects an accused only from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature.' " *Pennsylvania v. Muniz*, 496 U.S. 582, 588-89, 110 S.Ct. 2638, 110 L.Ed.2d 528 (1990) (citations omitted). As offered by Justice Oliver Wendell Holmes, "the prohibition of compelling a man in criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material." *Holt*, 218 U.S. at 252-53, 31 S.Ct. 2. Indeed, "in order to be testimonial, an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information. Only then is a person compelled to be a 'witness' against himself." *Doe v. United States*, 487 U.S. 201, 210, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988) ("*Doe II*") (footnote omitted).

[5] However, in the realm of the non-physical disclosure of information, the privilege is broad, as "compelled testimony that communicates information that may 'lead to incriminating evidence' is privileged even if the information itself is not inculpatory." *Id.*, 487 U.S. at 208 n.6, 108 S.Ct. 2341. Thus, it is a "protection against the prosecutor's use of incriminating information derived directly or indirectly from the compelled testimony." *Hubbell*, 530 U.S. at 38, 120 S.Ct. 2037.

[6] The primary policy undergirding the Fifth Amendment privilege against self-incrimination is our country's "fierce 'unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury or contempt' that defined the operation of the Star Chamber, wherein suspects were forced to choose between revealing incriminating private thoughts and forsaking their oath by committing perjury." *Muniz*, 496 U.S. at 596, 110 S.Ct. 2638 (quoting *Doe II*, 487 U.S. at 212, 108 S.Ct. 2341). This being the case, "the definition of 'testimonial' evidence articulated in *Doe* must encompass all responses to questions that, if asked of a sworn suspect during a criminal trial, could place the suspect in the 'cruel trilemma.' " *Id.* at 597, 110 S.Ct. 2638. As the Supreme Court reasoned, "[t]his conclusion is consistent with our recognition in *Doe* that '[t]he vast majority of verbal statements thus will be testimonial' because '[t]here are very few instances in which a verbal statement, either oral or written, will not convey information or assert facts.' " *Id.* Thus, "[w]henever a suspect is asked for a response requiring him to communicate an express or implied assertion of fact or belief, the suspect confronts the 'trilemma' of truth, falsity, or silence, and hence the response (whether based on truth or falsity) contains a testimonial component." *Id.* (footnote omitted).

[7] To invoke the Fifth Amendment privilege against the forced provision of information, a defendant must show (1) the evidence is self-incriminating; (2) the evidence is compelled; and (3) the evidence is testimonial in nature. *Hubbell*, 530 U.S. at 34, 120 S.Ct. 2037. Thus, the government may not force someone to provide an incriminating communication that is "testimonial" in nature. It is only this last requirement — whether the evidence sought to be compelled is testimonial — that is at issue in this appeal.

The United States Supreme Court has not rendered a decision directly addressing whether compelling a person to disclose a computer password is testimonial. In a series of foundational, but somewhat complex, cases, however, the high Court has discussed whether the act of production of documents may be testimonial for purposes of the Fifth Amendment.

***544** In *Fisher*, the high Court examined the question of what acts of production were testimonial in nature. *Fisher* involved consolidated cases in which the Internal Revenue Service ("IRS") sought to obtain voluntarily-prepared documents the defendant taxpayers had given to their attorneys. The IRS issued summonses on the defendant taxpayers' attorneys to produce the documents which included accountants' work papers, copies of the defendant taxpayers' returns, and copies of other reports and correspondence. The attorneys responded that producing the documents would violate their clients' rights against self-incrimination, after which the IRS brought an enforcement action.

Ultimately, the Supreme Court, after rejecting the attorneys' argument that the Fifth Amendment protected them from being compelled to produce the documents, determined that the Fifth Amendment privilege was applicable where defendant taxpayers were required to produce incriminating evidence, and that the act of producing even unprivileged evidence could have communicative aspects rendering it testimonial and entitled to Fifth Amendment protection. *Fisher*, 425 U.S. at 409-10, 96 S.Ct. 1569. Under the facts in *Fisher*, the Court found that the government was not relying on the "truth-telling" of the defendant taxpayers to establish the existence of the documents, their access to them, or their authentication of them, as they had been produced by accountants, and not the defendant taxpayers themselves. *Id.* at 411, 96 S.Ct. 1569. Thus, the Court concluded that the act of producing the subpoenaed documents did not involve self-incriminating testimony.

This analysis served as the basis of the foregone conclusion exception to the Fifth Amendment, discussed below. The Court offered that, because the existence, location, and authenticity of the documents sought was known to the government, the Fifth Amendment privilege was rendered inapplicable. The Court explained that "[t]he existence and

location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers." *Id.* Thus, the Court reasoned that the defendant taxpayers' production of the documents was non-testimonial because the government knew of the existence of the documents, that the defendant taxpayers possessed the documents, and that the government could show their authenticity — not through the use of the defendant taxpayers' minds, but through the testimony of others. Thus, the Fifth Amendment privilege did not apply to the third-party production of documents requested. *Id.* at 414, 96 S.Ct. 1569.

Almost a decade later, in *United States v. Doe*, 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552 (1984) ("*Doe I*"), the Court considered a Fifth Amendment challenge to a subpoena that did not seek specific, known files, but broad categories of general business records of a sole proprietorship. The Court found that, while the contents of the documents were not privileged, the act of producing the business documents could have testimonial aspects and an incriminating effect. The Court opined that the enforcement of the subpoena would compel the defendant to admit that the records existed, that they were in his possession, and that they were authentic, which was sufficient to establish a valid claim of privilege against self-incrimination. While concluding that, by producing the documents, the defendant would relieve the government of the need for authentication, the Court mentioned (although did not apply) the foregone conclusion analysis: "This is not to say that the Government was foreclosed ***545** from rebutting respondent's claim by producing evidence that possession, existence, and authentication were a 'foregone conclusion.' ... In this case, however, the Government failed to make such a showing." *Id.* at 614 n.13, 104 S.Ct. 1237 (citation omitted).

In a subsequent, unrelated, decision in *Doe II*, the high Court considered the legality of an order compelling the target of a grand jury investigation to authorize foreign banks to disclose records of his accounts. 487 U.S. at 202, 108 S.Ct. 2341. The defendant contended that compelling him to sign the bank consent form would provide the government with incriminating records that would otherwise be unavailable, as the court had no power to order foreign banks to produce records. *Id.* at 204, 108 S.Ct. 2341. In rejecting this contention, the high Court indicated that "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Id.* at 210, 108 S.Ct. 2341. The Court reasoned that the written authorization did not have testimonial significance, as it did not communicate any factual assertion, implicit or explicit, or convey any information to the government.

Importantly, for purposes of the issue before us, in response to a dissent by Justice John Paul Stevens, wherein he would have found the Fifth Amendment gave the defendant the right to refuse to sign the consent authorizing access to his bank accounts on the basis that he was compelled to use his mind as a witness against himself, the majority first agreed with the dissent by acknowledging that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Id.* at 210 n.9, 108 S.Ct. 2341. Thus, the Court was unanimous in its holding on this issue. The majority continued, however, that "[w]e simply disagree with the dissent's conclusion that the execution of the consent directive at issue here forced petitioner to express the contents of his mind. *In our view, such compulsion is more like 'be[ing] forced to surrender a key to a strongbox containing incriminating documents' than it is like 'be[ing] compelled to reveal the combination to [petitioner's] wall safe.' "* *Id.* (quoting Stevens, J. dissenting, 487 U.S. at 219, 108 S.Ct. 2341) (emphasis added). Thus, the Court emphasized a clear physical/mental distinction in the context of a foregone conclusion analysis.

Another decade later, the Court in *Hubbell* again spoke to testimonial evidence in the business record context. In that case, Webster Hubbell, as part of the "Whitewater" investigation by Independent Counsel Kenneth Starr during the presidency of Bill Clinton, had pleaded guilty to charges of mail fraud and tax evasion arising out of his billing practices. In the plea agreement, Hubbell promised to provide the Independent Counsel with "full, complete, accurate, and truthful information" about matters relating to the Whitewater investigation. *Hubbell*, 530 U.S. at 30, 120 S.Ct. 2037. Later, while Hubbell was in prison, a grand jury investigating the activities of the Whitewater Development Corporation,

issued a *subpoena* demanding from Hubbell the production of eleven categories of documents. *Id.* at 31, 120 S.Ct. 2037. Hubbell invoked his Fifth Amendment privilege. The Independent Counsel then obtained an order from the federal district court directing Hubbell to comply with the subpoena and granting him immunity against the government's use and derivative use of the compelled testimony. Hubbell then delivered 13,120 pages of the specified documents, after which the grand jury returned an indictment against Hubbell for various wire fraud, mail fraud, and tax crimes. In response, Hubbell asserted ***546** his right against self-incrimination and a violation of the immunity previously granted. The district court dismissed this new indictment, but the United States Court of Appeals for the District of Columbia Circuit reversed, and the Supreme Court granted *certiorari*.

Citing *Fisher*, the Supreme Court reiterated that "a person may be required to produce specific documents even though they contain incriminating assertions of fact or belief because the creation of those documents was not 'compelled' within the meaning of the privilege." *Id.* at 35-36, 120 S.Ct. 2037. Accordingly, the simple fact that the documents contained incriminating evidence did not mean that Hubbell could avoid complying with the subpoena.

Importantly, however, the Court reaffirmed that the very act of producing documents in response to a subpoena may have a compelled testimonial aspect in and of itself: "The 'compelled testimony' that is relevant ... is not to be found in the *contents* of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents." *Id.* at 40, 120 S.Ct. 2037. (emphasis added.) Noting that in *Fisher*, the government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants, the *Hubbell* Court nevertheless found that the government had not shown it had prior knowledge of the existence or whereabouts of the documents produced by Hubbell. Moreover, in rejecting the government's assertion that its possession of the documents was the result of the physical act of producing the documents, the Court explained that it was Hubbell's responses that had provided the government with this information, and that it was "unquestionably necessary for [Hubbell] to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena." *Id.* at 43, 120 S.Ct. 2037. Indeed, in discussing the government's subpoena, which had required Hubbell to provide numerous responses to very broad requests, the Court, harkening back to the *Doe II* distinction, made clear that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." *Id.* at 43, 120 S.Ct. 2037 (citation omitted).

The Court then considered whether the act of producing the records was sufficiently testimonial because the existence and possession of such records was a foregone conclusion. The Court held that "[w]hatever the scope of this 'foregone conclusion' rationale," it did not apply to overcome the testimonial aspects of Hubbell's production of documents because the government did not have prior knowledge of the existence or location of the documents. *Id.* at 44-45, 120 S.Ct. 2037. Thus, the Court concluded that the Fifth Amendment privilege applied, and that Hubbell's act of production of the documents had testimonial aspects, at least regarding the existence and location of the documents, which was not overcome by being a foregone conclusion. *Id.* at 45, 120 S.Ct. 2037.

Finally, the Supreme Court's decision in *Muniz* informs our analysis. Muniz, after failing field sobriety tests, was arrested for driving while intoxicated, and asked various questions when he was being booked. 496 U.S. at 585-86, 110 S.Ct. 2638. Specifically, the defendant was asked, *inter alia*, for identifying information such as his name, address, and date of birth, along with the date of his sixth birthday. The high Court considered the issue of whether the defendant's statements during the booking process were testimonial, and, thus, subject to the Fifth Amendment privilege ***547** against self-incrimination, which was implicated because the defendant had not been provided with *Miranda* warnings. *Id.* at 589-90, 110 S.Ct. 2638. The Court held that descriptions by police of the defendant's speech as "slurred," although incriminating, were not testimonial, but akin to other physical characteristics that do not enjoy Fifth Amendment protection. *Id.* at 590-91, 110 S.Ct. 2638. However, the substance of

the defendant's answers, specifically involving his birthday, were held to be testimonial. The *Muniz* Court emphasized that the Fifth Amendment spares an accused from "having to reveal, directly or indirectly, his knowledge of facts relating him to the offense or from having to share this thoughts and beliefs with the Government." *Id.* at 595, 110 S.Ct. 2638 (citation omitted). Moreover, the Court reasoned that when the defendant was asked about his birthday, he had to admit that he did not know, or answer untruthfully, raising the specter of the "cruel trilemma." *Id.* at 596, 110 S.Ct. 2638. This, according to the Court, was entirely consistent with the Court's prior admonition that "[t]he vast majority of verbal statements thus will be testimonial" because they likely "convey information or assert facts." *Id.*, 496 U.S. at 597, 110 S.Ct. 2638 (quoting *Doe II*, 487 U.S. at 213, 108 S.Ct. 2341). Thus, the testimonial statements revealing the contents of the defendant's own mind disclosed consciousness of fact subject to the privilege.

[8] **[9]** From this foundational law noted above, we can distill certain guiding principles. First, the Supreme Court has made, and continues to make, a distinction between physical production and testimonial production. As made clear by the Court, where the government compels a physical act, such production is not testimonial, and the privilege is not recognized. *See* *Holt*; *Doe II*. Second, an act of production, however, may be testimonial when the act expresses some explicit or implicit statement of fact that certain materials exist, are in the defendant's custody or control, or are authentic. *See* *Fisher*; *Hubbell*. The crux of whether an act of production is testimonial is whether the government compels the defendant to use the "contents of his own mind" in explicitly or implicitly communicating a fact. *See* *Doe II*; *Hubbell*. Third, and broadly speaking, the high Court has recognized that the vast majority of compelled oral statements of facts will be considered testimonial, as they convey information or assert facts. *See* *Muniz*; *Doe II*. This is consistent with the Court's deep concern regarding placing a suspect in the "cruel trilemma" of telling the truth, lying and perjuring himself, or refusing to answer and facing contempt and jail. *Id.* Indeed, the Court has unanimously concluded that "[t]he expression of the contents of an individual's mind" is testimonial communication for purposes of the Fifth Amendment. *Doe II*, 487 U.S. at 210 n.9, 108 S.Ct. 2341.

Finally, and consistent with this historical repulsion of the prospect of compelling a defendant to reveal his or her mental impressions, we find it particularly revealing that, when addressing Justice Stevens's dissent in *Doe II*, the majority of the Court noted that compelling the defendant to sign the bank disclosure forms was more akin to "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it was to "be[ing] compelled to reveal the combination to [petitioner's] wall safe." *Id.*, at 210 n.9, 108 S.Ct. 2341. This is a critical distinction. Consistent with a physical/mental production dichotomy, in conveying the combination to a wall safe, versus surrendering a key to a strongbox, a person must use the "contents of [their] own mind." If one is protected from telling an inquisitor the combination to a wall safe, it is a short ***548** step to conclude that one is protected from telling an inquisitor the password to a computer.

[10] **[11]** Based upon these cases rendered by the United States Supreme Court regarding the scope of the Fifth Amendment, we conclude that compelling the disclosure of a password to a computer, that is, the act of production, is testimonial. Distilled to its essence, the revealing of a computer password is a verbal communication, not merely a physical act that would be nontestimonial in nature. There is no physical manifestation of a password, unlike a handwriting sample, blood draw, or a voice exemplar. As a passcode is necessarily memorized, one cannot reveal a passcode without revealing the contents of one's mind. Indeed, a password to a computer is, by its nature, intentionally personalized and so unique as to accomplish its intended purpose — keeping information contained therein confidential and insulated from discovery. Here, under United States Supreme Court precedent, we find that the Commonwealth is seeking the electronic equivalent to a combination to a wall safe — the passcode to unlock Appellant's computer. The Commonwealth is seeking the password, not as an end, but as a pathway to the files being withheld. As such, the compelled production of the computer's password demands the recall of the contents of Appellant's mind, and the act of production carries with it the implied factual assertions that will be used

to incriminate him. Thus, we hold that compelling Appellant to reveal a password to a computer is testimonial in nature.

Numerous other courts have come to similar conclusions. *See, e.g.*, *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1346 (11th Cir. 2012) (holding "the decryption and production of the hard drives would require the use of the contents of Doe's mind and could not be fairly characterized as a physical act that would be nontestimonial in nature," thus Fifth Amendment protections were triggered); *United States v. Kirschner*, 823 F.Supp.2d 665 (E.D. Mich. 2010) (finding the government could not compel the defendant to reveal his password because this amounted to "testimony" from him which would "requir[e] him to divulge through his mental processes his password"). [6]

[12] This, however, does not end our analysis. As noted above, the United States Supreme Court has found information, otherwise testimonial in nature, to be unprotected where the production of such information is a foregone conclusion. In essence, this judicial toleration of certain compelled testimony renders otherwise privileged testimonial communication non-testimonial. Specifically, under a foregone conclusion analysis, the Supreme Court has reasoned that an act of production does not render communication testimonial where the facts conveyed already are known to the government such that the evidence sought "adds little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569. Thus, what is otherwise testimonial in nature is rendered nontestimonial, as the facts sought to be compelled are a foregone conclusion. As described above, for the exception to apply, the government must establish its knowledge of: (1) the ***549** existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence.

Based upon the United States Supreme Court's jurisprudence surveyed above, it becomes evident that the foregone conclusion gloss on a Fifth Amendment analysis constitutes an extremely limited exception to the Fifth Amendment privilege against self-incrimination. The Supreme Court has spoken to this exception on few occasions over the 40 years since its recognition in *Fisher*, and its application has been considered only in the compulsion of specific existing business or financial records. *See* *Doe I*; *Doe II*; *Hubbell*. Its circumscribed application is for good reason. First, the Fifth Amendment privilege is foundational. Any exception thereto must be necessarily limited in scope and nature. Moreover, business and financial records are a unique category of material that has been subject to compelled production and inspection by the government for over a century. *See*, *e.g.*, *Shapiro v. United States*, 335 U.S. 1, 33, 68 S.Ct. 1375, 92 L.Ed. 1787 (1948). The high Court has never applied or considered the foregone conclusion exception beyond these types of documents. Indeed, it would be a significant expansion of the foregone conclusion rationale to apply it to a defendant's compelled oral or written testimony. As stated by the Supreme Court, "[t]he essence of this basic constitutional principle is 'the requirement that the [s]tate which proposes to convict *and punish* an individual produce the evidence against him by the independent labor of its officers, not by the simple cruel expedient of forcing it from his own lips.' " *Estelle v. Smith*, 451 U.S. 454, 462, 101 S.Ct. 1866, 68 L.Ed.2d 359 (1981) (emphasis original). Broadly circumventing this principle would undercut this foundational right.

The Court's decisions have been ambiguous concerning the breadth of the rationale as well as its value. *See* *Hubbell*, 530 U.S. at 44, 120 S.Ct. 2037 ("Whatever the scope of this 'foregone conclusion' rationale...."); *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569 (finding that to succeed, the government must show that the sought after information is a "foregone conclusion" in that it "adds little or nothing to the sum total of the Government's information.") Thus, generally speaking, the exception to a large degree appears to be intentionally superfluous; hence, the accommodation to the government is of limited value. Accordingly, by definition, application of the foregone conclusion analysis in any given case will not be fatal to the government's prosecution.

Finally, the prohibition of application of the foregone conclusion rationale to areas of compulsion of one's mental processes would be entirely consistent with the Supreme Court decisions, surveyed above, which uniformly protect information arrived at as a result of using one's mind. To broadly read the foregone conclusion rationale otherwise would be to undercut these pronouncements by

the high Court. *See* *Doe II*; *Hubbell*; *Muniz*. When comparing the modest value of this exception to one's significant Fifth Amendment privilege against self-incrimination, we believe circumscribed application of the privilege is in order.

We acknowledge that, at times, constitutional privileges are an impediment to the Commonwealth. Requiring the Commonwealth to do the heavy lifting, indeed, to shoulder the entire load, in building and bringing a criminal case without a defendant's assistance may be inconvenient and even difficult; yet, to apply the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege. Nevertheless, this ***550** constitutional right is firmly grounded in the "realization that the privilege, while sometimes 'a shelter to the guilty,' is often 'a protection to the innocent.' " *Doe II*, 487 U.S. at 213, 108 S.Ct. 2341. Moreover, there are serious questions about applying the foregone conclusion exception to information that manifests through the usage of one's mind. As expressed by the California Court of Appeals in a matter involving an order compelling the production of a weapon allegedly used in a crime:

> Implicit in the prosecution's position, and the court's order, is the argument that independent evidence establishes defendant's possession of the gun at the time of the offense and after.... The Commonwealth does not simply assert that the evidence to be gained by production is here inconsequential or nonincriminating; rather it says that the evidence is unworthy of Fifth Amendment protection because it merely enhances other persuasive evidence obtained without the defendant's help. *The Commonwealth's argument is indeed curious. It is as if we were asked to rule that a confession could be coerced from an accused as soon as the government announced (or was able to show) that [in] a future trial it could produce enough independent evidence to get past a motion for a directed verdict of acquittal.*

Goldsmith v. Superior Court, 152 Cal. App. 3d 76, 87 n.12, 199 Cal.Rptr. 366 (1984) (quotations and citations omitted) (emphasis added).

We appreciate the significant and ever-increasing difficulties faced by law enforcement in light of rapidly changing technology, including encryption, to obtain evidence. However, unlike the documentary requests under the foregone conclusion rationale, or demands for physical evidence such as blood, or handwriting or voice exemplars, information in one's mind to "unlock the safe" to potentially incriminating information does not easily fall within this exception.[7] Indeed, we conclude the compulsion of a password to a computer cannot fit within this exception.

[13] **[14]** Thus, we hold that the compelled recollection of Appellant's password is testimonial in nature, and, consequently, privileged under the Fifth Amendment to the United States Constitution. Furthermore, until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application, and, consistent with its teachings in other decisions, believe the exception to be inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer.[8, 9, 10]

***552** For the above-stated reasons, we reverse the order of the Superior Court and remand the matter to the Superior Court, for remand to the trial court, for proceedings consistent with our Opinion.

Jurisdiction relinquished.

Chief Justice Saylor and Justices Donohue and Wecht join the opinion.

Justice Baer files a dissenting opinion in which Justice Dougherty and Mundy join.

JUSTICE BAER, Dissenting

I respectfully dissent from the majority's decision, which holds that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination does not apply to the compelled disclosure of a computer password because the password manifests from one's mind. I further disagree with the majority's alternative holding that if the foregone conclusion exception would apply under the circumstances presented, the Commonwealth ***553** failed to satisfy the requisites thereof because it did not establish that it had knowledge of the various files stored on Appellant's computer hard drive in addition to the single previously identified file that contained child pornography.

Preliminarily, I acknowledge that the issue presented in this appeal is one of first impression, with which courts across the nation have struggled. *See generally* Marjorie A. Shields, *Fifth Amendment Privilege Against Self-Incrimination as Applied to Compelled Disclosure of Password or Production of Otherwise Encrypted Electronically Stored Data*, 84 A.L.R. 6th 251 (2019) (compiling Fifth Amendment cases involving "compelled disclosure of an individual's password, means of decryption, or unencrypted copy of electronically stored data"). Upon review of the High Court's seminal decision in *Fisher v. United States*, 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976), which first recognized the foregone conclusion exception, and its progeny, I would hold that the foregone conclusion analysis applies to the compelled disclosure of a password to an electronic device, which the Commonwealth has seized pursuant to a warrant.

My analysis focuses on the compulsion order, which directed Appellant to "supply the Commonwealth with any and all passwords used to access" a specific desktop computer and hard drive seized from his residence. Trial Court Order, 6/30/2016. In my view, this order compels an act of production that has testimonial aspects in that it conveys, as a factual matter, that Appellant has access to the particular computer seized by the Commonwealth pursuant to a warrant, and that he has possession and control over the password that will decrypt the encrypted files stored on that computer. As discussed in detail *infra*, because the Commonwealth was already aware of these facts based upon its own investigation and Appellant's candid discussion with government agents, the password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination, and may be constitutionally compelled. Notably, critical to my position is the recognition that this case does not involve a Fourth Amendment challenge based upon Appellant's privacy rights in his encrypted computer files but, rather, solely a challenge to the compelled disclosure of his password based upon his Fifth Amendment privilege against self-incrimination.

I. The Fifth Amendment As Applied To Acts of Production

As noted by the majority, the Fifth Amendment provides, in relevant part, that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend V. Courts have interpreted the privilege as protecting a citizen "from being compelled to testify against himself, or otherwise provide the State with evidence of a testimonial or communicative nature." *Pennsylvania v. Muniz*, 496 U.S. 582, 588-89, 110 S.Ct. 2638, 110 L.Ed.2d 528 (1990) (citations omitted). The Fifth Amendment "does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating." *Fisher*, 425 U.S. at 408, 96 S.Ct. 1569. To be testimonial, a communication must either "explicitly or implicitly ... relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988).

In *Fisher*, the High Court explained that in addition to traditional testimony, acts of production may implicate the Fifth Amendment because the "act of producing evidence in response to a subpoena nevertheless ***554** has communicative aspects of its own, wholly aside from the contents of the papers produced." 425 U.S. at 410, 96 S.Ct. 1569. The Court explained that compliance with a request for evidence "tacitly concedes" the existence of the evidence, possession or control of the evidence by the individual, and the belief that the evidence is, in fact, the item requested by the government. *Id.* Whether the act of production has a testimonial aspect sufficient to warrant Fifth Amendment protection "depends on the facts and circumstances of particular cases or classes thereof." *Id.*

It is well established that some compelled acts have no testimonial aspects and, thus, no Fifth Amendment protection, as the acts do not require an accused to relate a factual assertion, disclose knowledge, or "speak his guilt." *Doe v. United States*, 487 U.S. 201, at 210-11, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988). These include, for example, furnishing a blood sample, providing a voice or handwriting exemplar, or standing in a line-up. *Id.* (collecting cases). Other compelled acts, such as the production of certain subpoenaed documents, may have a compelled testimonial aspect warranting Fifth Amendment protection where the government's demand is akin to a "detailed written interrogatory or a series of questions at a discovery deposition," characterized as a "fishing expedition." *United States v. Hubbell*, 530 U.S. 27, 36, 41-42, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000). [1]

Finding that an act of production has testimonial aspects, however, does not necessarily mean that the Fifth Amendment privilege precludes compulsion of the evidence sought. As the majority cogently observes, the United States Supreme Court has found that information, otherwise testimonial in nature, is unprotected where the production of such information is a foregone conclusion. Majority Opinion at 548. The foregone conclusion exception applies where the existence and location of the compelled evidence "adds little or nothing to the sum total of the government's information." *Fisher*, 425 U.S. at 410, 96 S.Ct. 1569. The High Court in *Fisher* explained that a foregone conclusion exists where "[t]he question is not of testimony but of surrender." *Id.* at 411 (quoting *In re Harris*, 221 U.S. 274, 279, 31 S.Ct. 557, 55 L.Ed. 732 (1911)). Thus, as the majority recognizes, "what is otherwise testimonial in nature is rendered non-testimonial, as the facts sought to be compelled are a foregone conclusion." Majority Opinion at 548.

In my opinion, the compulsion of Appellant's password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in *Fisher*. [2] *See* Trial Court Order, 6/20/2016 (directing Appellant to "supply the Commonwealth with any and all passwords used to access the HP Envy 700 desktop computer with serial # MXX4100000042C containing Seagate 2 TB hard drive with serial ***555** # Z4Z1AAAEFM"). An order compelling disclosure of the password, here a 64-character password, has testimonial attributes, not in the characters themselves, but in the conveyance of information establishing that the password exists, that Appellant has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files. The Commonwealth is not seeking the 64-character password as an investigative tool, as occurred in *Hubbell*, where the government compelled the disclosure of thousands of documents to engage in a fishing expedition to discover evidence of the defendant's guilt. To the contrary, the Commonwealth already possesses evidence of Appellant's guilt, which it set forth in an affidavit of probable cause to obtain a warrant to search Appellant's computer. Stated differently, the Commonwealth is not asking Appellant to "speak his guilt," but merely to allow the government to execute a warrant that it lawfully obtained.

Because I view the compulsion order as requiring the "surrender" of Appellant's password to decrypt his computer files, I would apply *Fisher's* act-of-production test. The majority declines to apply the foregone conclusion rationale to the compelled disclosure of Appellant's computer password, finding that to do so would constitute a "compulsion of one's mental processes" in violation of the Fifth Amendment. Majority Opinion at 549. There is appeal to this conclusion, as requiring Appellant to supply his password involves some mental effort in recalling the 64 characters used to encrypt the computer files. [3] However, one would expend similar mental effort when engaging in virtually any other act of production, such as the disclosure of business or financial records, as the individual must retrieve the contents of his mind to recall the documents' location before disclosing them to the government. Under the majority's reasoning, the compelled production of documents would be tantamount to placing the defendant on the stand and requiring him to testify as to the location of the documents sought. The mere fact that Appellant is required to think in order to complete the act of production, in my view, does not immunize that act of production from the foregone conclusion rationale.

II. Application of the Foregone Conclusion Test

Having determined that the foregone conclusion rationale may potentially apply to cases involving the compelled disclosure of a computer password, significant questions arise regarding how to administer the three-part test. As observed by the majority, to satisfy the foregone conclusion exception to the Fifth Amendment privilege, "the government must establish its knowledge of: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence." Majority Opinion at 549.

As an alternative holding, the majority opines that if the Court were to find that the foregone conclusion exception could ***556** apply to the compelled disclosure of a password, it would apply *Fisher's* act-of-production test to the computer files stored on Appellant's computer. *See* Majority Opinion at 551 n.9 (holding that "because the Commonwealth has failed to establish that its search is limited to the single previously identified file [containing child pornography], and has not asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to the Commonwealth upon Appellant's compelled disclosure of the password, we find the Commonwealth has not satisfied the foregone conclusion exception").

Respectfully, it is my position that the foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating, testimonial evidence. *See* *Doe v. United States (In re Grand Jury Subpoena)*, 383 F.3d 905, 910 (9th Cir. 2004) (providing that "it is the government's knowledge of the existence and possession of the actual documents [subpoenaed by the government], not the information contained therein, that is central to the foregone conclusion inquiry"). This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection. The High Court in *Fisher* made this point clear by stating, "We cannot cut the Fifth Amendment loose from the moorings of its language, and make it serve as a general protector of privacy – a word not mentioned in its text and a concept directly addressed in the *Fourth Amendment*." 425 U.S. at 401, 96 S.Ct. 1569 (quoting *United States v. Nobles*, 422 U.S. 225, 233 n.7, 95 S.Ct. 2160, 45 L.Ed.2d 141 (1975) (emphasis in original)).

Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone conclusion exception by focusing only on the compelled evidence itself, *i.e.*, the computer password, and not the decrypted files that the password would ultimately reveal. *See, e.g.*, *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 n.7 (3rd Cir. 2017) ("[A] very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the device is 'I, John Doe, know the password for these devices.' "); *State v. Johnson*, 576 S.W.3d 205, 277 (Mo. Ct. App. 2019) (holding that the focus of the foregone conclusion exception as applied to the compelled entering of one's cell phone passcode is the extent of the government's knowledge about the existence of the passcode, his possession and control of the phone's passcode, and the passcode's authenticity); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 615 (Mass. 2014) (holding that the compelled decryption of computer files satisfied the elements of the foregone conclusion exception because the government already knew the implicit facts conveyed ***557** through the act of entering the encryption key, such as the defendant's ownership and control of the computers, knowledge of the encryption, and knowledge of the encryption key); *State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. 2018) (holding that whether the government was aware of the possible contents of

the defendant's cell phones was immaterial "because the order requires defendant to disclose the passcodes, not the contents of the phones unlocked by those passcodes").

III. Application to Future Cases

Finally, it is my belief that the majority's approach could render inconsistent results as the determination of whether there was a Fifth Amendment violation in compelled decryption cases could depend upon the type of password that the individual employed to protect his encrypted files. For example, according to the majority, if the accused used a multi-character password to encrypt computer files, as occurred here, and the government compelled the individual to supply the password, a Fifth Amendment violation would result because the password manifests through the use of one's mind. Majority Opinion at 550. However, if the individual employed a biometric password, such as facial recognition or a fingerprint, the majority's analysis would arguably lose its force. Under those circumstances, the individual is not using the contents of his mind but, rather, is performing a compelled act of placing his finger or face in the appropriate position to decrypt the files. Additional questions arise when the act of compulsion is not the disclosure of the password itself, but the entry of the password into the computer. It is my position that all these examples constitute acts of production that would be subject to the foregone conclusion rationale in the appropriate case. The same legal analysis should apply to the underlying act of compelled decryption of digital information when the government has obtained a warrant to search the digital container. To hold to the contrary would create an entire class of evidence, encrypted computer files, that is impervious to governmental search. This could potentially alter the balance of power between governmental authorities and criminals, and render law enforcement incapable of accessing relevant evidence.

IV. Conclusion

Accordingly, I would hold that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination applies to render non-testimonial Appellant's compelled act of producing the password to his encrypted, lawfully seized computer. As the majority observes, when government agents attempted to execute the search warrant, Appellant voluntarily informed them that he was the sole user of the computer, that he used hardwired Internet services that were password protected, that only he knew the password to decrypt his computer files, and that he would never disclose the password, as it would incriminate him.

In addition to Appellant's voluntary disclosure to government agents that he knew the password that would decrypt the files stored on the computer that the Commonwealth lawfully seized, there is ample circumstantial evidence demonstrating Appellant's knowledge of the password. Before seizing the computer, government agents conducted an investigation of the "eMule" peer-to-peer network to identify internet users sharing child pornography. Agents made a direct connection with a device that used a particular IP address over the eMule network, which agents subsequently linked to Appellant. Using this direct connection, agents downloaded one child pornography video file from Appellant's IP ***558** address. Affidavit of Probable Cause, 10/20/2015, at 7. Based on this download, the agents obtained the search warrant for Appellant's residence. *Id.* at 9.

Upon executing the search warrant, agents seized a single desktop computer, as that was the only device connected to Appellant's IP address. N.T., 1/14/2016, at 33. Forensic analysis revealed that Appellant's IP address had used the eMule file-sharing program on 23 dates from July 4, 2015, through October 19, 2015, to share files indicative of child pornography. Affidavit of Probable Cause, 10/20/2015, at 10-11; N.T., 1/14/2016, at 29. Agent Daniel Block explained that the government reached this conclusion based upon the "SHA value," which is essentially a "digital fingerprint" that corresponds with known SHA values of child pornography files. N.T., 1/14/2016, at 20. This evidence demonstrates that Appellant possessed the password to decrypt files on the computer seized by the Commonwealth, as his own words established that he was the sole user of the computer and forensic analysis demonstrated that he was accessing the encrypted files on the days leading up to his arrest.

Under these circumstances, it was a foregone conclusion that the government knew that the password to decrypt the files existed, that Appellant had exclusive control over the password, and that the password was authentic.[4] Accordingly, the testimonial aspects of the password

disclosure "adds little or nothing to the sum total of the government's information." *Fisher*, 425 U.S. at 410, 96 S.Ct. 1569. Thus, I would find that the compelled disclosure of Appellant's password does not violate his Fifth Amendment privilege against self-incrimination.

Justices Dougherty and Mundy join this dissenting opinion.

All Citations

220 A.3d 534

Footnotes

1 IP addresses identify computers on the Internet, enabling data transmitted from other computers to reach them. *National Cable & Telecomm. Ass'n v. Brand X Internet Services*, 545 U.S. 967, 987 n.1, 125 S.Ct. 2688, 162 L.Ed.2d 820 (2005).

2 The Dell computer seized in this search is not the subject of the Commonwealth's motion to compel a password at issue in this matter.

3 The Superior Court initially considered whether it had jurisdiction to entertain the trial court's interlocutory order on appeal. In sum, the court determined that the order satisfied each of the requirements of the collateral order doctrine as set forth in Pa.R.A.P. 313(b). The parties do not question this determination on appeal. While the matter is jurisdictional in nature, and, thus, non-waivable and subject to *sua sponte* consideration by this Court, *Commonwealth v. Shearer*, 584 Pa. 134, 882 A.2d 462, 465 n.4 (2005), we do not disagree with the Superior Court's analysis.

4 Appellant also argues an independent basis for protection against disclosure of the password under Article I, Section 9 of the Pennsylvania Constitution. Appellant engages in a detailed analysis, offering that the text of the Pennsylvania charter as well as the history of the provision suggests broader protections thereunder. The Commonwealth strongly asserts throughout its brief that Appellant has waived his state constitutional law claim, and maintains that, in any event, such claim has no merit, stressing the numerous decisions in which our Court has indicated the rights under the sister sections are coterminous. As we resolve this matter on federal Constitutional grounds, we need not address the Commonwealth's waiver contention or Appellant's underlying assertion of the recognition of greater rights under the Pennsylvania Constitution.

5 *Amicus* for Appellant, the Electronic Frontier Foundation, stresses that compulsion to disclose a computer password subjects an individual to a "cruel trilemma" — to choose between providing the allegedly incriminating information; lying about the purported inability to do so; or refusing to cooperate and be held in contempt. According to *Amicus*, the privilege was designed to prevent this trilemma. In a joint *amicus* brief in support of the Commonwealth, various states provide an interesting history of modern encryption, press the troubling consequences of Appellant's position — including the altering of the balance of power, rendering law enforcement incapable of accessing large amounts of relevant evidence — and warn that adopting Appellant's position could result in less privacy, not more, in the form of draconian anti-privacy legislation.

6 In this regard, we reject the Commonwealth's seemingly newly-raised contention that there might be a slip of paper containing the password which would be covered by the trial court's order, Commonwealth's Brief at 1. There has been no suggestion in the proceedings in this matter that such a paper exists, and this case has proceeded under the assumption of an oral or written compulsion of Appellant to provide the password.

7 Because we are dealing with a motion to require an individual to recall and disclose a memorized password to a computer, in essence, revealing the contents of one's own mind, we need not address the related, but

distinct, area involving biometric features like fingerprints, thumbprints, iris scanning, and facial recognition, or whether the foregone conclusion rationale would be appropriate in these circumstances. The dissent, however, makes much of the potential for inconsistent results in "future cases" involving these types of biometric passwords. Dissenting Opinion at 556–57. Yet, not only are these communications not before our Court, it is the United States Supreme Court that long ago has created the dichotomy between physical and mental communication. *See* *Holt*, 218 U.S. at 252-53, 31 S.Ct. 2 ("the prohibition of compelling a man in criminal court to be witness against himself is a prohibition of the use of physical or moral compulsion to extort communications from him, not an exclusion of his body as evidence when it may be material."); *Doe II*, 487 U.S. at 210 n.9, 108 S.Ct. 2341. (finding the expression "more like 'be[ing] forced to surrender a key to a strong box containing incriminating documents' than it is like be[ing] compelled to reveal the combination to [petitioner's] wall safe.").

8 After oral argument, we granted Appellant's Motion for Leave to File Post-Argument Submission and now grant the Commonwealth's Motion for Leave to File Response to Post-Argument Submission with respect to this issue. However, as we resolve this matter in favor of Appellant exclusively under the Fifth Amendment to the United States Constitution, we need not address his additional contention that the Pennsylvania Constitution provides greater protections than the federal charter.

9 Even if we were to find that the foregone conclusion exception could apply to the compulsion to reveal a computer password, we nevertheless would conclude that the Commonwealth has not satisfied the requirements of the exception in this matter. As noted above, for the compelled evidence to fall within the exception, the Commonwealth must establish: (1) the existence of the evidence demanded; (2) the possession or control of the evidence by the defendant; and (3) the authenticity of the evidence.

As the Superior Court recounted below, there is a high probability that child pornography exists on Appellant's computer, as evidenced by: Appellant's IP address utilizing a peer-to-peer file sharing network to share videos depicting child pornography; the fact that the sole computer seized had hardwire Internet; and the fact that Appellant "implied as to the nefarious contents of the computer on numerous occasions." *Davis*, 176 A.3d at 876. However, for the exception to apply, the facts sought to be compelled must be already known to the Commonwealth. It is not merely access to the computer that the Commonwealth seeks to obtain through compelling Appellant to divulge his computer password, but all of the files on Appellant's computer. The password is merely a means to get to the computer's contents. While it is conceivable, and indeed, likely, that a single video containing child pornography (as previously viewed by the OAG agents) may be on the computer, the compelled revelation of the password could lead to a trove of a presently unknown number of files. Indeed, the record establishes that the entire hard drive of the computer was encrypted and "there was no data that could be read without opening the TrueCrypt volume." N.T. Hearing, 1/14/16, at 46. Agent Cook could only confirm that there was "Windows on the computer and the TrueCrypt," and he had no knowledge of any specific files other than the operating system files. *Id.* at 50-51.

In sum, because the Commonwealth has failed to establish that its search is limited to the single previously identified file, and has not asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to the Commonwealth upon Appellant's compelled disclosure of the password, we find the Commonwealth has not satisfied the foregone conclusion exception.

10 The dissent agrees that the information the Commonwealth seeks to compel is testimonial in nature. Dissenting Opinion at 553. The dissent, however, contends that, in these circumstances, governmentally forced testimony involving a computer password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination. Respectfully, the dissent's position is unpersuasive.

Initially, the dissent broadly dilutes the historic and contextual underpinnings of the application of the foregone conclusion exception, which, as noted above, constitutes an extremely narrow exception. Indeed, the high

Court has found the exception to have been satisfied only one time in the over 40 years since it was created; moreover, the exception's provenance is exclusively in cases involving subpoenaed paper documents — never in the context of oral testimony. Thus, application of the foregone conclusion exception outside of this narrow context is dubious at best. For that reason, we will not apply the foregone conclusion exclusion in the absence express guidance from the high Court.

Furthermore, the dissent adopts a minority interpretation of that exception which focuses on the password itself, rather than on the underlying files. Yet, even employing this password-centric approach, the circumstances, *sub judice*, do not satisfy the foregone conclusion doctrine. As set forth above, and noted by the dissent, to satisfy the foregone conclusion doctrine, the government must establish, *inter alia*, the authenticity of the evidence, *i.e.*, the password, with reasonable particularity. Of course, here, the Commonwealth cannot establish with reasonable particularity the authenticity of the password. Rather, authenticity may only be established after the information — the password — is turned over to the Commonwealth. The dissent is turning the authenticity requirement on its head, allowing the Commonwealth to satisfy its burden by, in essence, saying, "Turn over the facts we want, and we will tell you if it is authentic or not." Of course, this is not how the exception works. Rather, the burden is on the Commonwealth to establish its independent knowledge of, *inter alia*, the authenticity of the documents or evidence sought, *before* that information is properly compelled over a defendant's Fifth Amendment assertion of his or her right against self-incrimination. *Fisher*. Indeed, the dissent's password-centric logic was recently rejected by the Third District Court of Appeal of Florida in *Pollard v. State*, —— So.3d ——, 2019 WL 2528776 (Fla. Dist. Ct. App. June 20, 2019), where the court forcefully explained the logical shortcomings of this approach:

> [The foregone conclusion exception's] three-part test is tautological when applied to passwords because all password-protected cellphones have an "authentic" password, making the [*State v. Stahl*, 206 So.3d 124 (Fla. Dist. Ct. App. 2016)] test somewhat circular. In this regard, the court in *Stahl* said that '[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic. 206 So.3d at 136, which begs the question of whether sufficient evidence established that the passcode is authentic *before* it had been compelled and used successfully. The state must have sufficient proof of authenticity *before* it can compel the password's production; simply because a compelled password unlocks a cellphone after the fact doesn't make it authentic ex ante. To do otherwise is "like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." [citing *Hubbell*].

Pollard, —— So.3d at ——, 2019 WL 2528776 at *4.

Related thereto, and as noted above, the United States Supreme Court has limited the application of this narrow exception to Fifth Amendment protections to contexts where the facts sought "add[ ] little or nothing to the sum total of the Government's information." *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569. Nothing could be farther from the case here, as the password which the Commonwealth seeks to compel could disclose a vast swath of files of which the Commonwealth, it appears, currently has no knowledge.

Finally, and directly related thereto, the dissent gives scant attention or significance to the Supreme Court's consistent approach that revealing the contents of one's mind is protected by the Fifth Amendment. This unmistakable overarching jurisprudential theme has been consistently applied in all of the high Court's decisions in this area. *Doe II*; *Hubbell*; *Muniz*. Indeed, the dissent speaks volumes by reducing to a footnote, without analysis, its mention of the United States Supreme Court's distinction between the production of documents and the forced compulsion of mental processes such as the combination to a safe, which, in the high Court's view, plainly violates the Fifth Amendment. *Doe II*; *Hubbell*. Simply stated,

there is no meaningful distinction between the government compelling a suspect to provide the combination to access a safe, and the government forcing one to disclose a password to access a computer. Here, it is unquestionably necessary for Appellant to make use of "the contents of his own mind" in providing the password. In essence, the dissent's approach is effectively the same as compelling Appellant to affirm that, "I know the password, this is my computer, I have knowledge of the existence and location of incriminating files, and I have the capability to decrypt the files." To accept the dissent's position is to embrace a stance contrary to the foundational privilege against the probing of an individual's mind to compel communication that is incriminating.

1 In *Hubbell*, the Supreme Court held that the act of producing thousands of subpoenaed documents had testimonial aspects in that the act of production communicated information about the documents' existence, custody, and authenticity. The High Court concluded that, unlike in *Fisher*, the government had shown no prior knowledge of either the existence or whereabouts of the documents, thus, the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination did not apply.

2 The summonses in *Fisher* directed the defendants' attorneys to produce documents relating to the defendants' tax returns in connection with an investigation into possible civil or criminal liability under federal income tax laws.

3 I recognize that the majority's conclusion in this regard finds support in commentary found in federal cases, suggesting a constitutional distinction between the compelled surrender of a key and the compelled disclosure of a combination to a wall safe. For the reasons set forth herein, however, I do not find any such distinction dispositive in a case involving current day technology relating to the compelled disclosure of a password to encrypted digital information, where the Commonwealth has a warrant to search the digital container. Only the High Court can make the final determination in this regard for purposes of the Fifth Amendment, and the present case offers an attractive vehicle by which the Court could do so.

4 I would hold that the authenticity prong of the foregone conclusion exception requires the government to establish that the compelled information is what it purports to be, *i.e.*, a password that will decrypt the computer files on Appellant's hard drive. The Commonwealth may prove the authenticity of the password by Appellant's own voluntary statements. *See* Pa.R.E. 901(b) (providing that the requirement of authenticating an item of evidence may be satisfied by testimony of a witness with knowledge that an item is what it is claimed to be). Here, Appellant's voluntary statements establish that the password would decrypt the files on his hard drive; thus, I would conclude that the authenticity requirement has been satisfied.

End of Document

No. 00-0000

IN THE SUPREME COURT OF THE UNITED STATES

PENNSYLVANIA

Petitioner

v.

JOSEPH J. DAVIS

Respondent

ON PETITION FOR WRIT OF *CERTIORARI* TO THE SUPREME COURT OF PENNSYLVANIA

PETITION FOR WRIT OF *CERTIORARI*

JOSH SHAPIRO
Attorney General
Commonwealth of Pennsylvania

JENNIFER C. SELBER
Executive Deputy Attorney General
Director, Criminal Law Division

JAMES P. BARKER
Chief Deputy Attorney General
Appeals & Legal Services Section

WILLIAM R. STOYCOS *
Senior Deputy Attorney General
Counsel of Record

Office of Attorney General
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-6348

QUESTIONS PRESENTED

For more than forty years, courts have allowed law enforcement authorities to compel an individual to disclose information when the information adds little or nothing to the sum total of information already possessed by the government and is a foregone conclusion. During that same time, advances in technology have changed the ways information may be stored to include electronic media as opposed to paper documents, which were the exclusive manner of keeping business records in former days. Concurrent with the development of electronic media has been the creation of the means of making information inaccessible through virtually unbreakable encryption technology. Both developments have given rise to criminal activity that takes advantage of new technology and an urgent need for law enforcement to access data and information kept beyond its lawful reach by the encryption technology. This Court has not considered the foregone conclusion doctrine in the context of electronic media and encryption.

1. Does the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination established in *Fisher v. United States*, 425 U.S. 391 (1976) and its progeny apply to the compelled production of passwords to encrypted electronic devices when the government has seized a device pursuant to a valid search warrant and has independent knowledge that the password exists, is known by

the suspect, and will decrypt the device, such that the compelled information itself lacks testimonial significance and any testimony implied by the compelled act is already known by the government, not in issue, and adds little or nothing to the sum total of the government's information?

2. Assuming the foregone conclusion exception applies, what is the government's burden of proof to support the exception, and more specifically, must the government demonstrate knowledge relating solely to the password sought or must it also demonstrate knowledge of the contents of the encrypted device for which a judge has already authorized a search?

PARTIES TO THE PROCEEDING

All parties appear in the caption of the case on the cover page.

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

Page(s)

Cases

Constitutional Provisions and Statutes

Rules

Other Authorities

OPINIONS BELOW

The opinion of the four-justice majority of the Supreme Court of Pennsylvania reversing the decision of the Superior Court of Pennsylvania and holding that the compelled production by Davis to the government of the digital password to his encrypted, lawfully-seized computer violated the Fifth Amendment to the Constitution of the United States is published at *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), and is reprinted at Pet. App. 1a. The opinion of the three-justice minority of the state Supreme Court dissenting from the majority's decision also is published at *Commonwealth v. Davis*, 220 A.3d 534 (Pa. 2019), and is reprinted at Pet. App. 1b. The unanimous opinion and order of the three-judge panel of the Superior Court of Pennsylvania holding that the foregone conclusion doctrine applies to render Davis' compelled act of production of the password to his encrypted, lawfully-seized computer non-testimonial and therefore not violative of the Fifth Amendment is published at *Commonwealth v. Davis*, 176 A.3d 869 (Pa. Super. 2017), and is reprinted at Pet. App. 1c. The opinion of the Court of Common Pleas of Luzerne County, Pennsylvania, holding that the foregone conclusion doctrine applies to render Davis' compelled act of production of the password to his encrypted, lawfully-seized computer non-testimonial and not violative of the Fifth Amendment is unpublished and is reprinted at Pet. App. 1d.

STATEMENT OF JURISDICTION

On November 20, 2019, a four-justice majority of the Supreme Court of Pennsylvania ruled that "until the United States Supreme Court holds otherwise," the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination established in *Fisher v. United States*, 425 U.S. 391 (1976) and its progeny does not apply in the context of compelled production of digital passwords to encrypted electronic devices seized pursuant to a judicially-authorized search warrant and such compelled acts of production violate the Fifth Amendment. The jurisdiction of this Court is invoked under 28 U.S.C. § 1257(a).

CONSTITUTIONAL PROVISION INVOLVED

> No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; *nor shall be compelled in any criminal case to be a witness against himself,* nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

U.S.C.A. Const. Amend. V (emphasis added).

STATEMENT OF THE CASE

In July 2014, agents from the Pennsylvania Office of Attorney General ("OAG") conducted an undercover investigation into the possession and distribution of child pornography via the internet. The investigation focused on individuals using an online, peer-to-peer electronic file-sharing network known as "eMule." More specifically, agents determined that a computer at a specific internet protocol ("IP") address was used to share child pornography. Agents used computers running specially-designed, investigative software to make a direct connection to the device at that IP address and downloaded an electronic file believed to be child pornography that was transferred from the device. Thereafter, Special Agent Justin Leri viewed the file and determined that it was a video depicting a prepubescent child engaging in unlawful sexual activity.

Agent Leri subsequently determined that the IP address was registered to Comcast Cable Company ("Comcast"). OAG agents then obtained and served upon Comcast a court order directing the disclosure to law enforcement of the subscriber information related to that particular IP address, with which Comcast complied. As a result, OAG agents determined that the subscriber for the IP address was the Respondent, Joseph Davis.

Agent Leri thereafter obtained a warrant from a local magistrate judge to search Davis' residence. Agents executed the warrant on September 9, 2014. The only occupant, Davis, acknowledged understanding and voluntarily waived his *Miranda* rights, admitted to being the sole user of the Dell computer system found in the

residence, and denied the existence of any child pornography on the computer. He also stated that he had previously been arrested for child pornography offenses and "did my time for that."

Agents seized the Dell computer and two DVDs. Agents from the OAG Computer Forensics Unit ("CFU") attempted without success to analyze the computer system in the residence. The computer had no readable data. The search was ended and no arrest was made. Agents subsequently learned from Davis that he wiped his computer clean with a DVD known as "DBAN" just days prior to the execution of the search warrant.

Fifteen months later, on October 4, 2015, OAG agents conducted another undercover investigation of persons using the eMule network to share child pornography. At that time, agents observed that a specific IP address was distributing electronic files of child pornography. A direct connection was made from OAG computers using investigative software to the IP address and agents downloaded one electronic file transferred to them that contained suspected child pornography. Special Agent Daniel Block viewed the file and determined that the file was a video of a prepubescent child engaging in prohibited sexual activity.

Agent Block subsequently determined that the IP address was registered to Comcast. He sent an administrative subpoena to Comcast directing the disclosure of the subscriber information related to that particular IP address, with which Comcast complied. As a result, OAG agents determined that the subscriber for the IP address was the same Joseph Davis.

OAG agents thereafter obtained a warrant from a court to search that residence, which the agents executed on October 20, 2015. Davis, the sole occupant of the residence, voluntarily waived his *Miranda* rights and agreed to speak with the agents. He informed the agents that: (1) he had lived alone in the apartment since 2006; (2) he had not had any long-term guests during his time at the residence; (3) he utilized Comcast internet and had done so on and off for many years; (4) he did not have Wi-Fi and only used hardwired internet services so that no one could steal his Wi-Fi; (5) he was the sole user of the desktop computer in the residence; and (6) the desktop computer was password-protected and only he knew the password allowing access to the computer (R. at 39a). Agent Block asked Davis to give him (Agent Block) the password and Davis refused to do so.

Davis also informed the agents that: (1) he watched pornography on the computer, which is legal; (2) he was previously arrested for child pornography; (3) child pornography is legal in other countries like Japan and the Czech Republic; (4) he did not understand why it is illegal here; and (5) what people do in the privacy of their own homes is their own business.

Agents located the desktop computer, an HP Envy 700 ("the computer"), in the home. CFU agents attempted to analyze it, but Special Agent Braden Cook determined that the computer was encrypted via software known as "TrueCrypt" that prevented OAG agents from accessing the contents of the computer. In order for the computer to "boot" into the Windows operating system, a user-created password must be input into the "TrueCrypt" volume. According to Agent Cook, "when the computer

power is [turned] on, it goes directly to a screen that says, 'TrueCrypt Boot Version 7.1' and it requires a password to be entered in order to have the computer function."[1]

Following his arrest, Davis told the agents his computer was encrypted with "TrueCrypt" and he claimed he could not remember the password. He also told Agent Block that "even if he could ... it would be like, quoting him exactly, putting a gun to his head and pulling the trigger." Thereafter, when Agent Block asked him if he remembered the password, Davis said "he would die in jail before ever remembering the password."

About an hour or two after the agents entered Davis' residence, following his arrest, agents transported him to court for an arraignment. During the transport, Davis voluntarily spoke with Agent Block. According to Agent Block:

---

[1] "Encryption technology allows a person to transform plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process. Only those who possess a corresponding 'key' can return the information into its original form, i.e. decrypt that information. Encrypted information remains on the device in which it is stored, but exists only in its transformed, unintelligible format. Although encryption may be used to hide illegal material, it also assists individuals and businesses in lawfully safeguarding the privacy and security of information. Many new devices include encryption tools as standard features, and many federal and state laws either require or encourage encryption to protect sensitive information." *United States v. Apple MacPro Computer,* 851 F.3d 238, 242 n. 1 (3rd Cir. 2017).

> While we were in transport to his arraignment, Mr. Davis was talking about gay x-rated movies he likes to watch and stated he liked 10, 11, 12, and 13 year olds, referring to them as "a perfectly ripe apple." He further stated he didn't see what the big deal was. He's not taking kids and raping them. There's nothing wrong with watching kids that age in the privacy of your own home ...
>
> ...Then I asked if he would give the password [to me]. He replied, "It's 64 characters and why would I give that to you? We both know what's on there [the computer]. It's only going to hurt me. No [expletive] way I'm going to give it to you." Then he made several jokes referring to the password but did not give us the password.

OAG agents observed that the IP address belonging to Davis was active on the peer-to-peer file sharing network eMule twenty-five times during the year 2015. The investigation determined that, on those occasions, the file-sharing had qualities that were indicative of child pornography.

On December 17, 2015, the Commonwealth of Pennsylvania ("the Commonwealth") filed a pretrial motion in the Luzerne County Court of Common Pleas ("the trial court") seeking an order compelling Davis to provide OAG agents with the password to the encryption software on his computer so that they could execute the search warrant. In support of the motion, the Commonwealth argued that Davis' act of producing

the password would not communicate any facts of testimonial significance beyond what he had already admitted to investigators, namely that a password existed that will decrypt Davis' computer, that he had possession and control of that password, and that the computer contained images of child pornography. The Commonwealth argued that the act of production falls under the foregone conclusion exception to the Fifth Amendment right against self-incrimination articulated in *Fisher v. United States*, 425 U.S. 391 (1976), and is constitutionally permissible. The Commonwealth requested "that Joseph Davis be ordered to assist the Commonwealth in the execution of the previously executed search warrant by providing his TrueCrypt password to his HP Envy computer or by inputting the password into the device."

Davis responded that such government compulsion would violate his right against self-incrimination under the Fifth Amendment.[2] Central to his argument was the assertion that, because the government could not state with any specificity what is contained in the computer files, the foregone conclusion exception established in *Fisher* is inapplicable.

While the motion was pending, the Commonwealth filed a Criminal Information charging Davis with two counts of sexual abuse of children (distribution of child

---

[2] Davis also contended that it would violate his right against self-incrimination under Article I, Section 9 of the state Constitution. However, he conceded that the Pennsylvania Supreme Court construes the state and federal constitutional provisions coextensively and follows this Court's lead on the proper analysis to be utilized.

pornography)[3] and two counts of criminal use of a communication facility.[4]

Following an evidentiary hearing, the trial court entered an order granting the Commonwealth's motion to compel. It specifically required that "Defendant supply the Commonwealth with any and all passwords used to access the HP Envy 700 desktop computer with serial # Z4Z1AAAEFM or [sic] within thirty (30) days from the date of this order." The trial court filed an opinion in support of its order which cited to *Fisher* as well as decisions of this Court and other courts applying *Fisher* and found that the foregone conclusion exception applies to the record facts. Notably, the court focused not only on the fact that the Commonwealth proved it had knowledge independent of the act of production that Davis has possession and control of the decryption password but also had independent knowledge regarding the existence and whereabouts of child pornography on the computer. For these reasons, the court held that Davis' act of production would lose its testimonial significance because the information is a "foregone conclusion."

Davis appealed that determination to the Superior Court of Pennsylvania. On November 30, 2017, a three-judge panel of that Court filed a unanimous, published Opinion affirming the trial court order compelling Davis to produce the password pursuant to the foregone conclusion exception. Davis subsequently

---

[3] 18 Pa.C.S.A. § 6312(c)

[4] 18 Pa.C.S.A. § 7512(a)

filed an application for reargument *en banc* that was denied.

On March 7, 2018, Davis filed a petition for allowance of appeal in the Supreme Court of Pennsylvania. On October 3, 2018, the Court granted that petition, articulating the issue as:

> May [Petitioner] be compelled to disclose orally the memorized password to a computer over his invocation of privilege under the Fifth amendment to the Constitution of the United States, and Article I, [S]ection 9 of the Pennsylvania Constitution?

Following briefing and oral argument, the state Supreme Court filed its decision on November 20, 2019. A four-justice majority reversed the Superior Court, holding that the foregone conclusion exception to the right against self-incrimination does not apply to the compelled disclosure of a computer password because the password is a mental construct stored in the suspect's mind rather than a physical object and the compelled production would require the suspect to use the contents of his own mind.

The majority relied in large part on this Court's prior decisions indicating that a compelled surrender of the key to a strongbox survives Fifth Amendment scrutiny but the compelled production of a lock combination does not. In the words of the majority:

> [C]onsistent with this historical repulsion of the prospect of compelling a defendant to reveal his or her mental impressions, we find it particularly revealing that, when addressing

> Justice Steven's dissent in *Doe II*, the majority of the Court noted that compelling the defendant to sign the bank disclosure forms was more akin to "be[ing] forced to surrender a key to a strongbox containing incriminating documents" than it was to "be[ing] compelled to reveal the combination to [petitioner's] wall safe." ...This is a critical distinction. Consistent with a physical/mental production dichotomy, in conveying the combination to a wall safe, versus surrendering a key to a strongbox, a person must use the "contents of [their] own mind." If one is protected from telling an inquisitor the combination to a wall safe, it is a short step to conclude that one is protected from telling an inquisitor the password to a computer.

220 A.3d at 547-548.

The majority held in the alternative that, even if the foregone conclusion exception is applicable under the circumstances presented, the Commonwealth failed to satisfy a prerequisite to that application because it failed to establish that it had knowledge of the contents of the files stored on Davis' computer hard drive, which it had already received judicial permission to search. In the words of the majority, "until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application, and, consistent with its teachings in other decisions, believe the exception to be inapplicable to compel the disclosure of a defendant's

password to assist the Commonwealth in gaining access to a computer." *Id.* at 551.

A three-justice minority of the Court dissented, holding that the foregone conclusion analysis articulated in *Fisher* and its progeny logically applies to the compelled disclosure of a digital password to an electronic device seized pursuant to a warrant. According to the minority:

> My analysis focuses on the compulsion order, which directed Appellant to "supply the Commonwealth with any and all passwords used to access" a specific desktop computer and hard drive seized from his residence...." In my view, this order compels an act of production that has testimonial aspects in that it conveys, as a factual matter, that Appellant has access to the particular computer seized by the Commonwealth pursuant to a warrant, and that he has possession and control over the password that will decrypt the encrypted files stored on that computer. As discussed in detail *infra*, because the Commonwealth was already aware of these facts based upon its own investigation and Appellant's candid discussion with government agents, the password falls within the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination, and may be constitutionally compelled. Notably, critical to my position is the recognition that this case does not involve a Fourth Amendment challenge based upon Appellant's privacy rights in his encrypted computer files but,

> rather, solely a challenge to the compelled disclosure of his password based upon his Fifth Amendment privilege against self-incrimination.

Id. at 553.

With regard to the majority's concern that compelled disclosure of the password would compel that suspect to utilize his mental processes, the minority stated:

> There is an appeal to this conclusion, as requiring Appellant to supply his password involves some mental effort in recalling the 64 characters used to encrypt the computer files. However, one would expend similar mental effort when engaging in virtually any other act of production, such as the disclosure of business or financial records, as the individual must retrieve the contents of his mind to recall the documents' location before disclosing them to the government... The mere fact that Appellant is required to think in order to complete the act of production, in my view, does not immunize that act of production from the foregone conclusion rationale.

Id. at 555.

Regarding the physical/mental dichotomy noted by this Court in its pre-digital era Fifth Amendment decisions, the minority observed:

> I recognize that the majority's conclusion in this regard finds support in commentary found

> in federal cases, suggesting a constitutional distinction between the compelled surrender of a key and the compelled disclosure of a combination to a wall safe. For the reasons set forth herein, however, I do not find any such distinction dispositive in a case involving current day technology relating to the compelled disclosure of a password to encrypted digital information, where the Commonwealth has a warrant to search the digital container. Only the High Court can make the final determination in this regard for purposes of the Fifth Amendment, and the present case offers an attractive vehicle by which the Court could do so.

Id. at 555 n.3.

The minority also observed that adopting the majority's approach would produce a bizarre anomaly in which the type of encryption password chosen by a user would dictate whether production of that password could be constitutionally compelled. Although an alphanumerical password committed to memory would be off limits, the government could require the production of a biometric password such as facial recognition or a fingerprint because those types of gateways to a device do not require use of the contents of one's mind.[5] The minority warned that the

---

[5] *See, e.g., State v. Diamond*, 905 N.W.2d 870, 877 (Minn. 2018) (ordering defendant to provide his fingerprint to unlock his cell phone did not violate right against self-incrimination); *Matter of Search of [Redacted] Washington, District of Columbia*, 317 F.Supp.3d 523, 539 (D.D.C. 2018) (compelled use of biometric

majority's approach would "create an entire class of evidence, encrypted computer files, that is impervious to government search" and "potentially alter the balance of power between governmental authorities and criminals, and render law enforcement incapable of accessing relevant evidence." *Id.* at 557.

The minority also disagreed with the majority about the extent of the government's burden under the foregone conclusion exception, noting that requiring the Commonwealth to prove knowledge of the contents of the computer files is an untenable application of *Fisher* that conflates the meaning and purposes of the Fourth and Fifth Amendments to the Constitution:

> [T]he foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to

---

features to open digital device found during execution of search warrant did not violate privilege against self-incrimination); *Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case*, 398 F.Supp.3d 785 (D. Idaho 2019) (compelled placement of suspect's finger on cellphone to unlock phone did not violate right against self-incrimination); *Matter of Search Warrant Application for Cellular Telephone in United States v. Barrera*, 415 F.Supp.3d 832 (N.D. Ill. East. Div. 2019) (same); *contra Matter of Residence in Oakland, California*, 354 F.Supp.3d 1010 (N.D. Cal. 2019) (foregone conclusion exception does not apply to permit government to compel use of biometric features to unlock cellphone; biometric features are the equivalent of a digital password); *In re Application for a Search Warrant*, 236 F.Supp.3d 1066 (N.D. Ill. West. Div. 2017) (same); *United States v. Wright*, -- F.Supp.3d –, 2020 WL 60239 (D. Nevada Jan. 6, 2020) (same).

decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating evidence. *See Doe v. United States* (*In re Grand Jury Subpoena*), 383 F.3d 905, 910 (9th Cir. 2004) (providing that "it is the government's knowledge of the existence and possession of the actual documents [subpoenaed by the government], not the information contained therein, that is central to the foregone conclusion inquiry"). This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection. The High Court in *Fisher* made this clear by stating, "We cannot cut the Fifth Amendment loose from the moorings of its language, and make it serve as a general protector of privacy – a word not mentioned in its text and a concept directly addressed in the *Fourth Amendment.*" 425 U.S. at 401 (quoting *United States v. Nobles*, 422 U.S. 225, 233 n. 7 (1975) (emphasis in original).

> Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone conclusion by focusing only on the compelled evidence itself, i.e., the computer password, and not the decrypted files that the password would ultimately reveal...

Id. at 556.

Succinctly stated, the majority of the state Supreme Court reached the conclusion that the Fifth Amendment bars a court from ordering disclosure of the password to an encrypted computer or other electronic device. The foregone conclusion doctrine does not apply because revealing the password would communicate implicitly the suspect's knowledge and possession of the password and ability to access the contents of the computer. The majority also held that being compelled to disclose the password was equivalent to providing the incriminating evidence contained in files on the computer. The dissent concluded that the government already had the information concerning the suspect's knowledge and control of the password and so the foregone conclusion exception applied. Also, discussion of the files contained within the computer are a matter for Fourth Amendment, not Fifth Amendment, analysis. Most courts considering the question to date have agreed with the dissent's position, but there is substantial division on the issue.

REASONS FOR GRANTING THE WRIT

The Court should grant the petition for writ of *certiorari* for the following reasons.

A. The Pennsylvania Supreme Court's decision addresses an important and pressing federal question in a manner that directly conflicts with the decisions of United States courts of appeals and decisions of other state courts of last resort.

This Court has previously noted that the sophisticated encryption technology that has recently emerged can render electronic devices "all but 'unbreakable' unless police know the password." *Riley v. California*, 573 U.S. 373, 389 (2014). Courts at all levels are now grappling with the dilemma created when an investigative search of a digital device has been approved by a court as reasonable under the Fourth Amendment but is being thwarted by encryption software that cannot be unlocked due to the suspect's refusal to provide the password on Fifth Amendment self-incrimination grounds.

The Supreme Court of Pennsylvania determined that the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination articulated in *Fisher v. United States*, 425 U.S. 391 (1976), does not extend beyond subpoenaed documents to apply to the compelled production of a password to an encrypted electronic device that is subject to a valid search warrant. This holding directly conflicts with decisions of United States courts of appeals and with decisions of other state courts of last resort on the same question. *See, e.g., United States v. Apple MacPro Computer,* 851 F.3d 238, 247 (3rd Cir. 2017); *United*

States v. Bright, 596 F.3d 683, 692 (9th Cir. 2010); *United States v. Gavegnano*, 305 Fed.Appx. 954 (4th Cir. 2009); *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 612 (Mass. 2014); *see also Commonwealth v. Jones*, 117 N.E.3d 702 (Mass. 2019) (holding that state constitutional privilege against self-incrimination tracks Fifth Amendment jurisprudence permitting compelled production of digital password where government can show it has independent knowledge that suspect knows the password); *Seo v. State*, 119 N.E.3d 90 (Ind. Dec. 6, 2018) (vacating lower court decision that foregone conclusion doctrine does not apply to compelled production of a digital password).

Only one United States court of appeals has ruled in a manner consistent with the Pennsylvania Supreme Court. *See In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (11th Cir. 2012). No state court of last resort has, to date, come to the same conclusion as Pennsylvania's highest court.

The lower state and federal courts are also profoundly divided on the questions presented. Many have found that the foregone conclusion exception applies to render compelled production of a digital password or compelled decryption of digital data constitutional. *See, e.g., State v. Johnson*, 576 S.W.3d 205, 277 (Mo. Ct. App. W.D. 2019); *State v. Pittman*, 452 P.3d 1011 (Or. App. 2019), *rev. allowed*, 458 P.3d 1121 (Or. 2020); *State v. Andrews*, 197 A.3d 200, 205 (N.J. Super. 2018); *State v. Stahl*, 206 So.3d 124, 131 (Fla. 2nd DCA 2016); *Commonwealth v. Baust*, 89 Va. Cir. 267 (Va. Cir. Ct. 2014); *United States v. Spencer*, 2018 WL 1964588 (N.D. Cal. April 26, 2018); *United States v. Fricosu*, 841 F.Supp.2d 1232, 1235 (D. Col.

2012); *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009).

Other courts have ruled to the contrary. *See, e.g., Pollard v. State*, 287 So.3d 649 (Fla. 1st DCA 2019); *People v. Spicer*, 125 N.E.3d 1286 (Ill. App. 3d 2019); *Sec. & Exch. Comm'n v. Huang*, 2015 WL 5611644 (E.D. Pa. Sept. 23, 2015); *United States v. Kirschner*, 823 F.Supp.2d 665, 669 (E.D. Mich. 2010).

Not only is there a lack of consensus and uniformity on the question of the applicability of the foregone conclusion exception in the context of digital passwords, but there is also widespread disagreement on the proper construction of the law established by *Fisher*, including: (1) the nature and quantity of independent knowledge the government must prove in order to trigger applicability of the exception;[6] (2) how past precedent addressing acts of production in the

---

[6] *Compare, e.g., MacPro Computer*, 851 F.3d at 248 n. 7 (noting that although the government could establish independent of the compelled production both the suspect's knowledge of the password and the existence of child pornography on the encrypted device, "a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production...[the suspect's] stating that 'I, John Doe, know the password for these devices'"), *Gelfgatt*, 11 N.E.3d 605 (government's burden is limited to showing independent knowledge of the password's existence, possession by suspect, and authenticity; its knowledge of the contents of the device itself is irrelevant to the analysis) with *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335 (government's ability to establish with reasonable particularity the presence of the files on the electronic device controls disposition of the question).

physical domain can be applied to productions of digital information;[7] and (3) the significance of the physical/mental distinction between biometric data and memorized passwords, both of which can unlock an encrypted device.[8]

This doctrinal disarray in the courts has been well-documented by legal scholars who have written extensively on the subject and have advanced various theoretical models for attaining a unified and coherent

---

[7] *Compare, e.g., Stahl*, 206 So.3d 124 (questioning whether compelling the production of a key to open a strongbox is in fact distinct from telling an officer the combination to a safe and questioning the continued viability of that distinction given the advancement of technology) with *Davis*, 220 A.3d 534 (adhering to the pre-digital era key to a strongbox/combination to a wall safe distinction in the context of digital passwords); *see also Spencer*, 2018 WL 1964588 (while storing evidence on an encrypted device may be equivalent to storing items in a safe protected by a combination, it is irrelevant to a compelled decryption because forcing the suspect to open the safe with his password does not provide the combination to the government); *United States v. Oloyede*, 933 F.3d 302 (4th Cir. 2019) (same).

[8] *Compare Spencer*, 2018 WL 1964588 (determining the constitutionality of a compelled production of a digital password based on whether the defendant protected his electronic files with a fingerprint key or an alphanumeric password produces an absurd result) with *Matter of Residence in Oakland, California*, 354 F. Supp. 1010 (biometric features are the equivalent of a digital password for purposes of foregone conclusion exception).

jurisprudence on the subject. *See, e.g.,* Orin Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 TEX. L. REV. 767 (2019) (noting in the context of encrypted digital containers the important distinction between evidence that "opens the door" of the container [a password] and the "treasure" that resides inside it [the computer contents] and arguing that the Fifth Amendment provides no protection from compelled production of a password when the government can show it has independent knowledge that the suspect knows the password); Aloni Cohen, Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries,* 32 HJVLT 169 (2019) (examining the wide variety of technical variations in encryption technology that are relevant to the compelled decryption analysis and must be considered in order to develop a robust doctrine that will remain unequivocal and relevant over time); Joseph Jarone, *An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption*, 10 FIULR 767 (2015) (noting that difference between compelled production of decryption password and compelled production of physical documents has been the source of much confusion and that rejection of the foregone conclusion exception in the context of digital passwords provides encryption users with greater protection than the Fifth Amendment requires); Wayne R. LaFave, Jerold H. Israel, Nancy J. King, Orin S. Kerr, *Testimonial Character and the Foregone Conclusion Standard,* CRIMPROC § 8.13(a) (December 2019 Update) (collecting cases applying *Fisher* and its progeny to encrypted electronic device cases).

The disparity in the holdings of courts, state and federal, throughout the country on this subject is precisely the type of case that warrants review by this Court. The Court's governing rule provides that "[r]eview on a writ of certiorari is not a matter of right, but of judicial discretion" and "will be granted only for compelling reasons." U.S. Sup. Ct. R. 10. Among the reasons that the Court will consider is that a state supreme court "has decided an important federal question in a way that conflicts with the decision of another state court of last resort or of a United States court of appeals" or "has decided an important question of federal law that has not been, but should be, settled by this Court..." *Id.* These considerations describe this case precisely.

These intractable issues surrounding the application of *Fisher* to compelled decryption of encrypted information that is subject to a judicially-sanctioned search urgently require this Court's attention and resolution. Guidance from the Court will furnish desperately-needed clarity, uniformity, stability, and predictability of the governing Fifth Amendment jurisprudence that will stem the tide of growing judicial chaos on the subject.

CONCLUSION

The Court should grant the petition.

Respectfully submitted,

JOSH SHAPIRO
Attorney General
Commonwealth of Pennsylvania

JENNIFER C. SELBER
Executive Deputy Attorney General
Director, Criminal Law Division

JAMES BARKER
Chief Deputy Attorney General
Appeals & Legal Services Section

WILLIAM R. STOYCOS *
Senior Deputy Attorney General
Counsel of Record

Office of Attorney General
16th Floor, Strawberry Square
Harrisburg, PA 17120
(717) 787-6348

Counsel for Petitioner

Date: April 20, 2020

148 N.E.3d 952
Supreme Court of Indiana.

Katelin EUNJOO SEO, Appellant (Defendant)
v.
STATE of Indiana, Appellee (Plaintiff)

Supreme Court Case No. 18S-CR-595
|
Argued: April 18, 2019
|
Filed June 23, 2020

Synopsis

Background: Defendant who was found to be in contempt by the Superior Court, Hamilton County, Steven R. Nation, J., for refusing to grant police access to her phone during an investigation for stalking. Defendant appealed, and the Court of Appeals, reversed and remanded. Defendant petitioned to transfer decision.

[Holding:] On grant of petition to transfer, as matter of first impression, the Supreme Court, Rush, C.J., held that defendant was not required, under foregone conclusion exception to Fifth Amendment's Self-Incrimination Clause, to unlock phone.

Reversed and remanded.

Massa, J., filed dissenting opinion in which Slaughter, J., joined.

Slaughter, J., filed dissenting opinion.

Opinion, 109 N.E.3d 418, vacated.

Procedural Posture(s): Appellate Review; Preliminary Hearing or Grand Jury Proceeding Motion or Objection.

West Headnotes (8)

[1] **Criminal Law** Compelling Self-Incrimination

Fifth Amendment's Self-Incrimination Clause requires the State to produce evidence against an individual through the independent labor of its officers, not by the simple, cruel expedient of forcing it from his own lips. U.S. Const. Amend. 5.

[2] **Criminal Law** Compelling Self-Incrimination

Fifth Amendment's Self-Incrimination Clause protects an accused from being forced to provide the State with even a link in the chain of evidence needed for prosecution. U.S. Const. Amend. 5.

[3] **Witnesses** Self-Incrimination

Not all compelled, incriminating evidence falls under Fifth Amendment's Self-Incrimination Clause: the evidence must also be testimonial. U.S. Const. Amend. 5.

[4] **Witnesses** Self-Incrimination

To be "testimonial" for purposes of Fifth Amendment privilege against self-incrimination, accused's communication must itself, explicitly or implicitly, relate factual assertion or disclose information. U.S. Const. Amend. 5.

[5] **Witnesses** Self-Incrimination

Physical acts can be "testimonial" for purposes of Fifth Amendment privilege against self-incrimination. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[6] **Witnesses** Privilege as to production of documents

When the State compels a suspect to produce physical evidence, that act is testimonial, for purposes of Fifth Amendment privilege against self-incrimination, if it implicitly conveys information; in certain contexts, however, the communicative aspects of the act may be rendered nontestimonial if the State can show that it already knows the information conveyed, making it a foregone conclusion. U.S. Const. Amend. 5.

3 Cases that cite this headnote

[7] **Witnesses** Privilege as to production of documents

A suspect surrendering an unlocked smartphone implicitly communicates, at a minimum, three things: (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possessed those files; and, unless the State can show it already knows this information, the communicative aspects of the production fall within the Fifth Amendment's protection against self-incrimination. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[8] **Witnesses** Privilege as to production of documents

Defendant was not required, under foregone conclusion exception to Fifth Amendment's Self-Incrimination Clause, to unlock smartphone following her arrest for stalking and harassment, although police officers obtained warrant ordering defendant to unlock smartphone, where officers did not identify any particular files on the smartphone relevant to defendant's arrest and investigation. U.S. Const. Amend. 5.

3 Cases that cite this headnote

***953** Appeal from the Hamilton Superior Court, No. 29D01-1708-MC-5640, The Honorable Steven R. Nation, Judge

Attorneys and Law Firms

ATTORNEYS FOR APPELLANT: William J. Webster, Carla V. Garino, Webster & Garino LLC, Westfield, Indiana

ATTORNEYS FOR APPELLEE: Curtis T. Hill, Jr., Attorney General of Indiana, Stephen R. Creason, Chief Counsel, Ellen H. Meilaender, Deputy Attorney General, Indianapolis, Indiana

ATTORNEYS FOR AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION, AMERICAN CIVIL LIBERTIES UNION, AND AMERICAN CIVIL LIBERTIES UNION OF INDIANA: Kenneth J. Falk, ACLU of Indiana, Indianapolis, Indiana, Andrew Crocker, Electronic Frontier Foundation, San Francisco, California

ATTORNEY FOR AMICI CURIAE STATES OF UTAH, GEORGIA, IDAHO, LOUISIANA, MONTANA, NEBRASKA, OKLAHOMA, AND PENNSYLVANIA: Kevin S. Smith, Special Assistant Utah Attorney General, Church Church Hittle & Antrim, Fishers, Indiana

On Petition to Transfer from the Indiana Court of Appeals, No. 29A05-1710-CR-2466

Rush, Chief Justice.

When Katelin Seo was placed under arrest, law enforcement took her iPhone believing it contained incriminating evidence. A detective got a warrant to search the smartphone, but he couldn't get into the locked device without Seo's assistance. So the detective got a second warrant that ordered Seo to unlock her iPhone. She refused, and the trial court held her in contempt.

We reverse the contempt order. Forcing Seo to unlock her iPhone would violate her Fifth Amendment right against self-incrimination. By unlocking her smartphone, Seo would provide law enforcement with information it does not already know, which the State could then use in its prosecution against her. The Fifth Amendment's protection from compelled self-

incrimination prohibits this result. We thus reverse and remand.

Facts and Procedural History

Katelin Seo contacted her local sheriff's department claiming D.S. had raped her. Detective Bill Inglis met with Seo, and she told him that her smartphone—an iPhone 7 Plus—contained relevant communications with the accused. With Seo's consent, officers completed a forensic download of the device and returned it.

Based on the evidence recovered from the iPhone and the detective's conversations with Seo, no charges were filed against D.S. Instead, law enforcement's focus switched to Seo. D.S. told Detective Inglis that Seo stalked and harassed him, and the detective's ensuing investigation confirmed those claims.

Detective Inglis learned that Seo first contacted D.S. from the phone number associated with her iPhone. But D.S. then began receiving up to thirty calls or text messages daily from dozens of different, unassigned numbers. Yet, because the substance of the contact was consistent, the detective believed that Seo placed the calls and texts using an app or internet program to disguise her phone number. As a result of this investigation, the State charged Seo with several offenses and issued an arrest warrant.

***954** When Detective Inglis arrested Seo, he took possession of her locked iPhone. Officers asked Seo for the device's password, but she refused to provide it. To clear this hurdle, Detective Inglis obtained two search warrants. The first authorized a forensic download of Seo's iPhone so that law enforcement could search the device for "incriminating evidence." And the second "compelled" Seo to unlock the device and stated that she would be subject "to the contempt powers of the court" if she failed to do so. After Seo again refused to unlock her iPhone, the State moved to hold her in contempt.

At the ensuing hearing, Seo argued that forcing her to unlock the iPhone would violate her Fifth Amendment right against self-incrimination. The trial court disagreed and held Seo in contempt, concluding that "[t]he act of unlocking the phone does not rise to the level of testimonial self-incrimination." Seo appealed, and the trial court stayed its contempt order.

While her appeal was pending, Seo entered into a plea agreement with the State. She pleaded guilty to one count of stalking, and the State dismissed eighteen other charged offenses without prejudice. But because the contempt citation remained in place, Seo still faced the threat of further sanction for disobeying that order. A divided panel of our Court of Appeals reversed the court's pending contempt order. *Seo v. State*, 109 N.E.3d 418, 440–41 (Ind. Ct. App. 2018).

We granted transfer, vacating the Court of Appeals decision. Ind. Appellate Rule 58(A). [1]

Standard of Review

Seo's challenge to the trial court's contempt order alleges a constitutional violation, and thus our review is de novo. *See* *Myers v. State*, 27 N.E.3d 1069, 1074 (Ind. 2015).

Discussion and Decision

[1] [2] [3] The Fifth Amendment's Self-Incrimination Clause protects a person from being "compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. Embedded within this constitutional principle is the requirement that the State produce evidence against an individual through "the independent labor of its ***955** officers, not by the simple, cruel expedient of forcing it from his own lips." *Estelle v. Smith*, 451 U.S. 454, 462, 101 S.Ct. 1866, 68 L.Ed.2d 359 (1981) (cleaned up). The privilege thus protects an accused from being forced to provide the State with even a link in the chain of evidence needed for prosecution. *See* *Hoffman v. United States*, 341 U.S. 479, 486, 71 S.Ct. 814, 95 L.Ed. 1118 (1951). Yet, not all compelled, incriminating evidence falls under this constitutional protection: the evidence must also be testimonial. *Hiibel v. Sixth Judicial Dist. Court of Nev., Humboldt Cty.*, 542 U.S. 177, 189, 124 S.Ct. 2451, 159 L.Ed.2d 292 (2004).

[4] [5] To be testimonial, "an accused's communication must itself, explicitly or implicitly, relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988).

The most common form of testimony is verbal or written communications—the vast amount of which will fall within the privilege. *Id.* at 213–14, 108 S.Ct. 2341. But physical acts can also have a testimonial aspect. *See* *Fisher v. United States*, 425 U.S. 391, 410, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976).

[6] When the State compels a suspect to produce physical evidence, that act is testimonial if it implicitly conveys information. *See* *United States v. Hubbell*, 530 U.S. 27, 36, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000); *Pennsylvania v. Muniz*, 496 U.S. 582, 595 n.9, 110 S.Ct. 2638, 110 L.Ed.2d 528 (1990). In certain contexts, however, the communicative aspects of the act may be rendered nontestimonial if the State can show that it already knows the information conveyed, making it a "foregone conclusion." *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569. In other words, the inquiry is whether the testimonial communications implicit in producing the evidence provide the State with something it does not already know.

Here, Seo argues that the State, by forcing her to unlock her iPhone for law enforcement, is requiring her to "assist in the prosecution of her own criminal case" and thus violating her right against self-incrimination. The State disagrees, claiming it already knows the implicit factual information Seo would convey by unlocking her iPhone—namely, that she "knows the password and thus has control and use of the phone."

We agree with Seo. The compelled production of an unlocked smartphone is testimonial and entitled to Fifth Amendment protection—unless the State demonstrates the foregone conclusion exception applies. Here, the State has failed to make that showing; and this case also highlights concerns with extending the limited exception to this context.

I. The act of producing an unlocked smartphone communicates a breadth of factual information.

Giving law enforcement an unlocked smartphone communicates to the State, at a minimum, that (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possesses those files. This broad spectrum of communication is entitled to Fifth Amendment protection unless the State can show that it already knows this information, making it a foregone conclusion. We make these determinations after carefully reviewing the U.S. Supreme Court precedent that has created and evaluated both the act of production doctrine and its accompanying foregone conclusion exception.

Our starting point is *Fisher v. United States*, 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). There, the IRS subpoenaed several taxpayers' documents that accountants prepared and the taxpayers' attorneys possessed. *Id.* at 394–96, 96 S.Ct. 1569. The attorneys responded that complying with the subpoenas would violate ***956** their clients' rights against self-incrimination. *Id.* at 395–96, 96 S.Ct. 1569.[2] The Court disagreed. *Id.* at 414, 96 S.Ct. 1569.

In reaching that conclusion, *Fisher* considered what, if any, incriminating testimony would be compelled by responding to a documentary summons. *Id.* at 409, 96 S.Ct. 1569. It was here that the Court created the act of production doctrine: producing documents in response to a subpoena can be testimonial if the act concedes the existence, possession, or authenticity of the documents ultimately produced. *Id.* at 410, 96 S.Ct. 1569. But when the government can show that it already knows this information, then the testimonial aspects of the act are a "foregone conclusion," *id.* at 411, 96 S.Ct. 1569, and complying with the subpoena becomes a question "not of testimony but of surrender," *id.* (quoting *In re Harris*, 221 U.S. 274, 279, 31 S.Ct. 557, 55 L.Ed. 732 (1911)). This was the situation in *Fisher*—the Government knew who possessed the tax documents, and it could independently confirm the documents' existence and authenticity through the accountants who prepared them. *Id.* at 412–13, 96 S.Ct. 1569. So, the Court narrowly held that "compliance with a summons directing the taxpayer to produce the accountant's documents involved in these cases" did not implicate incriminating testimony within the Fifth Amendment's protection. *Id.* at 414, 96 S.Ct. 1569.

Fisher was the first, and only, Supreme Court decision to find that the testimony implicit in an act of production

was a foregone conclusion. In contrast, the government failed to make that showing in the other two relevant decisions: *United States v. Doe*, 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552 (1984) (*Doe I*) and *United States v. Hubbell*, 530 U.S. 27, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000).

In *Doe I*, the Government served five subpoenas commanding a business owner to produce certain documents. 465 U.S. at 606–07, 104 S.Ct. 1237. He refused, arguing that complying with the subpoenas would violate his right against self-incrimination. *Id.* at 607–08, 104 S.Ct. 1237. The District Court agreed, finding that compliance would compel the business owner "to admit that the records exist, that they are in his possession, and that they are authentic." *Id.* at 613 & n.11, 104 S.Ct. 1237.

The *Doe I* Court affirmed the District Court's finding "that the act of producing documents would involve testimonial self-incrimination." *Id.* at 613–14, 104 S.Ct. 1237. The Court then explained that the Government was not foreclosed from producing "evidence that possession, existence, and authentication were a 'foregone conclusion,' " but that it had "failed to make such a showing." *Id.* at 614 n.13, 104 S.Ct. 1237 (quoting *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569).

Similarly, the Court in *Hubbell* found that the foregone conclusion exception did not apply. 530 U.S. at 44, 120 S.Ct. 2037. There, the Government served a subpoena requesting a vast array of documents. *Id.* at 31, 120 S.Ct. 2037. In response, Hubbell produced 13,120 pages; and he was later indicted based on information gleaned from their contents. *Id.* In finding that Hubbell's compliance with the subpoena violated his right against self-incrimination, the Court rejected two of the Government's arguments.

***957** *Hubbell* first refused to equate the physical act of handing over the documents with the testimony implicit in the act. *Id.* at 40–41, 120 S.Ct. 2037. The Court agreed that the testimonial aspect of responding to a documentary summons "does nothing more than establish the existence, authenticity, and custody of items that are produced." *Id.* But it rebuffed the Government's "anemic view" of the act of production as a "simple physical act." *Id.* at 43, 120 S.Ct. 2037. The Court explained that a physical act, nontestimonial in character, cannot be "entirely divorced from its 'implicit' testimonial aspect." *Id.*

Hubbell also rejected the Government's argument that, under *Fisher*, "the existence and possession of such records by any businessman is a 'foregone conclusion.' " *Id.* at 44, 120 S.Ct. 2037. The Court referred to *Fisher*'s unique context and explained, "Whatever the scope of this 'foregone conclusion' rationale, the facts of this case plainly fall outside of it." *Id.* Unlike in *Fisher*, the *Hubbell* Court reasoned that, because the Government failed to show "it had any prior knowledge of either the existence or the whereabouts of the ... documents ultimately produced," the foregone conclusion exception did not apply. *Id.* at 45, 120 S.Ct. 2037.

Fisher, *Doe I*, and *Hubbell* establish that the act of producing documents implicitly communicates that the documents can be physically produced, exist, are in the suspect's possession, and are authentic. And this trilogy of Supreme Court precedent further confirms that the foregone conclusion exception must consider these broad communicative aspects. *See Commonwealth v. Davis*, 220 A.3d 534, 547 (Pa. 2019) (recognizing that "the Supreme Court has made, and continues to make, a distinction between physical production and testimonial production"), *petition for cert. filed* (U.S. Apr. 20, 2020) (No. 19-1254).

In this way, the act of production doctrine links the physical act to the documents ultimately produced. *See* Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 Tex. L. Rev. Online 63, 68 (2019). And the foregone conclusion exception relies on this link by asking whether the government can show it already knows the documents exist, are in the suspect's possession, and are authentic. *Id.* True, the documents' contents are not protected by the Fifth Amendment because the government did not

compel their creation. *See* *Doe I*, 465 U.S. at 611–12, 104 S.Ct. 1237; *Fisher*, 425 U.S. at 409–10, 96 S.Ct. 1569. But the specific documents "ultimately produced" implicitly communicate factual assertions solely through their production. *See* *Hubbell*, 530 U.S. at 36 & n.19, 45, 120 S.Ct. 2037.

When extending these observations to the act of producing an unlocked smartphone, we draw two analogies. First, entering the password to unlock the device is analogous to the physical act of handing over documents. Sacharoff, *supra*, at 68. And second, the files on the smartphone are analogous to the documents ultimately produced. *Id.*

[7] Thus, a suspect surrendering an unlocked smartphone implicitly communicates, at a minimum, three things: (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possessed those files.[3] And, unless the State can show it already knows this information, the communicative aspects of the production fall within the Fifth Amendment's ***958** protection. Otherwise, the suspect's compelled act will communicate to the State information it did not previously know—precisely what the privilege against self-incrimination is designed to prevent. *See* *Couch v. United States*, 409 U.S. 322, 328, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973).

This leads us to the following inquiry: has the State shown that (1) Seo knows the password for her iPhone; (2) the files on the device exist; and (3) she possessed those files?

II. The foregone conclusion exception does not apply.

[8] As discussed above, compelling Seo to unlock her iPhone would implicitly communicate certain facts to the State. And for those communicative aspects to be rendered nontestimonial, the State must establish that it already knows those facts.

Even if we assume the State has shown that Seo knows the password to her smartphone, the State has failed to demonstrate that any particular files on the device exist or that she possessed those files. Detective Inglis simply confirmed that he would be fishing for "incriminating evidence" from the device. He believed Seo—to carry out the alleged crimes—was using an application or internet program to disguise her phone number. Yet, the detective's own testimony confirms that he didn't know which applications or files he was searching for:

> There are numerous, and there's probably some that I'm not even aware of, numerous entities out there like Google Voice and Pinger and Text Now and Text Me, and I don't know, I don't have an all-encompassing list of them, however if I had the phone I could see which ones she had accessed through Google.

In sum, law enforcement sought to compel Seo to unlock her iPhone so that it could then scour the device for incriminating information. And Seo's act of producing her unlocked smartphone would provide the State with information that it does not already know. But, as we've explained above, the Fifth Amendment's privilege against compulsory self-incrimination prohibits such a result. Indeed, to hold otherwise would sound "the death knell for a constitutional protection against compelled self-incrimination in the digital age." *Commonwealth v. Jones*, 481 Mass. 540, 117 N.E.3d 702, 724 (2019) (Lenk, J., concurring); *see also Davis*, 220 A.3d at 549 ("[T]o apply the foregone conclusion rationale in these circumstances would allow the exception to swallow the constitutional privilege.").

Though the foregone conclusion exception does not apply to these facts, this case underscores several reasons why the narrow exception may be generally unsuitable to the compelled production of any unlocked smartphone. We discuss three concerns below.

III. This case highlights concerns with extending the limited foregone conclusion exception to the compelled production of an unlocked smartphone.

Extending the foregone conclusion exception to the compelled production of an ***959** unlocked smartphone is concerning for three reasons: such an expansion (1) fails to account for the unique ubiquity and capacity of smartphones;

(2) may prove unworkable; and (3) runs counter to U.S. Supreme Court precedent. We address each in turn.

A. The compelled production of an unlocked smartphone is unlike the compelled production of specific business documents.

Smartphones are everywhere and contain everything. They have become such "a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." *Riley v. California*, 573 U.S. 373, 385, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014); *see also* *City of Ontario v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). Indeed, a 2019 report from the Pew Research Center revealed that 81% of Americans own a smartphone, up from 35% in 2011.[4] The Supreme Court in *Fisher* (1976), *Doe I* (1984), or *Hubbell* (2000) surely could not have anticipated that such devices would become so common or imagined the breadth and depth of information they could contain.

Notably, in each of those cases, a subpoena confined the information implicated by the compelled production. *See* *Hubbell*, 530 U.S. at 45–46, 120 S.Ct. 2037; *Doe I*, 465 U.S. at 606–07, 607 nn.1–2, 104 S.Ct. 1237; *Fisher*, 425 U.S. at 394–95, 394 nn.2–3, 96 S.Ct. 1569. *Fisher* acknowledged this limited scope, stating that the subpoenas there sought "documents of unquestionable relevance to the tax investigation," but that "[s]pecial problems of privacy ... might be presented by subpoena of a personal diary." 425 U.S. at 401 n.7, 96 S.Ct. 1569; *see also* *Barrett v. Acevedo*, 169 F.3d 1155, 1167–68 (8th Cir. 1999) (en banc) (discussing the circuit split as to whether personal diaries can be subpoenaed); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27, 81 (1986) (opining that "certain types of highly private documents probably should not be obtainable by subpoena, regardless of whether they are self-incriminating"). And the *Doe I* Court remarked that the compelled documents, which "pertained to respondent's businesses," were less personal than those sought in *Fisher*, which "related to the taxpayers' individual tax returns." *Doe I*, 465 U.S. at 610 n.7, 104 S.Ct. 1237. An unlocked smartphone, however, contains far more private information than a personal diary or an individual tax return ever could. Yet, when suspects are compelled to surrender their unlocked smartphones, there is no limiter like a documentary subpoena for specific files. *See, e.g.*, *United States v. Bishop*, 910 F.3d 335, 336 (7th Cir. 2018), *cert. denied*, —— U.S. ——, 139 S. Ct. 1590, 203 L.Ed.2d 745 (2019).

Hubbell further illustrates the considerable difference between complying with a court order to produce an unlocked smartphone and complying with a documentary summons. Recall that, in *Hubbell*, the Government had not shown that it had any prior knowledge of either the existence or location of 13,120 pages of documents. 530 U.S. at 45, 120 S.Ct. 2037. Though not an insignificant amount of information, it pales in comparison to what can be stored on today's smartphones. Indeed, the cheapest model of last year's top-selling smartphone, with a capacity of 64 gigabytes of data, can hold over 4,000,000 pages of documents—more than 300 times the number of pages produced in *Hubbell*.[5] It is no ***960** exaggeration to describe a smartphone's passcode as "the proverbial 'key to a man's kingdom.' " *United States v. Djibo*, 151 F. Supp. 3d 297, 310 (E.D.N.Y. 2015).

This brings us to a second concern with extending the foregone conclusion exception—it may prove unworkable in this context.

B. Extending the foregone conclusion exception to the compelled production of a smartphone may prove unworkable.

Today's smartphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley*, 573 U.S. at 393, 134 S.Ct. 2473. And they can contain, in digital form, the "combined footprint of what has been occurring socially, economically, personally, psychologically, spiritually and sometimes even sexually, in the owner's life." *Djibo*, 151 F. Supp. 3d at 310.

Recognizing these realities, several courts have determined that the government—prior to compelling a suspect to unlock their smartphone—must specifically identify the files it seeks with reasonable particularity.[6] But even then, the government should have access to only those files. Yet, compelling the production of an unlocked smartphone gives the government access to everything on the device, not just those files it can identify with "reasonable particularity." For example, here, even if the State could show that it knew of and could identify specific files on Seo's iPhone, there is nothing to restrict law enforcement's access to only that information. After all, the warrant authorized a search of Seo's device without limitation.

Such unbridled access to potential evidence on her iPhone —or any smartphone—raises several complex questions. For example, if officers searching a suspect's smartphone encounter an application or website protected by another password, will they need a separate motion to compel the suspect to unlock that application or website? And would the foregone conclusion exception apply to that act of production as well? Suppose law enforcement opens an application or website and the password populates automatically. Can officers legally access that information? Or what if a suspect has a cloud-storage service—like iCloud or Dropbox—installed on the device, which could contain hundreds of thousands of files. Can law enforcement look at those documents, even though this ***961** windfall would be equivalent to identifying the location of a locked storage facility that officers did not already know existed? Such complexity is neither necessary nor surprising: the foregone conclusion exception is, in this context, a low-tech peg in a cutting-edge hole.

This leads to a third concern with extending the foregone conclusion exception—it seems imprudent in light of recent Supreme Court precedent concerning smartphones and the limited, questionable application of the exception.

C. U.S. Supreme Court precedent and the foregone conclusion exception's limited application counsel against extending it further.

The Supreme Court has hesitated to apply even entrenched doctrines to novel dilemmas, wholly unforeseen when those doctrines were created. Indeed, the Court recently observed that, when "confronting new concerns wrought by digital technology," it "has been careful not to uncritically extend existing precedents." *Carpenter v. United States*, —— U.S. ——, 138 S. Ct. 2206, 2222, 201 L.Ed.2d 507 (2018). To that point, four years earlier, in *Riley*, the Court held that the search-incident-to-arrest exception to the warrant requirement does not extend to a cell phone found on an arrestee. 573 U.S. at 401–02, 134 S.Ct. 2473. And in *Carpenter*, the Court held that the third-party doctrine does not extend to cellular site location information, at least when seven days' worth of data is obtained. 138 S. Ct. at 2217 & n.3. The Supreme Court's refusal to extend these two established doctrines—each far more deeply rooted than the foregone conclusion exception—is instructive.

Though *Riley* and *Carpenter* were decided under the Fourth Amendment, the Court's concern in each case was with the "privacy interests" implicated by smartphones. *Riley*, 573 U.S. at 397, 134 S.Ct. 2473; *Carpenter*, 138 S. Ct. at 2214–15. And that privacy concern likewise applies to the Fifth Amendment's privilege against self-incrimination. Even though this privilege is not "a general protector of privacy," *Fisher* recognized that it "truly serves privacy interests" by protecting suspects from being compelled to provide private, self-incriminating testimony. 425 U.S. at 399, 401, 96 S.Ct. 1569; *see also* *id.* at 416–17, 96 S.Ct. 1569 (Brennan, J., concurring in the judgment) ("Expressions are legion in opinions of this Court that the protection of personal privacy is a central purpose of the privilege against compelled self-incrimination."); *Murphy v. Waterfront Comm'n of N.Y. Harbor*, 378 U.S. 52, 55, 84 S.Ct. 1594, 12 L.Ed.2d 678 (1964); *In re Grand Jury Proceedings*, 632 F.2d 1033, 1042–44 (3d Cir. 1980).

The limited, and questionable, application of the foregone conclusion exception also cautions against extending it further. Indeed, *Fisher* was decided over forty-four years ago, and it remains the lone U.S. Supreme Court decision to find that the exception applied. In the intervening years, the Court has discussed it twice and in only one context: in grand jury proceedings when a subpoena compelled the production of business and financial records. During this

same time period, legal scholars—including three current members of the Supreme Court—have wondered whether *Fisher* interpreted the Fifth Amendment too narrowly, calling into question the viability of the foregone conclusion exception itself. *See* *Hubbell*, 530 U.S. at 49–56, 120 S.Ct. 2037 (Thomas, J., concurring); *Carpenter*, 138 S. Ct. at 2271 (Gorsuch, J., dissenting); Alito, Jr., *supra*, at 45–51; *see also, e.g.*, Bryan H. Choi, *The Privilege Against Cellphone Incrimination*, 97 Tex. L. Rev. Online 73, 74 n.6 (2019); Richard A. Nagareda, ***962** *Compulsion "To Be a Witness" and the Resurrection of* Boyd, 74 N.Y.U. L. Rev. 1575, 1606 & nn.124–25 (1999); Robert Heidt, *The Fifth Amendment Privilege and Documents—Cutting* Fisher*'s Tangled Line*, 49 Mo. L. Rev. 439, 443 (1984). Regardless of the foregone conclusion exception's viability, it seems imprudent to extend it beyond its one-time application. *Cf.* *Silverman v. United States*, 365 U.S. 505, 510, 512, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961) (deciding not to extend the rationale of a factually distinct case "by even a fraction of an inch").

It is not surprising that courts to recently address this issue—how the Fifth Amendment applies to the compelled production of unlocked electronic devices—have either declined to extend the foregone conclusion exception or have not mentioned it at all.[7] Not only was the exception crafted for a vastly different context, but extending it further would mean expanding a decades-old and narrowly defined legal exception to dynamically developing technology that was in its infancy just a decade ago. And it would also result in narrowing a constitutional right. Yet, while we have identified three concerns with extending the foregone conclusion exception to this context, we do not need to make a general pronouncement on its validity because it simply does not apply here.

At the same time, we emphasize that there are several ways law enforcement can procure evidence from smartphones without infringing on an individual's Fifth Amendment rights. For example, officers could try to obtain information from third parties under the Stored Communications Act. *See* 18 U.S.C. 121 §§ 2701–2713 (2018). Alternatively, two companies—Cellebrite and Grayshift—offer law enforcement agencies affordable products that provide access to a locked smartphone. *See generally, e.g.*, *United States v. Chavez-Lopez*, 767 F. App'x 431, 433–34 (4th Cir. 2019). Or officers could seek an order compelling the smartphone's manufacturer to help bypass the lock screen. *See In re XXX, Inc.*, No. 14 Mag. 2258, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014). And if law enforcement wants to get into a smartphone for reasons other than prosecution, they can offer immunity to the device's owner. *See* *Doe I*, 465 U.S. at 614–15, 104 S.Ct. 1237. But the State cannot fish for incriminating evidence by forcing Seo to give unfettered access to her iPhone when it has failed to show that any files on Seo's smartphone exist or that she possessed those files.

Nearly a century ago, U.S. Supreme Court Justice Louis Brandeis cautioned, "Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home." *Olmstead v. United States*, 277 U.S. 438, 474, 48 S.Ct. 564, 72 L.Ed. 944 (1928) (Brandeis, J., dissenting). That day has come. And to allow the State, on these facts, to force Seo to unlock her iPhone for law enforcement would tip the scales too far in the State's favor, resulting in a seismic erosion of the Fifth Amendment's privilege against self-incrimination. This we will not do.

Conclusion

Forcing Seo to unlock her iPhone for law enforcement would violate her Fifth Amendment right against self-incrimination. We thus reverse the trial court's order finding Seo in contempt and instruct the court to dismiss the citation.

David and Goff, JJ., concur.

Massa, J., dissents with separate opinion in which Slaughter, J., joins in part.

Slaughter, J., dissents with separate opinion.

Massa, J., dissenting.

***963** I respectfully dissent from the Court's opinion deciding the merits of this case because it was mooted when the underlying criminal case was dismissed. And this now-moot case shouldn't be resolved under our "great public interest" exception because doing so could—in violation of the core

principles of federalism—leave our Court as the final arbiter of our nation's fundamental law.

The gist of Seo's purported behavior over the summer and fall of 2017 is this: starting in June, Seo unrelentingly implored a man to either marry or impregnate her. In July, Seo started following and sending troubling messages to a woman who reported her to a supervisor for showing a horror film to the woman's preschool children at the daycare where Seo worked. Seo was charged with various crimes in numerous cases for these interactions, and, on **August 8**, the trial court ordered Seo to unlock her iPhone to obtain evidence for a case involving the man, warning that her refusal could subject her to being held in contempt. On **September 22**, after she persistently refused to unlock the device, the trial court held Seo in contempt and ordered her incarcerated if she didn't comply by the end of the day. Three days later, however, the court stayed the order after Seo indicated she would appeal it.

The next July, Seo and the prosecution reached a global agreement: the State dismissed all other charges against Seo when she pleaded guilty to a single stalking charge involving the woman. All the charges in the cases involving the man—including those in the case where Seo was held in contempt for refusing to unlock her device—were dismissed. The next month, our Court of Appeals reversed the contempt order. Later yet, the State successfully opposed Seo's request for the return of her device pending our resolution of the case.

At the outset, we shouldn't reach Seo's constitutional claim because she is impermissibly waging a collateral attack on the trial court's August 8 order (compelling her to unlock her phone) through this appeal of the trial court's September 22 order (holding her in contempt). "Collateral attack of a previous order is allowed in a contempt proceeding only if the trial court lacked subject matter or personal jurisdiction to enter the order." *State v. Combs*, 921 N.E.2d 846, 851 (Ind. Ct. App. 2010) (quotation omitted). Because no one doubts the jurisdiction of the trial court here, and "[c]ontempt proceedings are not actions designed to correct errors previously made by trial courts," *id.* (quotation omitted), the Court shouldn't permit Seo to challenge the constitutional validity of the trial court's August 8 order through this appeal, *see* *Clark v. Atkins*, 489 N.E.2d 90, 96 (Ind. Ct. App. 1986) (explaining that even when "the questions raised concerning [an underlying] order are constitutional in nature," contempt proceedings cannot be used for a collateral attack) (citation omitted). Although her Fifth Amendment right could potentially be "irretrievably lost" if she were to unlock her device now, *Van Cauwenberghe v. Biard*, 486 U.S. 517, 524, 108 S.Ct. 1945, 100 L.Ed.2d 517 (1988) (citation omitted), we shouldn't flout well-settled procedure to resolve Seo's claim when she had forty-five days to file an interlocutory appeal of the August 8 order before being held in contempt. *See* Ind. Appellate Rule 14(B)(1)(c)(i) (permitting interlocutory appeal if a party believes she "will suffer substantial expense, damage[,] or injury if the order is erroneous and the ***964** determination of the error is withheld until after judgment.").

Nevertheless, this case is also moot. The Court, however, suggests it remains live because, as the State avows, "the 'threat of a sanction still hangs over [Seo's] head.' " *Ante*, at 954 n.1. But the order finding Seo in contempt was mooted—and this case was mooted—when Seo reached the agreement that, among other things, resolved the case underlying the order. "Contempts of court are classified as civil and criminal." *Perry v. Pernet*, 165 Ind. 67, 70, 74 N.E. 609, 610 (1905). Criminal contempt cases survive even after an underlying cause is mooted because this contempt is "an act directed against the dignity and authority of the court which obstructs the administration of justice and which tends to bring the court into disrepute or disrespect." *State v. Heltzel*, 552 N.E.2d 31, 34 (Ind. 1990). These contempt orders subsist, then, until a defendant "has served his contempt sentence and has been released." *Bell v. State*, 1 N.E.3d 190, 192 (Ind. Ct. App. 2013).

But Seo's contempt was civil: she refused "to do something which [s]he [wa]s ordered to do for the benefit or advantage of the opposite party." *Perry*, 165 Ind. at 70, 74 N.E. at 610 (quotation omitted). Since the opposing party "alone has an interest in the enforcement of" a civil contempt order, any associated punishment "terminates" the moment this party's interest ceases. *Id.* at 71, 610, 74 N.E. 609, 610. So when an underlying cause concludes by "settlement of all differences between the parties," any attendant civil contempt proceeding "necessarily" ends. *Gompers v. Buck's Stove & Range Co.*, 221 U.S. 418, 451–452, 31 S.Ct. 492, 55 L.Ed. 797 (1911). [1] Here, the State reached a global settlement with Seo resolving the claims it had against her. Once these charges were settled,

the civil contempt order automatically terminated. What could the State now gain from Seo unlocking her device?

The Court contends "that the State could not 'do a full investigation' or 'be in a position to either not bring or choose to bring new cases' until it had evidence from the device." *Ante*, at 954 n.1. But a year before opposing the return of Seo's device, the State returned the search warrant, acknowledging that "this matter is now closed." Return on Search Warrant, *In Re: Search Warrant*, No. 29D01-1708-MC-5624 (Hamilton Sup. Ct.); *see* Ind. Code § 35-33-5-4 (directing that, ordinarily, after a search warrant is executed, the executing officer must ensure a "return" of the warrant, stating the date and time of the search and what items were seized).[2] Instead of retaining the search warrant for ***965** further investigation, the State returned it after having settled all claims with Seo. Despite its later assertion "that its interest in accessing Seo's iPhone [wa]s 'not limited' to just the charges covered by the plea agreement," *ante*, at 954 n.1, the State should have, if it sought to trawl for further charges, awaited resolution of this appeal before settling the cases. But it didn't, so this case can't provide any relief " 'to the parties before the court.' " *T.W. v. St. Vincent Hosp. & Health Care Ctr., Inc.*, 121 N.E.3d 1039, 1042 (Ind. 2019) (quoting *Matter of Lawrance*, 579 N.E.2d 32, 37 (Ind. 1991)). When "[n]one of the parties seem to have any interest left in the case," this court of last resort should dismiss because it "ought not to be engaged in passing on moot-court questions." *State ex rel. Taylor v. Mount*, 151 Ind. 679, 694, 52 N.E. 407, 407 (1898).

But this Court has, for better or worse, decided moot cases " 'when the issue involves a question of great public importance which is likely to recur.' " *T.W.*, 121 N.E.3d at 1042 (quoting *Matter of Tina T.*, 579 N.E.2d 48, 54 (Ind. 1991)). Indeed, the Court acknowledges it believes that, "irrespective of mootness, this case presents a novel, important issue of great public importance that will surely recur." *Ante*, at 954 n.1. Because, however, constitutional questions should be avoided unless answering them is "absolutely necessary to a disposition of the cause on its merits," *State v. Darlington*, 153 Ind. 1, 4, 53 N.E. 925, 926 (1899), this Court should —in cases resolving federal questions—employ the Article-III-mirroring mootness test recently used by Senior Judge Shepard: whether " 'the issue concerns a question of great public importance which is likely to recur in a context which will continue to **evade review**,' " *Liddle v. Clark*, 107 N.E.3d 478, 482 (Ind. Ct. App. 2018) (quoting *DeSalle v. Gentry*, 818 N.E.2d 40, 49 (Ind. Ct. App. 2004)) (emphasis added), *trans. denied*. To be sure, then-Chief Justice Shepard noted that this heightened standard "is a federal mootness doctrine, stricter than our own, rooted in the requirement that Article III courts decide only live cases and controversies." *Lawrance*, 579 N.E.2d at 37 n.2. But *Lawrance* applied our relaxed standard when answering questions of Indiana law, not a federal question that could be unreviewable, depending wholly on the prevailing party,[3] by the U.S. Supreme Court.

Although the issue in this case is clearly one of great public importance and will surely recur with other defendants, it will not evade review. Seo entered into a global agreement resolving the case tied to her contempt order before our Court of Appeals issued its opinion reversing the order holding her in contempt. But her resolution of the case before appellate review is ***966** the outlier, not the norm. *Cf.* *Hartman v. State*, 988 N.E.2d 785 (Ind. 2013) (reversing under the Fifth Amendment—and in an interlocutory appeal—a trial court's denial of a defendant's motion to suppress). Perhaps we still exercise our lesser standard in cases like *Lawrance* involving only questions of Indiana law. Perhaps not. *See Wallace v. City of Indianapolis*, 40 Ind. 287, 289 (1872) ("It is not our duty to decide mere legal questions, when neither party can derive any legal benefit from such decision, and we have too many real questions before us, requiring our time and labor, to allow us to write mere speculative opinions to gratify ourselves or others, and in which no one has any legal right or interest depending."). But that is a question for another day.

Instead, we must ask whether this Court should use a federally moot case to decide an important question of federal constitutional law. The answer must be no. To be sure, "the constraints of Article III do not apply to state courts, and accordingly the state courts are not bound by the limitations of a case or controversy or other federal rules of justiciability even when they address issues of federal law, as when they are called upon to interpret the Constitution." *ASARCO Inc. v. Kadish*, 490 U.S. 605, 617, 109 S.Ct. 2037, 104 L.Ed.2d 696 (1989). But whether state courts entertain federal-law challenges absent Article III requirements "is entirely a matter

of state law." *Virginia v. Hicks*, 539 U.S. 113, 123 S.Ct. 2191, 156 L.Ed.2d 148 (2003). Our courts should not.

Both the "the national and State [judicial] systems are to be regarded as ONE WHOLE," with appeals from state courts interpreting federal laws naturally flowing "to that tribunal which is destined to unite and assimilate the principles of national justice and the rules of national decisions." Federalist No. 82 (Alexander Hamilton). To Hamilton, all cases determining federal law "shall, for weighty public reasons, receive their original or final determination in the courts of the Union." *Id.* And the nascent Supreme Court agreed, noting that a chief purpose of its review over state court opinions deciding questions of federal constitutional law

> is the importance, and even necessity of **uniformity** of decisions throughout the whole United States, upon all subjects within the purview of the constitution. Judges of equal learning and integrity, in different states, might differently interpret a statute, or a treaty of the United States, or even the constitution itself: If there were no revising authority to control these jarring and discordant judgments, and harmonize them into uniformity, the laws, the treaties, and the constitution of the United States would be different in different states, and might, perhaps, never have precisely the same construction, obligation, or efficacy, in any two states. The public mischiefs that would attend such a state of things would be truly deplorable; and it cannot be believed that they could have escaped the enlightened convention which formed the constitution.

Martin v. Hunter's Lessee, 14 U.S. (1 Wheat.) 304, 347–48, 4 L.Ed. 97 (1816). To protect the "vital interest to the nation" it was—and is—"essential" that the U.S. Supreme Court exercise "appellate power over those judgments of the State tribunals which may contravene the constitution or laws of the United States." *Cohens v. Virginia*, 19 U.S. (6 Wheat.) 264, 414–15, 5 L.Ed. 257 (1821).

"The judicial power **of the United States** is extended to all cases arising under the constitution." *Marbury v. Madison*, 5 U.S. (1 Cranch) 137, 178, 2 L.Ed. 60 (1803) (emphasis added). Irrefutably, the Supreme Court of the United States —not this state supreme court or any other—"is ***967** the final arbiter of federal law." *Danforth v. Minnesota*, 552 U.S. 264, 291–92, 128 S.Ct. 1029, 169 L.Ed.2d 859 (2008) (Roberts, C.J., dissenting). Rejecting the finality of that Court betrays a core first principle of this nation: when we decide issues of federal law by exercising a flexible exception that could divest a federal court of jurisdiction under its more-rigid Article III constraints, we usurp our role in this federal system, defenestrating the U.S. Supreme Court in the process. *See* *Cohens*, 19 U.S. (6 Wheat.) at 371 ("[T]he judicial control of the Union over State encroachments and usurpations, was indispensable to the sovereignty of the constitution—to its integrity—to its very existence. Take it away, and the Union becomes again a loose and feeble confederacy—a government of false and foolish confidence —a delusion and a mockery!").

Although "State courts are coequal parts of our national judicial system and give serious attention to their responsibilities for enforcing the commands of the Constitution," *Sawyer v. Smith*, 497 U.S. 227, 241, 110 S.Ct. 2822, 111 L.Ed.2d 193 (1990), this Court has long known "that the judicial power of the **United States** is extended, by the constitution, to all cases arising under the constitution, laws, and treaties of the **United States**," *Moyer v. McCullough*, 1 Ind. 339, 343 (1849). Indeed, Justice Blackford noted, while state courts may enjoy primary jurisdiction over federal questions, the "constitution requires the jurisdiction in such cases to be extended to the federal Courts." *Id.* And this view isn't constrained to the era immediately preceding the ratification of our 1851 constitution. Recently, for example—in a case unhampered by federal justiciability concerns—we chose to "await guidance from the Supreme Court and decline to find or assume [an issue of constitutional law] until the Supreme Court decides

the issue authoritatively." *State v. Timbs*, 84 N.E.3d 1179, 1183 (Ind. 2017), *vacated and remanded*. Noting that "Indiana is a sovereign state within our federal system,"[4] this Court unanimously avoided prematurely deciding an important question of federal law by declining to impose "federal obligations on the State that the federal government itself has not mandated." *Id.* at 1183–84; *see also Sparks v. State*, 499 N.E.2d 738, 741 (Ind. 1986) (declining to divine "[w]hether a federal Fifth Amendment right to due process attaches to a state grand jury proceeding"). This bedrock principle does not change—it has never been, and never will be, our role to predict decisions by the U.S. Supreme Court.

As Justice Jackson so famously proclaimed about the U.S. Supreme Court, "[w]e are not final because we are infallible, but we are infallible only because **we are final**." *Brown v. Allen*, 344 U.S. 443, 540, 73 S.Ct. 397, 97 L.Ed. 469 (1953) (Jackson, J., concurring) (emphasis added). "What, indeed, might then have been only prophecy"—that our Court now firmly establishes that it will reject that finality by ***968** deciding cases that can bypass the revising authority of the U.S. Supreme Court on important questions of federal constitutional law—"has now become fact." *Martin*, 14 U.S. (1 Wheat.) at 348. By deciding this case, the Court's message is crystal clear: it will anoint itself, at times, as the final adjudicator of federal law. To this, I cannot assent.

And as for the adjudication of that federal law, this Fifth Amendment question is the closest of close calls. Courts around the country split, falling into two camps. *See generally* Orin S. Kerr, *Compelled Decryption and the Privilege Against Self-Incrimination*, 97 Tex. L. Rev. 767 (2019); Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr*, 97 Tex. L. Rev. Online 63 (2019). Reasonable minds can disagree; indeed, many have. Our Court's decision on the merits today is thus not unreasonable, though I would come out the other way for the reasons further explained by Professor Kerr.[5]

Slaughter, J., joins in part.

Slaughter, J., dissenting.

I respectfully dissent. Although I agree with Justice Massa that this case is moot, I write separately because I disagree that a mootness exception justifies our reaching the merits of Seo's constitutional claim. In ***969** my view, our prevailing mootness standard does not conform to our constitution's mandate of separate governmental powers. In lieu of our prevailing standard, I would adopt the federal standard because, consistent with Article 3, Section 1 of our state constitution, it requires that courts decide only actual disputes. Applying this standard here, I would find Seo's appeal moot and not reach the merits of her Fifth Amendment claim.

A

As Justice Massa recites correctly, appellate case law in Indiana holds that our courts may decide otherwise moot cases if the legal question is sufficiently important and will likely recur. The Court says that Seo's appeal is such a case, thus justifying our reaching the merits even if her case were moot. Although case authority generally supports such a broad mootness exception, the cases are not uniform.

Some cases appear to have applied the stricter federal exception, in which a court will not decide a moot issue unless it is capable of repetition, yet evading review. But courts that have applied the federal exception confuse the issue by also invoking our laxer state mootness standard. See, e.g., *Horseman v. Keller*, 841 N.E.2d 164, 170 (Ind. 2006) (invoking state standard first: "Where there is a matter of great public importance, however, and the possibility of repetition, Indiana courts may choose to adjudicate a claim."; but concluding with federal standard: "Because the question before us is capable of repetition, yet evading review, we now address the constitutionality of [the disputed statute].") (cleaned up); *Gaither v. Indiana Dep't of Correction*, 971 N.E.2d 690, 693-94 (Ind. Ct. App. 2012) (same).

I would clarify any ambiguity in our appellate precedent and hold that any mootness doctrine consistent with our state constitution's mandate of separate governmental powers requires an actual dispute.

B

Our constitution divides the powers of government among "three separate departments; the Legislative, the Executive including the Administrative, and the Judicial". Ind. Const. art. 3, § 1. It also mandates that "except as in this Constitution expressly provided", "no person, charged with official duties under one of these departments, shall exercise any of the functions of another". *Id.* After discussing the powers and functions of the other departments, our constitution charges courts with exercising the "judicial power". *Id.* art 7, § 1. This delegation of power to the judiciary has two aspects: courts may exercise only the judicial power; and only courts may exercise this power. *Id.*

What, precisely, is the judicial power? It is the power to resolve actual disputes between adverse parties by issuing binding decrees that pronounce the parties' rights and responsibilities and afford meaningful relief to the prevailing party. Although our constitution does not contain an express "case or controversy" requirement like Article III of the federal constitution, "our explicit separation of powers clause fulfills a similar function." *Pence v. State*, 652 N.E.2d 486, 488 (Ind. 1995). Relevant here, that function limits courts to deciding justiciable controversies.

Justiciability concerns the power and propriety of a court to hear a case and award relief. As I wrote in *Horner v. Curry*, standing is an essential aspect of justiciability because it ensures that a judicial decree redresses an actual injury attributable to the defendant's wrong. 125 N.E.3d 584, 612, 615 (Ind. 2019) (Slaughter, J., concurring in the judgment). Also essential are the related doctrines of ripeness and mootness. Standing asks **who** ***970** may bring suit. Ripeness and mootness ask **when** suit may be brought. With ripeness, the issue is whether the claim has sufficiently developed—matured—into an actual controversy so that courts are resolving real disputes, not anticipated cases based on hypothetical facts. With mootness, the issue is whether a once-mature claim has "over-ripened" to the point that a court's judgment can no longer afford the claimant effective relief.

These justiciability doctrines respect and implement separation of powers. They ensure that the judiciary retains its proper role within our constitutional order and leaves the political branches undisturbed, absent a legal wrong. And even then, courts will not exercise their power unless a claimant has standing and the case is ripe. In other words, courts will hear a case only when a claim is sufficiently mature such that the claimant has sustained an actual injury; the claimant can obtain meaningful relief from a judgment against the defendant; and the claimant continues to have a personal stake in the outcome throughout the lawsuit. What follows from these doctrines is that the only mootness standard consistent with our constitution's requirement of distributed governmental powers is one requiring an actual, ongoing controversy between adverse parties. The federal mootness standard fills that bill.

To be justiciable, the federal standard requires that an otherwise moot case be capable of repetition, yet evading review. See *Honig v. Doe*, 484 U.S. 305, 318–20, 108 S.Ct. 592, 98 L.Ed.2d 686 (1988). In other words, it requires a case to present a question likely to recur between the same parties in circumstances that will likely skirt judicial review. See *id.* Although the evade-review requirement is a prudential consideration, the capable-of-repetition requirement is constitutionally required, demanding a "demonstrated probability" that the same issue will arise between the same parties. *Murphy v. Hunt*, 455 U.S. 478, 482, 102 S.Ct. 1181, 71 L.Ed.2d 353 (1982). "Where the conduct has ceased for the time being but there is a demonstrated probability that it **will** recur, a real-life controversy between parties with a personal stake in the outcome continues to exist[.]" *Honig*, 484 U.S. at 341, 108 S.Ct. 592 (Scalia, J., dissenting) (emphasis in original). Thus, this so-called "exception" to the mootness doctrine is really no exception at all but a test for determining whether an actual dispute remains.

In contrast, Indiana's prevailing mootness doctrine rejects the narrow federal doctrine, see *Matter of Lawrance*, 579 N.E.2d 32, 37 (Ind. 1991), and recognizes an open-ended exception for moot cases involving "questions of great public interest". *Id.* (cleaned up). Although these cases "typically contain issues likely to recur", *id.*, we assess whether the issues are likely to recur not with reference to a case's specific parties but to any conceivable party.

See *id.* Thus, a court may decide an otherwise moot case if someone—anyone—may face the same issue in the future. But this lone requirement—an issue of great public importance likely to recur—does not make a case suitable for adjudication under our constitution. The case must have a demonstrated probability that it will recur between the same parties; otherwise, there is no actual dispute, and any adjudication exceeds the judicial power.

Not only does our mootness doctrine lack any tie to our essential, though limited, constitutional role, but how we apply our justiciability principles has proved unpredictable in practice. Just last month, we held unanimously that the governor could not intervene in a pending disciplinary action involving the attorney general. *Matter of Hill*, 144 N.E.3d 200 (Ind. 2020). The governor asked us to answer the timely, pressing question whether our thirty-day ***971** suspension of the attorney general's law license created a vacancy in the office that triggered the governor's legal duty to fill it. No one disputed that the governor's motion raised an issue of "great public importance". Yet we denied intervention—correctly, in my view—because, among other reasons, we do not issue advisory opinions and the governor had no legally cognizable interest in the underlying case. In other words, the proposed intervention lacked the criteria for justiciability, despite the importance of the issue raised.

C

Even if I agreed that Seo has raised a "novel, important issue of great public importance that will surely recur", that standard cannot be reconciled with the actual-injury requirement implicit in our constitution's separation-of-powers command. Instead, I would adopt "capable of repetition, yet evading review" as our mootness standard. Applying it here, I would hold that Seo's Fifth Amendment claim is moot and not reach the merits.

All Citations

148 N.E.3d 952

Footnotes

1 Our dissenting colleagues are incorrect in finding this case moot, as there has not yet been "a settlement of all differences between the parties," *Gompers v. Buck's Stove & Range Co.*, 221 U.S. 418, 451, 31 S.Ct. 492, 55 L.Ed. 797 (1911). Justice Massa asks, "What could the State now gain from Seo unlocking her device?" *Post*, at 964. But the State has already answered that question—to complete its investigation of Seo and potentially file additional charges. After pleading guilty, Seo filed a motion requesting that law enforcement return her iPhone—which has remained in police custody since it was seized—because she had "no pending criminal cases." The State objected, and during a hearing on the motion, the State clarified that its interest in accessing Seo's iPhone is "not limited" to just the charges covered by the plea agreement. The prosecutor explained that the State could not "do a full investigation" or "be in a position to either not bring or choose to bring new cases" until it had evidence from the device. Then at oral argument, the State not only reiterated its continued interest in searching Seo's iPhone but also argued that the case was not moot because the "threat of a sanction still hangs over [Seo's] head." So, contrary to the dissenting view, the State has not settled all claims with Seo; and the stayed contempt order has not automatically terminated. *See* *Pac. Bell Tel. Co. v. Linkline Commc'ns, Inc.*, 555 U.S. 438, 446–47, 129 S.Ct. 1109, 172 L.Ed.2d 836 (2009) (recognizing that a case is not moot when there "remains a live dispute"); *United States v. Harris*, 582 F.3d 512, 516 (3d Cir. 2009) (finding that the termination of underlying criminal proceedings did not render a coercive civil contempt order moot when the purpose and intent of the order "remain alive and well"). In short, this case presents a

live dispute and thus our decision renders effective relief. But irrespective of mootness, this case presents a novel, important issue of great public importance that will surely recur.

2 *Fisher* recognized that compelling the attorneys to hand over the documents did not "implicate whatever Fifth Amendment privilege the taxpayer might have enjoyed from being compelled to produce them himself." 425 U.S. at 402, 96 S.Ct. 1569. But because the taxpayers had transferred the documents for legal advice protected by the attorney–client privilege, *id.* at 403–04, 96 S.Ct. 1569, the Court addressed whether the Government could have compelled the taxpayers themselves to produce the documents, *id.* at 405, 96 S.Ct. 1569.

3 The majority of courts to address the scope of testimony implicated when a suspect is compelled to produce an unlocked smartphone have reached a similar conclusion. *See State v. Trant*, No. 15-2389, 2015 WL 7575496, at *2–3 (D. Me. Oct. 27, 2015); *Sec. & Exch. Comm'n v. Huang*, No. 15-269, 2015 WL 5611644, at *2–4 (E.D. Penn. Sept. 23, 2015); *Pollard v. State*, 287 So. 3d 649, 656–57 (Fla. Dist. Ct. App. 2019), *reh'g denied*; *G.A.Q.L. v. State*, 257 So. 3d 1058, 1061–65 (Fla. Dist. Ct. App. 2018); *People v. Spicer*, 430 Ill.Dec. 268, 125 N.E.3d 1286, 1290–92 (Ill. App. Ct. 2019); *In re Grand Jury Investigation*, 92 Mass.App.Ct. 531, 88 N.E.3d 1178, 1180–82 (2017); *cf. United States v. Wright*, 431 F. Supp. 3d 1175, 1186–88 (D. Nev. 2020); *In re Search Warrant Application for Cellular Tel. v. Barrera*, 415 F. Supp. 3d 832, 838 n.2 (N.D. Ill. 2019); *In re Residence in Oakland, Cal.*, 354 F. Supp. 3d 1010, 1016 (N.D. Cal. 2019); *In re Application for a Search Warrant*, 236 F. Supp. 3d 1066, 1073 (N.D. Ill. 2017); *State v. Diamond*, 905 N.W.2d 870, 875 (Minn. 2018).

4 Pew Research Ctr., Mobile Fact Sheet (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/8ZUY-EJDG].

5 *See* Steve McCaskill, *iPhone XR Was Best-Selling Smartphone of 2019*, TechRadar (Feb. 26, 2020), https://www.techradar.com/news/iphone-xr-was-best-selling-smartphone-of-2019[https://perma.cc/6PAC-WZT9]; Apple iPhone XR Tech Specs, https://www.apple.com/iphone-xr/specs/ [https://perma.cc/X9MU-Q9W4]; *How Many Pages in a Gigabyte?*, Lexis Nexis Discovery Series Fact Sheet, https://www.lexisnexis.com/applieddiscovery/lawlibrary/whitePapers/ADI_ FS_PagesInAGigabyte.pdf [https://perma.cc/JJP7-JQK5].

6 *See* *In re Application for a Search Warrant*, 236 F. Supp. 3d at 1068, 1072–74; *Trant*, 2015 WL 7575496, at *2–3; *Huang*, 2015 WL 5611644, at *2–4; *Pollard*, 287 So. 3d at 657; *G.A.Q.L.*, 257 So. 3d at 1063–65; *Spicer*, 430 Ill.Dec. 268, 125 N.E.3d at 1290–92; *In re Grand Jury Investigation*, 88 N.E.3d at 1181–82. And several courts evaluating this issue in the context of other electronic devices, such as computers or hard drives, have similarly required the government to identify the information sought with reasonable particularity. *See* *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1345–47 (11th Cir. 2012); *In re Decryption of a Seized Data Storage Sys.*, No. 13-M-449, 2013 WL 12327372, at *4 (E.D. Wis. Apr. 19, 2013); *United States v. Hatfield*, No. 06-CR-0550 (JS), 2010 WL 1423103, at *1–2 (E.D.N.Y. Apr. 7, 2010); *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718, at *3–4 (D. Vt. Feb. 19, 2009); *cf.* *United States v. Apple MacPro Comput.*, 851 F.3d 238, 247–48 (3d Cir. 2017); *In re Search of a Residence*, No. 17-mj-70656-JSC-1, 2018 WL 1400401, at *8–12 (N.D. Cal. Mar. 20, 2018).

7 *See* *United States v. Jimenez*, 419 F. Supp. 3d 232, 233 (D. Mass. 2020); *Wright*, 431 F. Supp. 3d at 1186–88; *In re Residence in Oakland*, 354 F. Supp. 3d at 1016–18; *Davis*, 220 A.3d at 550.

1 *See also* State ex rel. Corn v. Russo, 90 Ohio St.3d 551, 740 N.E.2d 265, 269 (2001) ("It is well established that where the parties settle the underlying case that gave rise to the civil contempt sanction, the contempt proceeding is moot, since the case has come to an end."); Christensen v. Sullivan, 320 Wis.2d 76, 768 N.W.2d 798, 815 (2009) ("[T]he most obvious case of a contempt of court that has been terminated and is no longer continuing occurs when the underlying dispute between the parties has been settled."); 17 Am. Jur. 2d Contempt § 147 ("When the parties settle the underlying case that gave rise to a civil contempt sanction, the contempt proceeding is moot since the case has come to an end.").

2 To be sure, the trial court granted, nearly simultaneously, two "search warrants" involving Seo's cases, and this filing only "returned" the first. But in the request for the second, the State acknowledged that the trial court had already "issued a search warrant (cause number 29D01-1708-MC-5624)" for Seo's phone and merely additionally requested "that the court compel Katelin Eunjoo Seo to unlock the cell phone at issue," and that Seo "be subject to the contempt powers of the Court" if she failed to comply. Affidavit for Probable Cause, *In Re: Search Warrant*, No. 29D01-1708-MC-5640 (Hamilton Sup. Ct.).

3 If state courts find in favor of, but not against, asserted federal rights for non-Article III litigants, opposing parties may seek Supreme Court review because they, in some way, "are faced with 'actual or threatened injury' that is sufficiently 'distinct and palpable' to support" justiciability. ASARCO Inc. v. Kadish, 490 U.S. 605, 618, 109 S.Ct. 2037, 104 L.Ed.2d 696 (1989) (quoting Warth v. Seldin, 422 U.S. 490, 500, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975). But this asymmetrical grant of appeal crumbles under scrutiny. Suppose this Court held, correctly in my view, that Seo's Fifth Amendment rights were not violated. Under *ASARCO*, that holding—**declining** to clairvoyantly extend a criminal defendant's federal rights—evades U.S. Supreme Court review. That peculiarity alone should counsel this Court against deciding federal questions "in the rarified atmosphere of a debating society," *id.* at 636, 109 S.Ct. 2037 (Rehnquist, C.J., concurring in part and dissenting in part), especially considering the Judiciary Act of 1789 authorized Supreme Court review of state court decisions **only** when the state court decided a federal question **adversely** to the claimed federal right, Judiciary Act of 1789, ch. 20, § 25, 1 Stat. 73, 85–87 (1789).

4 Indeed, "Indiana has its own system of legal, including constitutional, protections" subject to our ultimate review. *State v. Timbs*, 84 N.E.3d 1179, 1184 (Ind. 2017), *vacated and remanded*. Although Seo mentioned Article 1, Section 14 in her briefing at the Court of Appeals (she filed nothing with this Court), she made no separate self-incrimination argument under the Indiana Constitution. *See* Ind. Const. art. 1, § 14 ("No person, in any criminal prosecution, shall be compelled to testify against himself."). Because she failed to offer a "separate analysis based on the state constitution," this "state constitutional claim is waived." *Dye v. State*, 717 N.E.2d 5, 11 n.2 (Ind. 1999). If she had separately and independently analyzed Article 1, Section 14, we could have considered Seo's case under our Indiana Constitution without needing to grapple with these heady Article III justiciability concerns.

5 A few months before our nation's bicentennial anniversary, the Supreme Court all but rang the death knell of longstanding precedent that barred the government from forcing a defendant "to give evidence that tends to criminate him," *Boyd v. United States*, 116 U.S. 616, 638, 6 S.Ct. 524, 29 L.Ed. 746 (1886), holding that the Fifth Amendment is not violated merely because the State compels a defendant to turn over incriminating evidence, *Fisher v. United States*, 425 U.S. 391, 409, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). But the endurance of that view remains to be seen. Indeed, at least three sitting Justices of the U.S. Supreme Court have questioned this understanding. *See* *Carpenter v. United States*, —— U.S. ——, 138 S. Ct. 2206, 2271, 201 L.Ed.2d 507 (2018) (Gorsuch, J., dissenting) ("[T]here is substantial evidence that the

privilege against self-incrimination was also originally understood to protect a person from being forced to turn over potentially incriminating evidence."); *United States v. Hubbell*, 530 U.S. 27, 49, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) (Thomas, J., concurring) ("A substantial body of evidence suggests that the Fifth Amendment privilege protects against the compelled production not just of incriminating testimony, but of any incriminating evidence."); Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. Pitt. L. Rev. 27, 78 (1986) ("The individuals who framed, adopted, and ratified the fifth amendment left no clear evidence that they ever considered the application of the privilege to subpoenas for documents."). Even then-Justices Brennan and Stevens—no originalists!—agreed that the new framework unnecessarily and detrimentally departed from *Boyd*. *See* *Fisher*, 425 U.S. at 414, 96 S.Ct. 1569 (Brennan, J., concurring in the judgment) (Because it represented "a serious crippling of the protection secured by the privilege against compelled production of one's private books and papers," *Fisher* was "but another step in the denigration of privacy principles settled nearly 100 years ago" in *Boyd*.); *Doe v. United States*, 487 U.S. 201, 221 n.2, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988) (Stevens, J., dissenting) ("The Fifth Amendment provides that no person 'shall be compelled in any criminal case to be a **witness** against himself.' A witness is one who 'gives evidence in a cause.' T. Cunningham, 2 New and Complete Law Dictionary (2d ed. 1771)."). A return to *Boyd* would end the constitutional hair-splitting that results when applying old precedents to new technology in this digital age. But this Court, especially in a moot case, should not prognosticate *Boyd*'s resurrection. *Cf.* *Timbs*, 84 N.E.3d at 1183 (choosing "to await guidance from the Supreme Court and decline to find or assume incorporation until the Supreme Court decides the issue authoritatively"). The Supreme Court must, at some point, decide how to apply its modern Fifth Amendment jurisprudence to the compelled unlocking of a smartphone or, perhaps, return to *Boyd*. In the meantime, that uncertainty further counsels that we dismiss this appeal as moot.

End of Document

243 N.J. 447
Supreme Court of New Jersey.

STATE of New Jersey, Plaintiff-Respondent,
v.
Robert ANDREWS, Defendant-Appellant.

A-72 September Term 2018
|
082209
|
Argued January 21, 2020
|
Decided August 10, 2020

Synopsis

Synopsis

Background: Defendant, who was a former county sheriff's officer, was indicted for second-degree official misconduct, third-degree hindering the apprehension or prosecution of another person, and fourth-degree obstructing the administration of the law or government function, arising out of his alleged efforts to help the target of a state narcotics investigation avoid criminal exposure. After state investigators were unable to access the information on defendant's seized smartphones, the Superior Court, Law Division, Essex County, granted State's motion to compel defendant to disclose the passcodes required to unlock the smartphones. Defendant filed motion for leave to appeal, which was denied, then filed motion for leave to appeal to the Supreme Court, which granted the motion and summarily remanded to the Superior Court, Appellate Division to consider defendant's arguments on the merits. The Superior Court, Appellate Division, Yannotti, J.A.D., 457 N.J. Super. 14, 197 A.3d 200, affirmed. Defendant sought leave to appeal, which was granted.

Holdings: In a case of first impression, the Supreme Court, Solomon, J., held that:

[1] Fifth Amendment privilege against self-incrimination did not protect defendant from the compelled disclosure of the passcodes;

[2] passcodes were not "incriminating," within meaning of statutes and evidence rules codifying the state law protection against compelled self-incrimination; and

[3] state common law privilege against self-incrimination was not violated by order compelling defendant to disclose the passcodes.

Affirmed and remanded.

LaVecchia, J., filed dissenting opinion in which Albin and Timpone, JJ., joined.

Procedural Posture(s): Appellate Review; Pre-Trial Hearing Motion.

West Headnotes (29)

[1] **Searches and Seizures** Persons, Places and Things Protected

Searches and Seizures Formal requirements

Searches and Seizures Particularity or generality and overbreadth in general

The Fourth Amendment to the United States Constitution and the corresponding provision of the state constitution protect individuals' rights to be secure in their persons, houses, papers, and effects by requiring that search warrants be supported by oath or affirmation and describe with particularity the places subject to search and people or things subject to seizure. U.S. Const. Amend. 4; N.J. Const. art. 1, par. 7.

[2] **Searches and Seizures** Search under warrant

Searches executed pursuant to warrants compliant with the constitutional requirements that they be supported by oath or affirmation

and describe with particularity the places subject to search are presumptively valid. U.S. Const. Amend. 4; N.J. Const. art. 1, par. 7.

[3] **Searches and Seizures** Scope of inquiry or review, in general

Reviewing courts should pay substantial deference to judicial findings of probable cause in search warrant applications. U.S. Const. Amend. 4; N.J. Const. art. 1, par. 7.

[4] **Searches and Seizures** Execution and Return of Warrants

The State has broad authority to effectuate searches permitted by valid search warrants. U.S. Const. Amend. 4; N.J. Const. art. 1, par. 7.

[5] **Searches and Seizures** Execution and Return of Warrants

Searches and Seizures Manner of Entry; Warning and Announcement

Pursuant to the state's broad authority to effectuate search warrants, the State may destroy property, forcibly enter a residence, and employ flash-bang devices, among other things, all in the name of executing a warrant. U.S. Const. Amend. 4; N.J. Const. art. 1, par. 7.

[6] **Criminal Law** Compelling Self-Incrimination

A lawful seizure does not allow compelled disclosure of facts otherwise protected by the Fifth Amendment privilege against self-incrimination. U.S. Const. Amends. 4, 5; N.J. Const. art. 1, par. 7.

[7] **Witnesses** Self-Incrimination

The Fifth Amendment right against self-incrimination applies only when the accused is compelled to make a testimonial communication that is incriminating. U.S. Const. Amend. 5.

[8] **Witnesses** Self-Incrimination

Testimonial communications may take any form, but must imply assertions of fact for the Fifth Amendment privilege against self-incrimination to attach. U.S. Const. Amend. 5.

[9] **Criminal Law** Compelling Self-Incrimination

Actions that do not require an individual to disclose any knowledge he might have or to speak his guilt are nontestimonial and therefore not protected by the Fifth Amendment privilege against self-incrimination. U.S. Const. Amend. 5.

[10] **Criminal Law** Exposing accused or person of accused to view of witness or jury, and compelling submission to physical examination

Criminal defendants may lawfully be compelled to display their physical characteristics and commit physical acts without violating the Fifth Amendment privilege against self-incrimination, because the display of physical characteristics is not coterminous with communications that relay facts. U.S. Const. Amend. 5.

[11] **Criminal Law** Compelling Self-Incrimination

Among the acts that a criminal defendant may be compelled to commit without violating the Fifth Amendment privilege against self-incrimination, because such acts are not communications relaying facts, are creating handwriting samples and voice samples, providing blood, hair, and saliva samples, standing in a lineup, and donning particular articles of clothing. U.S. Const. Amend. 5.

[12] **Criminal Law** Compelling Self-Incrimination

Consistent with the Fifth Amendment privilege against self-incrimination, individuals may be compelled to execute an authorization directing a foreign bank to disclose account records, because neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information to the Government. U.S. Const. Amend. 5.

[13] **Witnesses** Self-Incrimination

The Fifth Amendment privilege against self-incrimination is not an absolute bar to a defendant's forced assistance of the defendant's own criminal prosecution. U.S. Const. Amend. 5.

[14] **Witnesses** Self-Incrimination

In contrast to compelled physical communications, which do not generally violate the Fifth Amendment, if an individual is compelled to disclose the contents of his own mind, such disclosure implicates the Fifth Amendment privilege against self-incrimination. U.S. Const. Amend. 5.

[15] **Witnesses** Privilege as to production of documents

For purposes of the Fifth Amendment privilege against self-incrimination, the act of production must be considered in its own right, separate from the documents sought. U.S. Const. Amend. 5.

[16] **Witnesses** Privilege as to production of documents

Even production that is of a testimonial nature can be compelled, consistent with the Fifth Amendment privilege against self-incrimination, if the Government can demonstrate it already knows the information that act will reveal -- if, in other words, the existence of the requested documents, their authenticity, and the defendant's possession of and control over them, are a foregone conclusion. U.S. Const. Amend. 5.

[17] **Witnesses** Privilege as to production of documents

Communicating or entering a computer or smartphone passcode requires facts contained within the holder's mind, that is, the numbers, letters, or symbols composing the passcode; thus, it is a testimonial act of production for purposes of the Fifth Amendment privilege against self-incrimination. U.S. Const. Amend. 5.

[18] **Witnesses** Privilege as to production of documents

The "foregone conclusion" exception to the act of production doctrine, under which compelled testimonial acts of production do not violate the Fifth Amendment privilege against self-incrimination if the State establishes its knowledge of the existence of the evidence demanded, the defendant's possession and control of that evidence, and the authenticity of the evidence, applies to production of a passcode used to unlock a smartphone, rather than to the phone's contents. U.S. Const. Amend. 5.

[19] **Witnesses** Privilege as to production of documents

Although the act of producing the passcode used to unlock a smartphone is presumptively protected by the Fifth Amendment, its testimonial value and constitutional protection may be overcome if the passcode's existence, possession, and authentication are foregone conclusions. U.S. Const. Amend. 5.

[20] **Witnesses** Privilege as to production of documents

"Foregone conclusion" exception to the act of production doctrine applied to State's motion to compel defendant charged with official misconduct and other offenses to provide the passcodes to unlock two smartphones that had been seized, and thus Fifth Amendment privilege against self-incrimination did not protect defendant from the compelled disclosure of the passcodes; State established the existence of the passcodes by showing that the contents of the phones were passcode-protected, State established defendant's knowledge of the passcodes by showing that defendant owned and used the phones, which were in his possession when they were seized, and to the extent authentication was an issue, the passcodes would self-authenticate by providing access to the phones. U.S. Const. Amend. 5.

[21] **Criminal Law** Questions of Fact and Findings

Supreme Court gives deference to the trial court's factual findings and views them as binding upon appeal to the extent that they are supported by adequate, substantial and credible evidence.

[22] **Witnesses** Self-Incrimination

New Jersey's state law privilege against compelled self-incrimination is not expressed in state constitution, but the privilege is deeply rooted in the state's common law and codified in both statute and an evidence rule. N.J. Stat. Ann. §§ 2A:84A-18, 2A:84A-19; N.J. R. Evid. 503.

[23] **Witnesses** Self-Incrimination

Statutes codifying the state law protection against compelled self-incrimination define the right against self-incrimination, but also set forth specific limitations on that right. N.J. Stat. Ann. §§ 2A:84A-18, 2A:84A-19.

[24] **Witnesses** Self-Incrimination

Under statutes and rule of evidence codifying the state law protection against self-incrimination, for the right to refuse to disclose an incriminatory matter to apply, a matter must first be found to be incriminating. N.J. Stat. Ann. §§ 2A:84A-18, 2A:84A-19; N.J. R. Evid. 503.

[25] **Witnesses** Privilege as to production of documents

Passcodes needed to unlock two smartphones seized from defendant charged with official misconduct and other offenses were not "incriminating," within meaning of statutes and evidence rules codifying the state law protection against compelled self-incrimination, and thus compelled production of those passcodes did not violate the statutes or rules; passcodes were not an element of any crime with which defendant was charged, fact of defendant's ownership and control of the phones and their contents had already been established, and the passcodes themselves were merely amalgamations of characters with minimal evidentiary significance that did not support an inference that a crime had been committed. N.J. Stat. Ann. §§ 2A:84A-18, 2A:84A-19; N.J. R. Evid. 502, 503.

[26] **Witnesses** Privilege as to production of documents

Where ownership and control of an electronic device is not in dispute, its passcode is generally not substantive information, is not a clue to an element of or the commission of a crime, and does not reveal an inference that a crime has been committed, for purposes of the state law privilege against self-incrimination. N.J. Stat. Ann. §§ 2A:84A-18, 2A:84A-19; N.J. R. Evid. 502, 503.

[27] **Witnesses** Self-Incrimination

State common law privilege against self-incrimination generally parallels federal constitutional doctrine, but also offers broader protection than its federal counterpart under the Fifth Amendment. U.S. Const. Amend. 5.

[28] **Witnesses** Self-Incrimination

In contrast to federal law which distinguishes between Fourth and Fifth Amendment inquiries, New Jersey's common law views the privilege against self-incrimination as incorporating privacy considerations. U.S. Const. Amends. 4, 5.

[29] **Witnesses** Privilege as to production of documents

State common law privilege against self-incrimination, which incorporated privacy considerations, was not violated by order compelling defendant who was charged with official misconduct and other offenses to disclose the passcodes needed to unlock two seized smartphones; privacy considerations applicable to portions of the phones' contents of which disclosure had been ordered had already been considered and overcome through unchallenged search warrants granted in the prosecution. U.S. Const. Amend. 4; N.J. Const. art. 1, par. 7.

****1258** On appeal from the Superior Court, Appellate Division, whose opinion is reported at 457 N.J. Super. 14, 197 A.3d 200 (App. Div. 2018).

Attorneys and Law Firms

Charles J. Sciarra, Clifton, argued the cause for appellant (Sciarra & Catrambone, attorneys; Charles J. Sciarra, of counsel, and Deborah Masker Edwards, on the briefs).

Frank J. Ducoat, Special Deputy Attorney General/Acting Assistant Prosecutor, argued the cause for respondent (Theodore N. Stephens, II, Acting Essex County Prosecutor, attorney; Frank J. Ducoat, of counsel and on the briefs, and Caroline C. Galda, Special Deputy Attorney General/Acting Assistant Prosecutor, on the briefs).

Elizabeth C. Jarit, Deputy Public Defender, argued the cause for amicus curiae Public Defender of New Jersey (Joseph E. Krakora, Public Defender, attorney; Elizabeth C. Jarit, of counsel and on the brief).

Andrew Crocker (Electronic Frontier Foundation) of the California bar, admitted pro hac vice, argued the cause for amici curiae Electronic Frontier Foundation, American Civil Liberties Union, and American Civil Liberties Union of New Jersey (Electronic Frontier Foundation, American Civil Liberties Union Foundation, and American Civil Liberties Union of New Jersey Foundation, attorneys; Andrew Crocker, Jennifer Granick (American Civil Liberties Union Foundation) of the California bar, admitted pro hac vice, Alexander Shalom, and Jeanne LoCicero, on the brief).

Christopher J. Keating argued the cause for amicus curiae New Jersey State Bar Association (New Jersey State Bar Association, attorneys; Evelyn Padin, President, Hoboken, of counsel, and Christopher J. Keating, Richard F. Klineburger, Haddonfield, Brandon D. Minde, and Matheu D. Nunn, Denville, on the brief).

Megan Iorio (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, argued the cause for amicus curiae Electronic Privacy Information Center (Barry, Corrado, Grassi & Gillin-Schwartz and Electronic Privacy Information Center, attorneys; Megan Iorio, Alan Butler (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, Marc Rotenberg (Electronic Privacy Information Center) of the District of Columbia bar, admitted pro hac vice, and Frank L. Corrado, Wildwood, on the brief).

Matthew S. Adams argued the cause for amicus curiae Association of Criminal Defense Lawyers of New Jersey (Fox Rothschild, attorneys; Matthew S. Adams, Jordan B. Kaplan, Marissa Koblitz Kingman, and Victoria Salami, Morristown, on the brief).

Lila B. Leonard, Deputy Attorney General, argued the cause for amicus curiae Attorney General of New Jersey (Gurbir S. Grewal, Attorney General, attorney; Lila B. Leonard, of counsel and on the brief).

Gregory R. Mueller, First Assistant Sussex County Prosecutor, argued the cause for amicus curiae County Prosecutors Association of New Jersey (Francis A. Koch, Sussex County Prosecutor, President, attorney; Gregory R. Mueller, of counsel and on the brief).

Opinion

JUSTICE SOLOMON delivered the opinion of the Court.

****1259** ***456** This appeal presents an issue of first impression to our Court -- whether a court order requiring a criminal defendant to disclose the passcodes to his passcode-protected cellphones violates the Self-Incrimination Clause of the Fifth Amendment to the United States Constitution or New Jersey's common law or statutory protections against self-incrimination. We conclude that it does not and affirm the Appellate Division's judgment.

The target of a State narcotics investigation advised detectives that defendant, a law enforcement officer, had provided him with information about the investigation and advice to avoid criminal exposure. The target gave statements to investigators, confirmed in part by his cellphone, about photographs, cellphone calls, text message exchanges, and conversations with defendant during which defendant recommended that the target remove a tracking device that may have been placed on his car by the police; recommended that the target discard cellphones he and his cohorts used; and revealed the identity of an undercover officer and an undercover police vehicle.

The State obtained an arrest warrant for defendant and search warrants for defendant's iPhones, which were seized. Because the contents of the iPhones were inaccessible to investigators without the iPhones' passcodes, the State moved for an order compelling defendant to disclose the passcodes.

Defendant claimed the United States Constitution and New Jersey's common law and statutory protections against compelled self-incrimination protected his disclosure of the passcodes. The motion court and Appellate Division concluded that defendant's disclosure of the passcodes could be compelled. We agree and affirm.

I.

The State claims that defendant Robert Andrews, a former Essex County Sheriff's Officer, revealed an undercover narcotics investigation to its target, Quincy Lowery.

***457** The motion court and Appellate Division records disclose that Essex County Prosecutor's Office detectives went to the Essex County Sheriff's Office to interview Andrews, with his counsel present, about his association with Lowery. Andrews's attorney told the detectives that his client did "not wish to speak to anyone" and would be invoking his Fifth Amendment ****1260** privilege against self-incrimination. The attorney also requested the return of Andrews's two cellphones seized earlier that day. The detectives advised Andrews and his counsel that the cellphones were seized in connection with a criminal investigation and would not be immediately returned, but that Andrews was free to leave.

Later that day, detectives from the Essex County Prosecutor's Office interviewed Lowery, who detailed his relationship with Andrews. Lowery explained that they were members of the same motorcycle club and had known each other for about a year. During that time, Andrews registered a car and motorcycle in his name so that Lowery could use them. Lowery also told the detectives that he regularly communicated with Andrews using the FaceTime application on their cellphones.

Lowery claimed that during one of those communications, Andrews told him to "get rid of" his cellphones because law enforcement officials were "doing wire taps" following the federal arrests of Crips gang members.[1] According to Lowery, Andrews said that the State Police and the Sheriff's Office were "going to do a run" and Lowery should "just be careful."

Lowery also explained that he had suspected he was being followed by police officers after receiving a tip from a fellow drug dealer who observed a white van outside of Lowery's residence. Lowery relayed that suspicion to

Andrews and texted him the license plate number of one of the vehicles Lowery believed was following him. According to Lowery, Andrews informed him that the license plate number belonged either to the Prosecutor's Office ***458** or the Sheriff's Department and advised him to put his car "on a lift to see if there is a [tracking] device under there."

Lowery reported that he "stopped hustling" and discarded one of his cellphones after realizing he was being followed. Lowery also described one occasion when he noticed a man enter a restaurant shortly after Lowery arrived. Lowery explained that he suspected the man was an undercover police officer after noticing a bulge, believed to be a gun, on his hip. Using his cellphone, Lowery surreptitiously photographed the man. Lowery claimed that later that day he showed the picture to Andrews who identified the individual as a member of the Prosecutor's Office.

Further investigation following Lowery's statements largely corroborated his allegations. Lowery's Samsung Galaxy S5 cellphone was sent to the Cyber Crimes Unit for data extraction. The extraction report revealed that Lowery changed his telephone number shortly after he claims Andrews informed him of a potential wiretap. The report also revealed that two days after changing his number, Lowery texted an unknown subscriber to "Go get new phones." Seven minutes later, he texted another number advising that "Everybody around u need to get new ones 2."

A month later, Lowery texted a number associated with Andrews and asked "Where you at[?]" Forty-four minutes after that message, Lowery texted Andrews the license plate number of the car he suspected of following him. Lowery received a text message from one of Andrews's cellphone numbers two days later stating, "Bro call me we need to talk face to face when I get off."

****1261** Detectives later confirmed that the license plate number Lowery texted to Andrews was registered to a rental company and was being used by detectives on the Prosecutor's Office Narcotics Task Force. The extraction report also contained a photograph of a Narcotics Task Force detective matching the description of the undercover officer who followed Lowery into a restaurant. A review of State Motor Vehicle Commission records revealed that a 2002 Jeep Grand Cherokee Limited and 2007 Suzuki GSX motorcycle, ***459** which officers observed Lowery operating two weeks before his arrest, were registered to Andrews.

Following their second interview with Lowery, the State obtained Communication Data Warrants for cellphone numbers belonging to Andrews and Lowery. Over the next two weeks, the State sought and received additional search warrants for phones belonging to Lowery and Andrews, including a Communication Data Warrant for a second iPhone seized from Andrews. The warrants revealed 114 cellphone calls and text messages between Lowery and Andrews over a six-week period.

Andrews was indicted by an Essex County grand jury for (1) two counts of second-degree official misconduct (N.J.S.A. 2C:30-2); (2) two counts of third-degree hindering the apprehension or prosecution of another person (N.J.S.A. 2C:29-3(a)(2)); and (3) two counts of fourth-degree obstructing the administration of the law or other government function (N.J.S.A. 2C:29-1).

According to the State, its Telephone Intelligence Unit was unable to search Andrews's iPhones -- an iPhone 6 Plus and an iPhone 5s -- because they "had iOS systems greater [than] 8.1,[2] making them extremely difficult to access without the owner/subscriber's pass code." A State detective contacted and conferred with the New York Police Department's (NYPD) Technical Services unit, as well as a technology company called Cellebrite, both of which concluded that the cellphones' technology made them inaccessible to law enforcement agencies. The detective also consulted the Federal Bureau of Investigation's Regional Computer Forensics Laboratory, which advised that it employed "essentially ***460** the same equipment used by" the State and NYPD and would be unable to access the phones' contents. The State therefore moved to compel Andrews to disclose the passcodes to his two iPhones.

Andrews opposed the motion, claiming that compelled disclosure of his passcodes violates the protections against self-incrimination afforded by New Jersey's common law and statutes and the Fifth Amendment to the United States Constitution.

The trial court rejected Andrews's arguments, ruling that "the act of providing a PIN, password, or passcode is not a

testimonial act where the Fifth Amendment or New Jersey common and statutory law affords protection." The court reasoned that "[a]llowing the State to access the call logs and text messages on Andrews's iPhones will add little to nothing to the **1262 aggregate of the Government's information." The court added that "any testimonial act contained in the act of providing the PIN or passcode is a foregone conclusion because the State has established with reasonable particularity that it already knows that (1) the evidence sought exists, (2) the evidence was in the possession of the accused, and (3) the evidence is authentic."

Nevertheless, the trial court limited access to Andrews's cellphones "to that which is contained within (1) the 'Phone' icon and application on Andrews's two iPhones, and (2) the 'Messages' icon and/or text messaging applications used by Andrews during his communications with Lowery." The court also ordered that the search "be performed by the State, in camera, in the presence of Andrews's defense counsel and the [c]ourt," with the court "review[ing] the PIN or passcode prior to its disclosure to the State."

The Appellate Division denied Andrews's motion for leave to appeal from the trial court's order. We granted Andrews's motion for leave to appeal to this Court and summarily remanded to the Appellate Division to consider Andrews's arguments on the merits. State v. Andrews, 230 N.J. 553, 170 A.3d 331 (2017).

On remand, the Appellate Division affirmed the trial court's order requiring Andrews to disclose the passcodes to his two *461 iPhones. State v. Andrews, 457 N.J. Super. 14, 18, 197 A.3d 200 (App. Div. 2018). The panel acknowledged Andrews's Fifth Amendment concerns but held that the only testimonial aspects of providing the passcodes "pertain to the ownership, control, use, and ability to access the phones," which were facts already known to the State. Id. at 29, 197 A.3d 200. Therefore, the "foregone conclusion" exception to the "act of production" doctrine applied because the State "establish[ed] with reasonable particularity (1) knowledge of the existence of the evidence demanded; (2) defendant's possession and control of that evidence; and (3) the authenticity of the evidence." Id. at 22-23, 197 A.3d 200. In the Appellate Division's view, the State satisfied all three requirements of the exception by describing "the specific evidence it seeks to compel, which is the passcodes to the phones" and establishing that Andrews "exercised possession, custody, or control over" the seized iPhones. [3] Id. at 24, 197 A.3d 200.

The Appellate Division similarly rejected Andrews's state common law claims, noting the State would likely be unable to decipher information stored on the iPhones without their passcodes and that, when "the State has established the elements for application of the 'foregone conclusion' doctrine, New Jersey's common law privilege against self-incrimination does not bar compelled disclosure of passcodes for defendant's phones." Id. at 32, 197 A.3d 200.

Finally, the Appellate Division rejected Andrews's contention that the information sought is protected by N.J.S.A. 2A:84A-19 and N.J.R.E. 503, which provide protection from self-incrimination, subject to an exception for court orders compelling production of "a document, chattel or other thing" to which "some other person or a corporation or other association has a superior right." See id. at 32, 197 A.3d 200 (quoting N.J.S.A. 2A:84A-19(b); N.J.R.E. 503(b)). The panel concluded that the search warrants *462 issued for Andrews's iPhones "give the State a superior right to **1263 possession of the passcodes." Id. at 33, 197 A.3d 200.

We granted Andrews's motion for leave to appeal. 237 N.J. 572, 206 A.3d 964 (2019). We also granted amicus curiae status to the Office of the Attorney General, the County Prosecutors Association of New Jersey, the New Jersey State Bar Association, the Association of Criminal Defense Lawyers of New Jersey (ACDL), the Office of the Public Defender, the Electronic Frontier Foundation, the American Civil Liberties Union, the American Civil Liberties Union of New Jersey, and the Electronic Privacy Information Center.

II.

Andrews contends that the Appellate Division subverted New Jersey's broader privilege against self-incrimination and employed a "simplistic mechanical approach" to the Fifth Amendment's foregone conclusion exception. According to Andrews, that exception should not apply to digital technology because it "is distinctly different than paper documents," and the State "does not know what the passwords are, if Andrews knew them, or what is on the phones." Andrews also accuses the Appellate Division of treating his

state law right against self-incrimination as expendable and conflating the issuance of search warrants with ownership to construe the State's search as consistent with the language of N.J.S.A. 2A:84A-19(b).

The State argues in response that Andrews's contention concerning the exposure of incriminating information is baseless because the trial court's order mandates disclosure of the passcodes in camera prior to their communication to the State. Similarly, the State claims that the passcodes are "merely a random sequence of numbers with no testimonial significance," placing their compelled disclosure beyond the reach of the Fifth Amendment's Self-Incrimination Clause.

In answer to Andrews's state law claims, the State argues that communication between co-conspirators has no special privacy ***463** status, that the State "has established ... that it already knows what is on the phone[s]," and that the State has a superior right to the contents of the phones because of the unchallenged search warrant.

In support of the State, the County Prosecutors Association of New Jersey posits that the Fifth Amendment's privilege does not permit noncompliance with a search warrant valid under the Fourth Amendment. The Office of the Attorney General similarly warns that Andrews is attempting to use the Fifth Amendment to undermine the execution of a valid and enforceable search warrant. Additionally, the Attorney General argues that Andrews's constitutional, statutory, and common law rights against self-incrimination are not affected by the disclosure of his cellphone passcodes because compelled disclosure would communicate only his ability to unlock the phones.

The ACDL disagrees with the State and its supportive amici, contending that the Appellate Division's Fifth Amendment analysis was skewed by its focus on Andrews's ostensible knowledge of the phones' passcodes instead of the State's knowledge of the phones' contents. According to the ACDL, if we adopt the Appellate Division's reasoning with respect to mobile devices, self-incrimination protections will exist in name only.

The New Jersey State Bar Association, Electronic Frontier Foundation, American ****1264** Civil Liberties Union, and American Civil Liberties Union of New Jersey echo the ACDL's arguments and claim that the Fifth Amendment shields information that exists only in a criminal defendant's mind from government compelled disclosure. They also assert that the State failed to satisfy the reasonable particularity requirement of the foregone conclusion exception because it cannot identify the digital records it wants Andrews to produce through disclosure of his passcodes.

III.

The question before the Court -- whether defendant can be compelled to disclose the passcodes to his cellphones seized by law ***464** enforcement pursuant to a lawfully issued search warrant -- is ultimately answered by analyzing federal and state protections against compelled self-incrimination. But because the State contends that those protections do not allow defendant to ignore a lawfully issued search warrant, we begin with a brief review of the applicable principles of our search and seizure jurisprudence.

A.

[1] **[2]** **[3]** The Fourth Amendment to the United States Constitution and Article I, paragraph 7 of the New Jersey Constitution protect individuals' rights "to be secure in their persons, houses, papers, and effects" by requiring that search warrants be "supported by oath or affirmation" and describe with particularity the places subject to search and people or things subject to seizure. Searches executed pursuant to warrants compliant with those requirements are presumptively valid, State v. Jones, 179 N.J. 377, 388, 846 A.2d 569 (2004), and reviewing courts "should pay substantial deference" to judicial findings of probable cause in search warrant applications, State v. Kasabucki, 52 N.J. 110, 117, 244 A.2d 101 (1968).

[4] **[5]** Furthermore, the State has broad authority to effectuate searches permitted by valid search warrants. Pursuant to that authority, the State may destroy property, United States v. Ramirez, 523 U.S. 65, 69-71, 118 S.Ct. 992, 140 L.Ed.2d 191 (1998), forcibly enter a residence, United States v. Banks, 540 U.S. 31, 33, 40, 124 S.Ct. 521, 157 L.Ed.2d 343 (2003), and employ flash-bang devices,

State v. Rockford, 213 N.J. 424, 431-32, 64 A.3d 514 (2013), all in the name of executing a warrant.

Andrews does not challenge the search warrants issued for his cellphones. He does not claim that the phones were unlawfully seized or that the search warrants authorizing the State to comb their contents were unsupported by probable cause. Neither does defendant challenge the particularity with which the search warrants describe the "things subject to seizure." Thus, the State is permitted to access the phones' contents, as limited by the trial ***465** court's order, in the same way that the State may survey a home, vehicle, or other place that is the subject of a search warrant.

[6] But a lawful seizure does not allow compelled disclosure of facts otherwise protected by the Fifth Amendment. In re Search of a Residence in Oakland, 354 F. Supp. 3d 1010, 1014 (N.D. Cal. 2019); Michael S. Pardo, Disentangling the Fourth Amendment and the Self-Incrimination Clause, 90 Iowa L. Rev. 1857, 1860 (2005).

Andrews objects here to the means by which the State seeks to effectuate the ****1265** searches authorized by the lawfully issued search warrants -- compelled disclosure of his cellphones' passcodes -- which Andrews claims violate federal and state protections against compelled self-incrimination. We therefore consider whether the Fifth Amendment protects Andrews from being compelled to disclose his passcodes.

B.

1.

[7] The Fifth Amendment to the United States Constitution provides that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. That right against self-incrimination "applies only when the accused is compelled to make a testimonial communication that is incriminating." Fisher v. United States, 425 U.S. 391, 408, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976).

[8] **[9]** Testimonial communications may take any form, Schmerber v. California, 384 U.S. 757, 763-64, 86 S.Ct. 1826, 16 L.Ed.2d 908 (1966), but must "imply assertions of fact" for the Fifth Amendment privilege against self-incrimination to attach, Doe v. United States (Doe II), 487 U.S. 201, 209, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988). Thus, actions that do not require an individual "to disclose any knowledge he might have" or "to speak his guilt" are nontestimonial and therefore not protected by the Fifth ***466** Amendment. Id. at 211, 108 S.Ct. 2341 (quoting United States v. Wade, 388 U.S. 218, 222-23, 87 S.Ct. 1926, 18 L.Ed.2d 1149 (1967)).

[10] **[11]** **[12]** Accordingly, criminal defendants may lawfully be compelled to display their physical characteristics and commit physical acts because the display of physical characteristics is not coterminous with communications that relay facts. United States v. Hubbell, 530 U.S. 27, 35, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000). Among those acts are creating handwriting samples, Gilbert v. California, 388 U.S. 263, 266, 87 S.Ct. 1951, 18 L.Ed.2d 1178 (1967), and voice samples, United States v. Dionisio, 410 U.S. 1, 7, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973); providing blood, hair, and saliva samples, State v. Burke, 172 N.J. Super. 555, 557, 412 A.2d 1324 (App. Div. 1980); standing in a lineup, Wade, 388 U.S. at 221, 87 S.Ct. 1926; and donning particular articles of clothing, Holt v. United States, 218 U.S. 245, 252-53, 31 S.Ct. 2, 54 L.Ed. 1021 (1910). Also, consistent with the Fifth Amendment, individuals may be compelled to execute an authorization directing a foreign bank to disclose account records "because neither the form, nor its execution, communicates any factual assertions, implicit or explicit, or conveys any information to the Government." Doe II, 487 U.S. at 215, 108 S.Ct. 2341.

A handful of courts have held that compelled State access to electronic devices through the use of biometric features does not violate the Fifth Amendment. In re Search Warrant Application for Cellular Tel. in U.S. v. Barrera, 415 F. Supp. 3d 832, 833 (N.D. Ill. 2019) ("[C]ompelling an individual to scan their biometrics, and in particular their fingerprints, to unlock a smartphone device neither violates the Fourth nor

Fifth Amendment."); State v. Diamond, 905 N.W.2d 870, 878 (Minn. 2018) ("[P]roviding a fingerprint to the police to unlock a cellphone was not a testimonial communication protected by the Fifth Amendment."). But see In re Search of a Residence in Oakland, 354 F. Supp. 3d at 1018 (denying a search warrant seeking use of biometrical features to unlock electronic devices).

**1266 *467 [13] [14] As those examples suggest, the Fifth Amendment is not an absolute bar to a defendant's forced assistance of the defendant's own criminal prosecution. Doe II, 487 U.S. at 213, 108 S.Ct. 2341. In contrast to physical communications, however, if an individual is compelled "to disclose the contents of his own mind," such disclosure implicates the Fifth Amendment privilege against self-incrimination. Id. at 211, 108 S.Ct. 2341 (quoting Curcio v. United States, 354 U.S. 118, 128, 77 S.Ct. 1145, 1 L.Ed.2d 1225 (1957)).

In a series of cases, the United States Supreme Court has considered when an act of production constitutes a protected testimonial communication rather than a non-testimonial and therefore unprotected communication. In advancing that distinction, the Court has also developed an exception to the Fifth Amendment privilege against self-incrimination for acts of production that are testimonial in nature but of minimal testimonial value because the information they convey is a "foregone conclusion." We turn now to those developments.

2.

In Wilson v. United States, the Supreme Court upheld a contempt finding against a corporate officer who failed to comply with a grand jury subpoena compelling disclosure of potentially incriminating corporate records in his possession. 221 U.S. 361, 386, 31 S.Ct. 538, 55 L.Ed. 771 (1911). The Court explained that "the physical custody of incriminating documents does not of itself protect the custodian against their compulsory production." Id. at 380, 31 S.Ct. 538. Therefore "the fact of actual possession or of lawful custody would not justify the officer in resisting inspecting, even though the record was made by himself and would supply the evidence of his criminal dereliction." Ibid.

Sixty-five years later, the Fisher Court drew a distinction between the act of producing documents and the documents themselves in the context of subpoenaed tax records, finding that, even though the documents were not privileged,

> *468 [t]he act of producing evidence in response to a subpoena nevertheless has communicative aspects of its own, wholly aside from the contents of the papers produced. Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena.
>
> [425 U.S. at 409-10, 96 S.Ct. 1569.]

After those observations, the Court found that "the elements of compulsion are clearly present" in the production, "but the more difficult issues are whether the tacit averments of the taxpayer are both 'testimonial' and 'incriminating' for purposes of applying the Fifth Amendment." Ibid. Ultimately, the Court declared itself "confident that however incriminating the contents of the accountant's workpapers might be, the act of producing them -- the only thing which the taxpayer is compelled to do -- would not itself involve testimonial self-incrimination." Id. at 410-11, 96 S.Ct. 1569.

The reasoning with which the Court explained that conclusion ultimately gave rise to the foregone conclusion exception:

> It is doubtful that implicitly admitting the existence and possession of the papers rises to the level of testimony within the protection of the Fifth Amendment. ... The existence and location of **1267 the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers. Under these circumstances by enforcement of the summons "no constitutional rights are touched. The question is not of testimony but of surrender." In re Harris, 221 U.S. 274, 279, 31 S.Ct. 557, 55 L.Ed. 732 (1911).

....

Moreover, assuming that these aspects of producing the accountant's papers have some minimal testimonial significance, surely it is not illegal to seek accounting help in connection with one's tax returns or for the accountant to prepare workpapers and deliver them to the taxpayer. At this juncture, we are quite unprepared to hold that either the fact of existence of the papers or of their possession by the taxpayer poses any realistic threat of incrimination to the taxpayer.

As for the possibility that responding to the subpoena would authenticate the workpapers, production would express nothing more than the taxpayer's belief that the papers are those described in the subpoena. ... The documents would not be admissible in evidence against the taxpayer without authenticating testimony. Without more, responding to the subpoena in the circumstances before us would not appear to represent a substantial threat of self-incrimination.

[Id. at 411-13, 96 S.Ct. 1569 (emphases added; footnotes and citations omitted).]

***469** In United States v. Doe (Doe I), the Court applied the logic from Fisher in considering "whether, and to what extent, the Fifth Amendment privilege against compelled self-incrimination applies to the business records of a sole proprietorship," 465 U.S. 605, 606, 104 S.Ct. 1237, 79 L.Ed.2d 552 (1984), particularly where the district court indicated that "the Government had conceded that the materials sought in the subpoena were or might be incriminating," id. at 608, 104 S.Ct. 1237.

After "hold[ing] that the contents of those records are not privileged," the Court stressed, as did the Fisher Court, that even where "the contents of a document may not be privileged, the act of producing the document may be" because "[a] government subpoena compels the holder of the document to perform an act that may have testimonial aspects and an incriminating effect." Id. at 612, 104 S.Ct. 1237. Stressing the district court's factfinding that the subject documents did contain incriminating information, the Doe I Court distinguished Fisher. Id. at 613-14, 104 S.Ct. 1237.

The Doe I Court rejected the Government's argument "that any incrimination [flowing from the compelled production in that case] would be so trivial that the Fifth Amendment is not implicated," relying instead on "the findings made" by the trial court in holding that "the risk of incrimination was 'substantial and real' and not 'trifling or imaginary.' " Id. at 614 n.13, 104 S.Ct. 1237 (quoting Marchetti v. United States, 390 U.S. 39, 53, 88 S.Ct. 697, 19 L.Ed.2d 889 (1968)). The Court explained, "Respondent did not concede in the District Court that the records listed in the subpoena actually existed or were in his possession. Respondent argued that by producing the records, he would tacitly admit their existence and his possession." Ibid.

Although the Court reached its holding on that basis, it also noted the respondent's argument "that if the Government ****1268** obtained the documents from another source, it would have to authenticate them before they would be admissible at trial. By producing the documents, respondent would relieve the Government of the need for authentication." Ibid. (citation omitted).

***470** The Court stressed that a "valid claim of the privilege against self-incrimination" had been asserted, which the Government could then rebut "by producing evidence that possession, existence, and authentication were a 'foregone conclusion.' " Ibid. (emphasis added) (quoting Fisher, 425 U.S. at 411, 96 S.Ct. 1569). In Doe I, "however, the Government failed to make such a showing." Ibid.

In Hubbell, the Court reiterated, with respect to "13,120 pages of documents and records" produced in response to a grand jury subpoena, 530 U.S. at 31, 120 S.Ct. 2037, that "[t]he 'compelled testimony' that is relevant in this case is not to be found in the contents of the documents produced in response to the subpoena. It is, rather, the testimony inherent in the act of producing those documents," id. at 40, 120

S.Ct. 2037. Noting that the parties' dispute centered "on the significance of that testimonial aspect," the Court wrote, "The Government correctly emphasizes that the testimonial aspect of a response to a subpoena duces tecum does nothing more than establish the existence, authenticity, and custody of items that are produced." Id. at 40-41, 120 S.Ct. 2037.

But to convey that information, the Court stressed, "[i]t was unquestionably necessary for respondent to make extensive use of 'the contents of his own mind' in identifying the hundreds of documents responsive to the requests in the subpoena," such that "[t]he assembly of those documents was like telling an inquisitor the combination to a wall safe, not like being forced to surrender the key to a strongbox." Id. at 43, 120 S.Ct. 2037 (quoting Curcio, 354 U.S. at 128, 77 S.Ct. 1145). Indeed, the act of production at issue "was tantamount to answering a series of interrogatories asking a witness to disclose the existence and location of particular documents fitting certain broad descriptions." Id. at 41, 120 S.Ct. 2037.

In finding the act of producing the documents fell within the ambit of the Fifth Amendment's protection against self-incrimination, id. at 45, 120 S.Ct. 2037, the Court rejected the Government's argument that "the existence and possession of ... records [like those sought through the subpoena] by any businessman is a *471 'foregone conclusion' " as a misreading of Fisher and an end run around Doe I. Id. at 44, 120 S.Ct. 2037. The Court explained,

> Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it. While in Fisher the Government already knew that the documents were in the attorneys' possession and could independently confirm their existence and authenticity through the accountants who created them, here the Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.
>
> [Id. at 44-45, 120 S.Ct. 2037.]

[15] **[16]** From those cases, which all addressed the compelled production of documents, the following principles can be **1269 inferred: For purposes of the Fifth Amendment privilege against self-incrimination, the act of production must be considered in its own right, separate from the documents sought. And even production that is of a testimonial nature can be compelled if the Government can demonstrate it already knows the information that act will reveal -- if, in other words, the existence of the requested documents, their authenticity, and the defendant's possession of and control over them -- are a "foregone conclusion."

3.

Although the Supreme Court has considered the application of the foregone conclusion exception only in the context of document production, courts in other jurisdictions have grappled with the applicability of the exception beyond that context, and many have considered whether the exception applies to compelled decryption or to the compelled production of passcodes and passwords, reaching divergent results.

Among other causes for that divergence is a dispute over how to adapt the foregone conclusion analysis from the document-production context, which involves the act of producing the document and the contents of the document, to the context of passcode production, *472 which involves the act of producing the passcode that protects the contents of the electronic device.

Some courts to consider the issue have focused on the production of the passcode as a means to access the contents of the electronic device, treating the contents of the devices as the functional equivalent of the contents of documents at issue in the United States Supreme Court cases. Most recently, the Supreme Court of Indiana considered a woman's challenge to the order that she unlock her iPhone for law enforcement after she had been arrested for stalking. Seo v. State, 148 N.E.3d 952, 954 (2020).

After reviewing Fisher, Doe I, and Hubbell, id. at 957, the court in Seo "dr[ew] two analogies" in extending its observations on those cases "to the act of producing an unlocked smartphone": "First, entering the password to unlock the device is analogous to the physical act of handing over documents. And second, the files on the smartphone are analogous to the documents ultimately produced," id. at 957-58 (citing Laurent Sacharoff, What Am I Really Saying When I Open My Smartphone? A Response to Orin S. Kerr, 97 Tex. L. Rev. Online 63, 68 (2019)). "Thus," the court reasoned,

> a suspect surrendering an unlocked smartphone implicitly communicates, at a minimum, three things: (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possessed those files. And, unless the State can show it already knows this information, the communicative aspects of the production fall within the Fifth Amendment's protection.
>
> [Id. at 957-58 (footnote omitted).]

The court noted that "[t]he majority of courts to address the scope of testimony implicated when a suspect is compelled to produce an unlocked smartphone have reached a similar conclusion." Id. at 957-58 n.3 (collecting cases).

Applying that test, the court found in Seo the foregone conclusion exception inapplicable. Id. at 958. "Even if we assume the State has shown that Seo knows the password to her smartphone," the court wrote, "the State has failed to demonstrate **1270 that any particular files on the device exist or that she possessed those files." Id. at 958. Rather, if law enforcement were granted access *473 to the phone, they "would be fishing for 'incriminating evidence' from the device," such that "Seo's act of producing her unlocked smartphone would provide the State with information that it does not already know." Id. at 958.

After finding that the foregone conclusion exception did not apply, the Seo court also noted that "[t]his case highlights concerns with extending the limited foregone conclusion exception to the compelled production of an unlocked smartphone." Id. at 958-59; see also id. at 958-60 (explaining those concerns).

A four-Justice majority of the Supreme Court of Pennsylvania likewise focused on the files stored on a computer in considering whether production of the computer's password could be compelled. See Commonwealth v. Davis, —— Pa. ——, 220 A.3d 534, 537 (2019). The majority noted, "The Commonwealth is seeking the password, not as an end, but as a pathway to the files being withheld." Id. at 548. Reasoning that "the compelled production of the computer's password demands the recall of the contents of Appellant's mind, and the act of production carries with it the implied factual assertions that will be used to incriminate him," the court determined "that compelling Appellant to reveal a password to a computer is testimonial in nature" and thus protected by the Fifth Amendment. Id. at 548, 551.

The Davis majority took note of the foregone conclusion exception but stressed the limited context -- document production -- in which it has been applied by the United States Supreme Court, as well as the Supreme Court's sharp distinction between the physical and the mental. Id. at 548-51. The majority determined that, "until the United States Supreme Court holds otherwise, we construe the foregone conclusion rationale to be one of limited application and ... believe the exception to be inapplicable to compel the disclosure of a defendant's password to assist the Commonwealth in gaining access to a computer." Id. at 551.

In a footnote, the majority explained, "Even if we were to find that the foregone conclusion exception could apply to the compulsion to reveal a computer password, we nevertheless would conclude *474 that the Commonwealth has not satisfied the requirements of the exception in this matter." Id. at 551 n.9. Stressing that "[i]t is not merely access to the computer that the Commonwealth seeks to obtain through compelling Appellant to divulge his computer password, but all of the files on Appellant's computer," and that "[t]he password is merely a means to get to the computer's contents," the majority found that

> because the Commonwealth has failed to establish that its search is limited to the single previously identified file, and has not asserted that it is a foregone conclusion as to the existence of additional files that may be on the computer, which would be accessible to the Commonwealth upon Appellant's compelled disclosure of the password, ... the Commonwealth has not satisfied the foregone conclusion exception.

[Ibid.]

The three-Justice dissent in Davis took issue not only with the majority's determination that the foregone conclusion exception is inapplicable in the context of compelled password production, but also with its determination that the exception should **1271 not be applied in that case. Id. at 552-53 (Baer, J., dissenting).

In the dissent's view, "the compulsion of Appellant's password is an act of production, requiring him to produce a piece of evidence similar to the act of production requiring one to produce a business or financial document, as occurred in Fisher." Id. at 554. The dissent noted that "[a]n order compelling disclosure of the password ... has testimonial attributes, not in the characters themselves, but in the conveyance of information establishing that the password exists, that Appellant has possession and control of the password, and that the password is authentic, as it will decrypt the encrypted computer files." Id. at 555.

Stressing that "[t]he Commonwealth is not seeking the 64-character password as an investigative tool, as occurred in Hubbell," but rather "already possesses evidence of Appellant's guilt, which it set forth in an affidavit of probable cause to obtain a warrant to search Appellant's computer," the dissent viewed "the compulsion order as requiring the 'surrender' of Appellant's password to decrypt his computer files" -- an act to which "Fisher's *475 act-of-production test" and the foregone conclusion rationale would apply. Ibid.

The Davis dissent then explained why the foregone conclusion exception would apply in that case, contrary to the majority's analysis. Id. at 556-58. Notably, the dissent disagreed with the majority's focus on the files that would be made accessible if the password were revealed, reasoning instead

> that the foregone conclusion exception as applied to the facts presented relates not to the computer files, but to the password itself. Appellant's computer files were not the subject of the compulsion order, which instead involved only the password that would act to decrypt those files. This change of focus is subtle, but its effect is significant. While the government's knowledge of the specific files contained on Appellant's computer hard drive would be central to any claim asserted pursuant to the Fourth Amendment, the same is not dispositive of the instant claim based upon the Fifth Amendment right against self-incrimination, which focuses upon whether the evidence compelled, here, the password, requires the defendant to provide incriminating, testimonial evidence. ... This Court should not alleviate concerns over the potential overbreadth of a digital search in violation of Fourth Amendment privacy concerns by invoking the Fifth Amendment privilege against self-incrimination, which offers no privacy protection. ...
>
> Accordingly, I would align myself with those jurisdictions that examine the requisites of the foregone conclusion exception by focusing only on the compelled evidence itself, i.e., the computer password, and not the decrypted files that the password would ultimately reveal.
>
> [Id. at 557 (citations omitted) (collecting cases).]

The Florida District Courts of Appeals have similarly splintered when considering the focus of the foregone conclusion analysis and the scope of the exception. In State v. Stahl, the court opined that "[t]o know whether providing [a] passcode implies testimony that is a foregone conclusion, the relevant question is whether the State has established that it knows with reasonable particularity that the passcode exists, is within the accused's possession or control, and is authentic." 206 So. 3d 124, 136 (Fla. Dist. Ct. App. 2016).

**1272 The court held that the exception applied under the circumstances before it. Id. at 136-37. First, the court found that "the State established that the phone could not be searched without entry of a passcode" and that "[a] passcode therefore must exist," as well as that "the phone was [the defendant's] and therefore the *476 passcode would be in [the defendant's] possession." Id. at 136. And recognizing that, because "technology is self-authenticating [such that] no other means of authentication may exist," the court also found that "[i]f the phone or computer is accessible once the passcode or key has been entered, the passcode or key is authentic." Ibid.

In G.A.Q.L. v. State, another Florida District Court of Appeals viewed the issue differently. 257 So. 3d 1058, 1062-63 (Fla. Dist. Ct. App. 2018). There, the State sought to compel a minor charged with drunk driving "to provide the passcode for [her] iPhone and the password for an iTunes account associated with it." Id. at 1060. The court reasoned that "the 'evidence sought' in a password production case such as this is not the password itself; rather it is the actual files or evidence on the locked phone." Id. at 1064. In declining to apply the foregone conclusion exception, the court held that the State "must identify what evidence lies beyond the passcode wall with reasonable particularity" but "fail[ed] to identify any specific file locations or even name particular files that it [sought] from the encrypted, passcode-protected phone." Id. at 1064-65; see also Pollard v. State, 287 So. 3d 649, 651 (Fla. Dist. Ct. App. 2019) (holding that the "proper legal inquiry ... is whether the state is seeking to compel a suspect to provide a password that would allow access to information the state knows is on the suspect's cellphone and has described with reasonable particularity").

In Commonwealth v. Gelfgatt, the Supreme Judicial Court of Massachusetts took a slightly different view of the authentication element of the foregone conclusion test: "Here, the defendant's decryption of his computers does not present an authentication issue analogous to that arising from a subpoena for specific documents because he is not selecting documents and producing them, but merely entering a password into encryption software." 468 Mass. 512, 11 N.E.3d 605, 615 n.14 (2014).

The Gelfgatt court thus found authentication immaterial and applied the exception in the context of the issue before it: the ***477** prosecution's motion to compel a defendant charged with forgery and theft to enter an encryption key [4] in computers lawfully seized by law enforcement. Id. at 608, 614. The Supreme Judicial Court held that even though entering an encryption key would be a testimonial communication, "[t]he facts that would be conveyed by the defendant through his act of decryption -- his ownership and control of the computers and their contents, knowledge of the fact of encryption, and knowledge of the encryption key -- already are known to the government and, thus, are a 'foregone conclusion.' " Id. at 615.

Likewise, in United States v. Apple MacPro Computer, the United States Court of Appeals for the Third Circuit relied on the district court's fact findings, and affirmed its determination that the ****1273** compelled decryption of the defendant's devices was not testimonial within the meaning of the Fifth Amendment in light of what the police already knew would be found on those devices. 851 F.3d 238, 248 (3d Cir. 2017).

The Third Circuit pointedly added, however, that it was "not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the 'foregone conclusion' inquiry in the context of a compelled decryption order." Id. at 248 n.7. "Instead," the court noted, "a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production." Ibid. And the court explained that, "[i]n this case, the fact known to the government that is implicit in the act of providing the password for the devices is 'I, John Doe, know the password for these devices.' " Ibid.

Those cases from jurisdictions that have considered the viability of the foregone conclusion exception in the context of compelled ***478** decryption or passcode disclosure provide helpful guidance as we consider the issue before us, a matter of first impression for this Court.

C.

1.

Considering the foregoing in light of the facts of this case, we note first that the State correctly asserts that the lawfully issued search warrants -- the sufficiency of which Andrews does not challenge -- give it the right to the cellphones' purportedly incriminating contents as specified in the trial court's order. And neither those contents -- which are voluntary, not compelled, communications, see

Oregon v. Elstad, 470 U.S. 298, 306-07, 105 S.Ct. 1285, 84 L.Ed.2d 222 (1985) -- nor the phones themselves -- which are physical objects, not testimonial communications, see Pennsylvania v. Muniz, 496 U.S. 582, 589, 110 S.Ct. 2638, 110 L.Ed.2d 528 (1990) -- are protected by the Fifth Amendment privilege against self-incrimination. Therefore, production of Andrews's cellphones and their contents is not barred; indeed, had the State succeeded in its efforts to access the phones, this case would not be before us.

[17] But access to the cellphones' contents depends here upon entry of their passcodes. A cellphone's passcode is analogous to the combination to a safe, not a key. Communicating or entering a passcode requires facts contained within the holder's mind -- the numbers, letters, or symbols composing the passcode. It is a testimonial act of production.

2.

[18] The inquiry does not end there, however, because, if the foregone conclusion exception applies, production of the passcodes may still be compelled. To determine the exception's applicability, we must first determine to what it might apply -- the act of producing the passcodes, or the act of producing the cellphones' contents through the passcodes. To be consistent with the Supreme ***479** Court case law that gave rise to the exception, we find that the foregone conclusion test applies to the production of the passcodes themselves, rather than to the phones' contents.

The relevant Supreme Court cases explicitly predicate the applicability of the foregone conclusion doctrine on the fundamental distinction between the act of production ****1274** and the documents to be produced. The documents may be entitled to no Fifth Amendment protection at all -- and, indeed, they were not so entitled in Fisher -- but the act of producing them may nevertheless be protected.

In light of the stark distinction the Court has drawn between the evidentiary object and its production -- a division reinforced even in those cases where the foregone conclusion exception was held not to apply -- it is problematic to meld the production of passcodes with the act of producing the contents of the phones. As the Davis dissent observed, that approach imports Fourth Amendment privacy principles into a Fifth Amendment inquiry.

In Fisher, the Supreme Court rejected such importation when it rejected "the rule against compelling production of private papers" set forth in Boyd v. United States, 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746 (1886), to the extent the Boyd rule "rested on the proposition that seizures of or subpoenas for 'mere evidence,' including documents, violated the Fourth Amendment and therefore also transgressed the Fifth." 425 U.S. at 409, 96 S.Ct. 1569. The Fisher Court noted that "the foundations for the [Boyd] rule have been washed away" and that "the prohibition against forcing the production of private papers has long been a rule searching for a rationale consistent with the proscriptions of the Fifth Amendment against compelling a person to give 'testimony' that incriminates him." Ibid. (emphasis added); see also Pardo, 90 Iowa L. Rev. at 1882 ("Of the two Amendments, the Fifth Amendment plays the major role in subpoena doctrine. This is due, in part, to the absence of a significant role for the Fourth Amendment."). We agree with the Davis dissent that the proper focus here is on the Fifth Amendment and that the Fourth Amendment's privacy ***480** protections should not factor into analysis of the Fifth Amendment's applicability.

We also share the concerns voiced by other courts that holding passcodes exempt from production whereas biometric device locks may be subject to compulsion creates inconsistent approaches based on form rather than substance. The distinction becomes even more problematic when considering that, at least in some cases, a biometric device lock can be established only after a passcode is created, calling into question the testimonial/non-testimonial distinction in this context. See Kristen M. Jacobsen, Note, Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and its Chilling Effect on Law Enforcement, 85 Geo. Wash. L. Rev. 566, 582 (2017).

[19] In sum, we view the compelled act of production in this case to be that of producing the passcodes. Although that act of production is testimonial, we note that passcodes are a series of characters without independent evidentiary

significance and are therefore of "minimal testimonial value" -- their value is limited to communicating the knowledge of the passcodes. See Apple MacPro, 851 F.3d at 248 n.7. Thus, although the act of producing the passcodes is presumptively protected by the Fifth Amendment, its testimonial value and constitutional protection may be overcome if the passcodes' existence, possession, and authentication are foregone conclusions.

3.

[20] **[21]** Based on the record before us, we have little difficulty concluding that compelled production of the passcodes falls within the foregone conclusion exception. ****1275** The State established that the passcodes exist -- they determined the cellphones' contents are passcode-protected. Also, the trial court record reveals that the cellphones were in Andrews's possession when seized and that he owned and operated the cellphones, establishing his knowledge of the passcodes and that the passcodes enable access to the cellphones' ***481** contents.[5] See Gelfgatt, 11 N.E.3d at 615. Finally, to the extent that authentication is an issue in this context, the passcodes self-authenticate by providing access to the cellphones' contents. See Stahl, 206 So. 3d at 136; Gelfgatt, 11 N.E.3d at 615 n.14.

The State's demonstration of the passcodes' existence, Andrews's previous possession and operation of the cellphones, and the passcodes' self-authenticating nature render the issue here one of surrender, not testimony, and the foregone conclusion exception to the Fifth Amendment privilege against self-incrimination thus applies. Therefore, the Fifth Amendment does not protect Andrews from compelled disclosure of the passcodes to his cellphones.

Although we reach that decision by focusing on the passcodes, we note that, in this case, we would reach the same conclusion if we viewed the analysis to encompass the phones' contents. Cf. Apple MacPro, 851 F.3d at 248 & n.7. The search warrants and record evidence of the particular content that the State knew the phones contained provide ample support for that determination. In short, this was no "fishing expedition." Cf. Hubbell, 530 U.S. at 42, 120 S.Ct. 2037; Seo, 148 N.E.3d at 958.

Having concluded that the Fifth Amendment's Self-Incrimination Clause does not protect Andrews from government compelled disclosure of the cellphones' passcodes, we turn to state law.

IV.

[22] New Jersey's privilege against compelled self-incrimination is not expressed in its constitution, but the privilege "is deeply rooted in this State's common law and codified in both statute and an evidence rule." State v. Muhammad, 182 N.J. 551, 567, 868 A.2d 302 (2005).

***482** We begin with the relevant statutes and rules of evidence.

1.

[23] **[24]** In 1960, the Legislature codified the protection against compelled self-incrimination. See L. 1960, c. 152, §§ 18-19. "N.J.S.A. 2A:84A-18 and -19 define[ ] the right against self-incrimination," but also "set[ ] forth specific limitations on that right." In re Grand Jury Proceedings of Guarino, 104 N.J. 218, 229 n.6, 516 A.2d 1063 (1986). The statute and corresponding rule of evidence explicitly afford a suspect the "right to refuse to disclose ... any matter that will incriminate him or expose him to a penalty or a forfeiture of his estate." N.J.S.A. 2A:84A-19; N.J.R.E. 503 (emphasis added).[6] For the right of refusal to apply, therefore, a matter must first be found to be incriminating.

****1276** N.J.S.A. 2A:84A-18 and N.J.R.E. 502, in turn, define the circumstances under which a matter will be deemed incriminating:

> [A] matter will incriminate (a) if it constitutes an element of a crime against this State, or another State or the United States, or (b) is

> a circumstance which with other circumstances would be a basis for a reasonable inference of the commission of such a crime, or (c) is a clue to the discovery of a matter which is within clauses (a) or (b) above ....

[25] Applying that definition, we note first that the passcodes are obviously not an element of any crime charged against Andrews. They are only a method of production of or access to the contents of his cellphones. Although disclosure of a passcode is evidence of ownership and control of a cellphone and its contents, the State has already established both of those facts here. The passcodes then, as amalgamations of characters with minimal evidentiary significance,[7] do not themselves support an inference that a crime has been committed, nor do they constitute "clues."

***483** **[26]** Said another way, where ownership and control of an electronic device is not in dispute, its passcode is generally not substantive information, is not a clue to an element of or the commission of a crime, and does not reveal an inference that a crime has been committed. Cf. State v. Fisher, 395 N.J. Super. 533, 547-48, 929 A.2d 1130 (App. Div. 2007) ("The disclosure of one's name and address does not entail a substantial risk of self-incrimination. 'It identifies but does not by itself implicate anyone in criminal conduct.' " (emphasis added) (quoting California v. Byers, 402 U.S. 424, 434, 91 S.Ct. 1535, 29 L.Ed.2d 9 (1971))).

We turn, therefore, to New Jersey common law.

2.

[27] New Jersey's common law privilege against self-incrimination "generally parallels federal constitutional doctrine," State v. Chew, 150 N.J. 30, 59, 695 A.2d 1301 (1997), but also "offers broader protection than its federal counterpart under the Fifth Amendment," Muhammad, 182 N.J. at 568, 868 A.2d 302; accord Guarino, 104 N.J. at 229, 516 A.2d 1063. Our privilege derives from the notion of personal privacy established by the United States Supreme Court in Boyd. Guarino, 104 N.J. at 230, 516 A.2d 1063.

In Boyd, decided in 1886, the Court considered whether the production of private papers could be compelled and determined that "a compulsory production of the private books and papers of the owner of goods sought to be forfeited in such a suit is" not only "compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution," but also "is the equivalent of a search and seizure -- and an unreasonable search and seizure -- within the meaning of the Fourth Amendment." 116 U.S. at 634-35, 6 S.Ct. 524.

***484** As noted above, the Fisher Court overturned that rule in the context of federal constitutional analysis. See 425 U.S. at 407, 96 S.Ct. 1569 (explaining that "[s]everal of Boyd's express or implicit declarations **1277** have not stood the test of time" and listing examples, including private documents); see also Doe I, 465 U.S. at 618, 104 S.Ct. 1237 (O'Connor, J., concurring) ("[T]he Fifth Amendment provides absolutely no protection for the contents of private papers of any kind. The notion that the Fifth Amendment protects the privacy of papers originated in [Boyd], but our decision in [Fisher] sounded the death knell for Boyd."); Pardo, 90 Iowa L. Rev. at 1858 ("Subsequent doctrinal developments have torpedoed Boyd's view of the overlap [between the Fourth and Fifth Amendments] as the Court has systematically rejected and cabined Boyd's holding.").

In Guarino, this Court considered as a matter of first impression whether Fisher's overthrow of Boyd's private-papers rule would affect New Jersey law. 104 N.J. at 231, 516 A.2d 1063. The Guarino Court "affirm[ed] our belief in the Boyd doctrine and [held] that the New Jersey common law privilege against self-incrimination protects the individual's right 'to a private enclave where he may lead a private life.' " Ibid. (quoting Murphy v. Waterfront Comm'n, 378 U.S. 52, 55, 84 S.Ct. 1594, 12 L.Ed.2d 678 (1964)). Thus, despite the shift at the federal level, our common law privilege continues

to consider whether evidence requested is of an inherently private nature.

[28] The Guarino Court articulated the relevant test as follows:

> To determine whether the evidence sought by the government lies within that sphere of personal privacy a court must look to the "nature of the evidence." Couch v. United States, 409 U.S. 322, 350, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973) (Marshall, J., dissenting). In the case of documents, therefore, a court must look to their contents, not to the testimonial compulsion involved in the act of producing them, as the Supreme Court has done in Fisher and Doe. Neither Fisher nor Doe recognize the fundamental privacy principles underlying the New Jersey common-law privilege against self-incrimination. Thus, in defining the scope of our common-law privilege, we decline to follow the Court's rationale for its Doe decision.
>
> [Id. at 231-32, 516 A.2d 1063.]

***485** In other words, in contrast to federal law which distinguishes between Fourth and Fifth Amendment inquiries, New Jersey's common law views the privilege against self-incrimination as incorporating privacy considerations.

[29] Noting as much gives us our answer here. The constitutional privacy considerations, see U.S. Const. amend. IV; N.J. Const. art. I, ¶ 7, that would apply to those portions of the cellphones' contents of which disclosure has been ordered have already been considered and overcome through the unchallenged search warrants granted in this case. As we noted in the federal context, whether the inquiry is limited here to the passcodes or extended to the phones' contents, the result is the same.

We thus agree with the Appellate Division that New Jersey's common law and statutory protections against compelled self-incrimination do not apply here.

V.

For the reasons set forth above, neither federal nor state protections against compelled disclosure shield Andrews's passcodes. We therefore affirm the Order of the Appellate Division compelling Andrews's ****1278** disclosure of the passcodes to his cellphones seized consistent with the trial court's order of production, and remand to the trial court for further proceedings.

JUSTICE LaVECCHIA, dissenting.

In a world where the right to privacy is constantly shrinking, the Constitution provides shelter to our innermost thoughts -- the contents of our minds -- from the prying eyes of the government. The right of individuals to be free from the forced disclosure of the contents of their minds to assist law enforcement in a criminal investigation, until now, has been an inviolate principle of our law, protected by the Fifth Amendment and our state common law. No United States Supreme Court case presently requires otherwise. No case from this Court has held otherwise. That protection deserves utmost respect and should not be lessened to authorize ***486** courts to compel a defendant to reveal the passcode to a smartphone so law enforcement can access its secured contents.

We are at a crossroads in our law. Will we allow law enforcement -- and our courts as their collaborators -- to compel a defendant to disgorge undisclosed private thoughts -- presumably memorized numbers or letters -- so that the government can obtain access to encrypted smartphones? In my view, compelling the disclosure of a person's mental thoughts is anathema to fundamental principles under our Constitution and state common law.

The Court's outcome deviates from steadfast past principles protective of a defendant's personal autonomy in the face of governmental compulsion in a criminal matter. Those same principles should apply even in the face of the latest challenge presented by new technology. Respectfully, I dissent from the course the Court now takes.

I.

The facts that set up the pivotal legal question in this matter are these. Defendant Robert Andrews, a former

law enforcement officer in the Essex County Sheriff's Department, was suspected of helping a drug dealer named Quincy Lowery in Lowery's criminal scheme. Lowery knew Andrews through their joint interest in a motorcycle club. Lowery made the accusations that led to Andrews's investigation when Lowery began cooperating with police to gain benefit after being charged as part of a larger narcotics investigation.

The State obtained Lowery's phone by consent. According to Lowery, although some messages were deleted, his phone showed telephone calls and messages between him and Andrews. In the course of its investigation, the State seized two phones from Andrews and obtained a warrant to search them after Andrews refused to consent to a search. One phone was listed as Andrews's personal cell phone and registered to his home address. The other phone was subscribed to by Kay Transportation, LLC, a business ***487** with which Andrews presumably was associated, although its address is not listed as Andrews's home. Both phones were on him when seized.

Although the scope of the warrant to search the two phones contains no substantive limit on its face, its scope was later narrowed to permit a search of the phone icon and the message icon. There was no restriction to control with whom a conversation took place or the time periods within which a message or phone call took ****1279** place. The two aforementioned limitations were imposed by the court during proceedings on the State's motion to compel discovery of the passcodes to the phones. [1] According to the State, it could not then, or even by the time of argument before our Court, access the phones' contents, nor could Apple, the manufacturer of these iPhones, or the Federal Bureau of Investigation. The State also represents that no service company has been able to help it gain access.

Andrews resisted the State's motion, claiming a violation of the Fifth Amendment, as well as New Jersey common law and law governing privilege, to wit: N.J.S.A. 2A:84A-19 and Evidence Rules 501 and 503. Also, according to Andrews, the State waited two years to seek the passcodes; the State does not know what phone the sought-after information is on or where it is located; nor does it know with any particularity what information on the phones will provide evidence of criminality.

The motion court granted the motion to compel, and, on interlocutory review, the Appellate Division affirmed.

We are reviewing the Appellate Division's judgment, at which the court arrived by concluding that the forced disclosure of the passcode is a testimonial act for purposes of a Fifth Amendment analysis, but applying an exception (identified as "foregone conclusion") to avoid finding a constitutional violation. The Appellate ***488** Division also rejected all state law arguments that Andrews advanced.

This Court's majority opinion conveys the essence of the motion court and Appellate Division rulings, so, to avoid repetition, I turn directly to why I believe it to be error to sustain the compelled disclosure of presumably memorized passcodes to these smartphones under the Fifth Amendment or state law.

II.

A.

The Fifth Amendment of the United States Constitution provides that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." U.S. Const. amend. V. The privilege extends beyond compelled incriminatory testimony given in court to include other forced testimony that "would furnish a link in the chain of evidence needed to prosecute the claimant." United States v. Hubbell, 530 U.S. 27, 38, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) (quoting Hoffman v. United States, 341 U.S. 479, 486, 71 S.Ct. 814, 95 L.Ed. 1118 (1951)). In the Court's seminal decision of Boyd v. United States, it was recognized that "a compulsory production of the private books and papers of [an individual] is compelling him to be a witness against himself, within the meaning of the Fifth Amendment to the Constitution." 116 U.S. 616, 634-35, 6 S.Ct. 524, 29 L.Ed. 746 (1886).

Boyd was rooted in a privacy rationale that prevents "the invasion of [one's] indefeasible right of personal security, personal liberty and private property." Id. at 630, 6 S.Ct.

524. Its privacy principle was maintained for decades and reinforced in Couch v. United States. See 409 U.S. 322, 327, 93 S.Ct. 611, 34 L.Ed.2d 548 (1973) (explaining that the Fifth Amendment "respects a private inner sanctum of individual feeling and thought" -- an inner sanctum that **1280 necessarily includes an individual's papers and effects to the extent that the privilege bars their compulsory production *489 and authentication -- and "proscribes state intrusion to extract self-condemnation").

The precept that one's inner thoughts cannot be compelled to be disclosed because they are protected by the Fifth Amendment privilege against self-incrimination is still an accepted United States Supreme Court principle. The Supreme Court's continuous assertion of that principle about compelled production of information stored in the mind, even as recently as in its 2000 majority opinion in Hubbell, 530 U.S. at 43, 120 S.Ct. 2037, provides the polestar in this matter. Although that polestar has apparently been not as bright for some courts when addressing law enforcement efforts to force an individual to reveal passcodes for encrypted devices like the smartphones here, creating a divide in the jurisprudence in the federal and state courts, I see no basis to depart from that core Fifth Amendment principle.

The divide is rooted in applications of the altered analysis developed by the Supreme Court during the 1970s and 1980s, concerning the production of physical documents, leading to, among other things, a one-time application of an "exception" called "foregone conclusion." Although that exception has not been applied again by the Supreme Court, the aforementioned jurisprudential split exists because some courts have expansively, and in various ways, applied that concept to excuse alleged violations of the privilege against self-incrimination in applications of forced disclosure of mentally cached passcodes to bypass security for new technology. But, for me, there is no real difference between forcing one to divulge the mentally stored combination of a safe -- the very example that the Supreme Court has used, more than once, as a step too far in ordering a defendant to assist in his or her own prosecution -- and forcing one to divulge the passcode to a smartphone.

A recitation of that relevant Supreme Court precedent follows.

B.

It is well established that to fall within the self-incrimination privilege, an individual must show that the evidence is compelled, *490 testimonial, and self-incriminating. Hubbell, 530 U.S. at 34-35, 120 S.Ct. 2037. An order to compel a defendant to produce documents implicates the Fifth Amendment and, originally, the Supreme Court interpreted the Fifth Amendment as protecting all private papers. Boyd, 116 U.S. at 630-32, 6 S.Ct. 524. That was altered in Fisher v. United States, 425 U.S. 391, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976).

With its decision in Fisher, the Court shifted from a blanket protection for private papers to a new paradigm for evaluating a self-incrimination claim involving the production of existing documents -- documents which, because they already existed, were not themselves testimonial. Id. at 409-10, 96 S.Ct. 1569. The analysis thus turned from the content of the document to an examination of the act of production of documents, hence becoming known as the act of production doctrine. The Court's Fisher decision held that the act of producing documents in response to a government subpoena could be testimonial if the act of production used the contents of the mind and revealed, either explicitly or implicitly, the existence, possession and control, or authenticity of the physical documents. Id. at 410-13, 96 S.Ct. 1569. Thus, the facts in Fisher require attention.

**1281 Fisher involved consolidated cases in which the defendants, in each, were involved in an IRS investigation into possible civil or criminal federal tax liability. Id. at 393-94, 96 S.Ct. 1569. The taxpayers retrieved documents from their accountants related to the accountants' preparation of their tax returns, which the taxpayers then shared with their lawyers. Id. at 394, 96 S.Ct. 1569. When the lawyers were served with summonses from the IRS directing them to produce the accounting documents in question, they declined. Id. at 394-95, 96 S.Ct. 1569. After differing results in the circuit courts, the Supreme Court granted certiorari.

Focusing on the act of " 'physical or moral compulsion' exerted on the person asserting the privilege," the Court did not find the necessary personal compulsion and declined to extend Fifth Amendment protection to the compelled production of the documents. ***491** Id. at 397, 96 S.Ct. 1569 (quoting Perlman v. United States, 247 U.S. 7, 15, 38 S.Ct. 417, 62 L.Ed. 950 (1918); other citations omitted). The Court observed that the documents could be obtained without action from the accused, adding that the subpoena to the taxpayers' lawyer had no authority to compel the taxpayer to provide incriminating information against himself. Id. at 398, 96 S.Ct. 1569 ("It is extortion of information from the accused himself that offends our sense of justice." (quoting Couch, 409 U.S. at 328, 93 S.Ct. 611)). The documents in question were not prepared by the taxpayers, did not contain testimonial declarations by the taxpayers, and were prepared in an entirely voluntary manner. Id. at 409, 96 S.Ct. 1569. Because production of the documents would not "compel the taxpayer to restate, repeat, or affirm" the contents of those documents, the Court determined that compulsion to produce them was not testimonial. Ibid.

Importantly, the Court acknowledged that whether the Fifth Amendment lends its protection to the documents in question could not be answered without considering whether responding to a subpoena is itself communicative. Id. at 410, 96 S.Ct. 1569. "Compliance with the subpoena tacitly concedes the existence of the papers demanded and their possession or control by the taxpayer. It also would indicate the taxpayer's belief that the papers are those described in the subpoena." Ibid. However, that was not found to exist on the facts presented, as the subpoena was served on the lawyer. Id. at 410-11, 96 S.Ct. 1569.

The Court's new framework and its application in Fisher led the Court to establish the foregone conclusion doctrine. That doctrine was described as providing that if the government can demonstrate that the existence, possession or control, and authenticity of the identified documents or materials it seeks are a foregone conclusion, then the act of production itself "adds little or nothing to the sum total of the Government's information" because the government is not relying on the veracity of the statement implicit in the act of production to prove the existence, possession or control, or authenticity of the documents. Ibid. Ultimately, the ***492** Court stated, "[t]he question is not of testimony but surrender." Id. at 411, 96 S.Ct. 1569 (quoting In re Harris, 221 U.S. 274, 279, 31 S.Ct. 557, 55 L.Ed. 732 (1911)).

The Court expanded on the notion that the response to a subpoena itself could be incriminating in United States v. Doe (Doe I), 465 U.S. 605, 104 S.Ct. 1237, 79 L.Ed.2d 552 (1984). There the Court had to determine whether bank statements, phone records, and other business records of a sole proprietor of a business could be compelled for production. ****1282** Id. at 606-07, 104 S.Ct. 1237. Doe was the owner of several sole proprietorships. Id. at 606, 104 S.Ct. 1237. During the course of investigating "corruption in the awarding of county and municipal contracts," a grand jury issued subpoenas attempting to compel Doe to provide telephone, business, and bank records pertaining to his companies. Id. at 606-07, 104 S.Ct. 1237. Doe filed a motion in the District Court of New Jersey requesting that the subpoenas be quashed, and the court granted the motion, stating that "the relevant inquiry is ... whether the act of producing the documents has communicative aspects which warrant Fifth Amendment protection." Id. at 607-08, 104 S.Ct. 1237 (quoting In re Grand Jury Empanelled March 19, 1980, 541 F. Supp. 1, 3 (D.N.J. 1981)). The United States Court of Appeals for the Third Circuit affirmed. Id. at 608, 104 S.Ct. 1237.

The Supreme Court held that such production is protected by the Fifth Amendment because the government was not certain the defendant actually possessed and/or controlled those documents. The Court again noted that "[a]lthough the contents of a document may not be privileged, the act of producing the document may be." Id. at 612, 104 S.Ct. 1237. Producing documents would indicate that the defendant possesses them, controls them, and believes them to be the documents requested. Id. at 613 & n.11, 104 S.Ct. 1237. Relying on the Third Circuit's assessment that there was "nothing in the record that would indicate that the United States knows, as a certainty, that each of the myriad

documents demanded by the five subpoenas in fact is in the [defendant's] possession ***493** or subject to his control," id. at 613 n.12, 104 S.Ct. 1237 (quoting In re Grand Jury Empanelled March 19, 1980, 680 F.2d 327, 335 (3d Cir. 1982)), the Court upheld the determination that the act of producing the documents was testimonial, id. at 614, 104 S.Ct. 1237. As the Court emphasized, "the Government, unable to prove that the subpoenaed documents exist -- or that [Doe] even is somehow connected to the business entities under investigation -- is attempting to compensate for its lack of knowledge by requiring [Doe] to become, in effect, the primary informant against himself." Id. at 613 n.12, 104 S.Ct. 1237 (quoting In re Grand Jury Empanelled March 19, 1980, 680 F.2d at 335). Ultimately, the Court held that although the contents of the underlying documents were not privileged, the State could not compel defendant to provide them because "[t]he act of producing the documents at issue in this case is privileged and cannot be compelled without a statutory grant of use immunity pursuant to 18 U.S.C. §§ 6002 and 6003." Id. at 617, 104 S.Ct. 1237.

Completing the trilogy of cases in this vein, four years later, the Court issued a decision in the case known colloquially as Doe II. Doe v. United States, 487 U.S. 201, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988). There, the Court answered the question of "whether a court order compelling a target of a grand jury investigation to authorize foreign banks to disclose records of his accounts, without identifying those documents or acknowledging their existence, violates the target's Fifth Amendment privilege against self-incrimination." Id. at 202, 108 S.Ct. 2341. Doe was the target of a federal grand jury investigation into suspected "fraudulent manipulation of oil cargoes and receipt of unreported income." Ibid. The grand jury issued a subpoena and Doe was directed to produce records of transactions at three specific banks in Bermuda and the Cayman Islands. Ibid. Doe produced some records, but when asked about whether there were other records ****1283** and where they might be, he invoked his Fifth Amendment privilege against self-incrimination. Id. at 202-03, 108 S.Ct. 2341. When Doe invoked his Fifth Amendment rights, the United States branches of the foreign banks were also served with subpoenas attempting to compel ***494** them to produce the responsive documents. Id. at 203, 108 S.Ct. 2341. Because the banks were subject to their governments' privacy and secrecy laws and refused to comply with the subpoena, the government attempted to compel Doe to sign twelve forms that would permit release by the banks of any records relating to twelve foreign accounts the Government "knew or suspected" Doe controlled. Ibid.

The Supreme Court upheld the subpoena's enforcement, refining the issue to be whether compelling Doe to sign the form was a "testimonial communication." Id. at 207, 108 S.Ct. 2341. The Court's analysis emphasized that "[i]t is consistent with the history of and the policies underlying the Self-Incrimination Clause to hold that the privilege may be asserted only to resist compelled explicit or implicit disclosures of incriminating information." Id. at 212, 108 S.Ct. 2341.

Scrutinizing the form the defendant was forced to sign, the Court noted that it was "carefully drafted not to make reference to a specific account," and did "not acknowledge that an account in a foreign financial institution is in existence or that it is controlled by petitioner," "indicate whether documents or any other information relating to petitioner are present at the foreign bank, assuming that such an account does exist," or "even identify the relevant bank." Id. at 215, 108 S.Ct. 2341. The Court concluded that the act of signing the form was not testimonial. Ibid. The Court was untroubled by Doe being compelled to sign the form because "[b]y signing the form, Doe makes no statement, explicit or implicit, regarding the existence of a foreign bank account or his control over any such account." Id. at 215-16, 108 S.Ct. 2341. The Court concluded that the form did not direct the government to evidence; rather, it simply provided access to evidence if the government could independently find it. Id. at 215, 108 S.Ct. 2341.

In Doe II, there is passing reference to the foregone conclusion doctrine, but it is not used in the Court's analysis. Ibid. Indeed, it has never again been used by the Supreme Court, and was even questioned in a later case, as well as in separate opinions, making ***495** Doe II the end point of

Supreme Court cases leaving the door open to the use -- let alone expansion -- of that doctrine. See Hubbell, 530 U.S. at 44, 49-50, 120 S.Ct. 2037; see also Seo v. State, 148 N.E.3d 952, 956 (Ind. 2020) (similarly observing that "Fisher was the first, and only, Supreme Court decision to find that the testimony implicit in an act of production was a foregone conclusion. In contrast, the government failed to make that showing in the other two relevant decisions: [Doe I and Hubbell].").

Further -- and, importantly, foreshadowing a seeming retrenchment of that troika of Fifth Amendment cases -- Justice Stevens disagreed with the Court's decision in Doe II, 487 U.S. at 219-21, 108 S.Ct. 2341 (Stevens, J., dissenting). He aptly noted:

> A defendant can be compelled to produce material evidence that is incriminating. Fingerprints, blood samples, voice exemplars, handwriting specimens, or other items of physical evidence may be extracted from a defendant against his will. But can he be compelled to use his mind to assist the prosecution in convicting him of a crime? I think not. He may ****1284** in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe -- by word or deed.
>
> [Id. at 219, 108 S.Ct. 2341.]

Justice Stevens's analogy to disclosure of a memorized combination to a wall safe harkened back to the basic principle that the contents of one's mind are protected from compulsion under the Fifth Amendment.

Borrowing from the sound logic of that dissent in Doe II, the Court in Hubbell paused in continuing down this act-of-production line of cases. In Hubbell, the Court considered "whether the Fifth Amendment privilege protects a witness from being compelled to disclose the existence of incriminating documents that the Government is unable to describe with reasonable particularity," and whether the produced documents can be used to "prepare criminal charges" "if the witness produces such documents pursuant to a grant of immunity." 530 U.S. at 29-30, 120 S.Ct. 2037 (footnote omitted).

Hubbell, the witness in question, had pled guilty to mail fraud and tax evasion relating to his billing practices while at a law firm in Arkansas. Id. at 30, 120 S.Ct. 2037. In his plea agreement, ***496** Hubbell agreed to cooperate in an investigation into claims of federal law violation relating to the Whitewater Development Corporation. Ibid. While serving the sentence imposed as a result of his plea agreement, Hubbell was served with a subpoena for several categories of documents. Id. at 31, 120 S.Ct. 2037. He invoked his Fifth Amendment privilege and refused to comply. Ibid.

After he was offered immunity pursuant to 18 U.S.C. § 6003(a), Hubbell produced thousands of pages of requested documents and records. Ibid. Those documents led to incriminating information that spawned a second prosecution for unrelated wire fraud and other tax-related crimes. Ibid. The District Court dismissed the indictment, in part because the "use of the subpoenaed documents violated [18 U.S.C.] § 6002 because all of the evidence" that would be offered against Hubbell would be derived "from the testimonial aspects of respondent's immunized act of producing those documents." Id. at 31-32, 120 S.Ct. 2037. The Court of Appeals for the District of Columbia vacated the judgment and remanded for further proceedings. Id. at 32, 120 S.Ct. 2037.

In the Supreme Court's analysis, written by Justice Stevens, the question was framed as whether "incriminating information derived directly or indirectly from the compelled testimony" was protected by the Fifth Amendment. Id. at 38, 120 S.Ct. 2037. In fact, more narrowly, the Government was not intending to use the act of producing the documents and records against defendant at trial, but rather the information the underlying documents conveyed. Id. at 41, 120 S.Ct. 2037.

The Court concluded that the government had made "derivative use" of the material, and that "[i]t is apparent from the text of the subpoena itself that the prosecutor needed

respondent's assistance both to identify potential sources of information and to produce those sources." Ibid. The Court distinguished its analysis from that used in Fisher, noting:

> Whatever the scope of this "foregone conclusion" rationale, the facts of this case plainly fall outside of it. While in Fisher the Government already knew that the documents were in the attorneys' possession and could independently **1285 confirm their existence and authenticity through the accountants who created them, here the *497 Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent. The Government cannot cure this deficiency through the overbroad argument that a businessman such as respondent will always possess general business and tax records that fall within the broad categories described in this subpoena.
>
> [Id. at 44-45, 120 S.Ct. 2037 (emphasis added).]

The Court ultimately determined "that the constitutional privilege against self-incrimination protects the target of a grand jury investigation from being compelled to answer questions designed to elicit information about the existence of sources of potentially incriminating evidence." Id. at 43, 120 S.Ct. 2037. Given the breadth and depth of the requested documents, the Court concluded that the defendant's response was the "functional equivalent of the preparation of an answer to either a detailed written interrogatory or a series of oral questions at a discovery deposition," id. at 41-42, 120 S.Ct. 2037, and it was "abundantly clear" to the Court that Hubbell's compelled production of the documents was the catalyst to his eventual second prosecution, id. at 42, 120 S.Ct. 2037. Notably, the Court stated that the government's "fishing expedition," id. at 42, 120 S.Ct. 2037, was more akin to compelling someone to provide the combination to a safe than the key to a lockbox, id. at 43, 120 S.Ct. 2037. Thus, the Court resorted once again to the invariable Fifth Amendment protection that must shield inquisitions into mentally cached information or thought processes. Ibid. [2]

C.

From those Supreme Court decisions involving production of physical documents, state courts and the federal circuits differ in *498 their efforts to apply the act-of-production doctrine to the forced disclosure of a PIN or password to bypass security and obtain access to the contents of an encrypted device.

There appears near unanimity in recognizing that in compelling disclosure of a passcode the compelled individual must use his or her mind and, further, that the act provides at least inferences about the existence, possession or control, and authenticity of the material or documents sought by the government. Seo, 148 N.E.3d at 957-58 n.3. Thus, the cases agree that an act of production is involved in compelling disclosure of a passcode.

The decisions splinter, however, over what the compelled act produces, and that decision relatedly affects what those courts hold the government must establish in order for the foregone conclusion exception to apply. Some courts hold that the order **1286 for decryption seeks only the password. See, e.g., State v. Stahl, 206 So. 3d 124, 133 (Fla. Dist. Ct. App. 2016); Commonwealth v. Jones, 481 Mass. 540, 117 N.E.3d 702, 714 (2019); see also United States v. Apple MacPro Comput., 851 F.3d 238, 248 n.7 (3d Cir. 2017) (suggesting without deciding that the password is the proper focus). Other courts find such orders indistinguishable from compelling production of the documents and materials housed on the encrypted device. See, e.g., United States v. Doe (In re Grand Jury Subpoena Duces Tecum dated March 25, 2011), 670 F.3d 1335, 1346 (11th Cir. 2012) (analogizing decryption to the production of a combination to a safe because it uses the contents of the defendant's mind and implies factual statements about the defendant's connection to the contents on encrypted devices); G.A.Q.L. v. State, 257 So. 3d 1058, 1062 (Fla. Dist. Ct. App. 2018); Seo, 148 N.E.3d at 957 (describing the act of production as continuing to link the means of production to the documents ultimately produced).

*499 In Seo v. State, the Indiana Supreme Court recently addressed the constitutional implications of compelling an individual to produce the passcode to his or her locked

smartphone, holding such compulsion would violate one's Fifth Amendment privilege against self-incrimination. 148 N.E.3d at 954. While Seo addressed the Fifth Amendment question with respect to a subpoena that would have allowed an unlimited search of the contents of a woman's phone, the court in Seo highlighted the inapplicability of the foregone conclusion doctrine in the context of smartphones generally. Id. at 959-62.

The Seo opinion astutely observed that "production of an unlocked smartphone is unlike the compelled production of specific business documents." Id. at 959. The Seo court noted that even the Supreme Court in Fisher recognized the difference between subpoenas that sought business "documents of unquestionable relevance to the tax investigation," and subpoenas of more personal documents, which might present "[s]pecial problems of privacy." Id. at 959 (alteration in original) (quoting Fisher, 425 U.S. at 401 n.7, 96 S.Ct. 1569). Importantly, the Seo decision conveys the Indiana Supreme Court's reasons for being wary of employing the foregone conclusion exception, citing among those reasons both its questionable viability and that it was crafted for a different context. Id. at 962. The Seo court ultimately found that it would be "imprudent" to adopt the foregone conclusion exception to permit the State to compel a defendant to disclose a smartphone's passcode. Id. at 960. It is not the only recent case to have not walked down the "foregone conclusion" path. See id. at 962 n.7.

The United States Supreme Court has not addressed the differences that have developed from courts applying the act-of-production analytic framework -- developed in the context of the compelled production of books, records, and physical documents -- to encrypted devices. [3]

**1287 *500 D.

Until the Court clarifies its intentions about application of the act of production doctrine in this setting, I would follow the only sure directional signs the Court has given -- the same themes I introduced at the outset of this analytic section.

First, the forced disclosure of mentally cached information that represents the contents of one's mind is violative of the Fifth Amendment's protections. The Court's recurring metaphor of the combination to a safe, unmistakably included in the majority opinion in Hubbell, harkens back to the classic notion, first expressed in Boyd, that the Fifth Amendment has roots in protection of personal autonomy from government compulsion. It signals, for me, the Court's unwillingness to hold that the Fifth Amendment permits the government to compel one's inner held thoughts in order to assist in one's own prosecution. The memorized passcode is classic contents-of-mind material. See Seo, 148 N.E.3d at 960. It is simply off limits under the Fifth Amendment.

To the extent that Fisher created an act-of-production analysis for use in considering, from a Fifth Amendment perspective, the government's efforts to obtain already existing physical documents, I would not expansively apply that precedent to permit it to force disclosure of the contents of one's mind, as is required in the application involved in this matter. The government should not *501 be permitted to force defendant to cooperate in his own prosecution by obtaining, through his entry of passcodes, access to information the government believes will be incriminating. The government may have a search warrant for the phones' contents, and it may physically have the phones. But, like the wall safe, the government has to obtain access in a way other than compelling defendant into providing the PIN or passcode to obtain access. That testimonial act -- an act of compelled cooperation in his own prosecution -- is a step beyond what Hubbell says is required. See Hubbell, 530 U.S. at 43-44, 120 S.Ct. 2037.

Second, I would not adopt and apply the foregone conclusion exception, which, at last word, the Court has declined to use and has questioned what it even means. See id. at 44, 49-50, 120 S.Ct. 2037. In my judgment, the single use of the descriptor "foregone conclusion" in reference to the documents the Supreme Court found unprotected by the self-incrimination privilege in Fisher does not merit its current status as a "doctrine" deserving of expansive use outside of the original tax document setting in which it was first mentioned. Cf. Seo, 148 N.E.3d at 961-62 (questioning the exception's viability outside of its original context). [4]

***502** The exception's only use by the Court in Fisher does not resemble its application ****1288** to information on an encrypted device. Id. at 960-61. The exception originated in the setting of the government ferreting out already existing, physical documents held by another person. It requires expansion to be used here. Its lineage does not merit its use in the present context of overriding the privilege to keep one's thoughts and recollections to one's self and not turn that over to the government for use in easing its investigatory efforts. Other courts also have recently declined to apply it or have not even acknowledged it when addressing how the Fifth Amendment applies to compelled disclosure of the passcode to an encrypted smartphone. See, e.g., Commonwealth v. Davis, —— Pa. ——, 220 A.3d 534, 550 (2019) and other cases cited in Seo, 148 N.E.3d at 962 n.7). [5]

Rather, I would adhere to the Court's bright line: the contents of one's mind are not available for use by the government in its effort to prosecute an individual. The private thoughts, ideas, and information retained in one's mind are not subject to compelled recollection and disgorgement for use in a person's own prosecution. That practice, reminiscent of an inquisition, was abolished by the Fifth Amendment's inclusion in the Constitution and was as ***503** certainly forbidden through the common law of this state from its earliest times.

In sum, I would hold that the Fifth Amendment was properly invoked by defendant when resisting the State's motion to compel the passcodes. In my view, it is error to affirm the Appellate Division judgment. Further, I would not rest that determination on the application of federal constitutional principles alone.

Defendant also claims he is protected under State law from being compelled by judicial order to disclose the passcode to decrypt the secured contents of phones seized in the government's investigation of him. In my view, his claim is right.

III.

A.

New Jersey has historically provided broad protection against self-incrimination ****1289** through our common law, rules of evidence, and statutes. This expansive protection has been recognized as exceeding that which is provided under federal law. See State v. Hartley, 103 N.J. 252, 286, 511 A.2d 80 (1986). And we have never suggested any malleability in the steadfastly rigorous protection of the privilege because it is not codified in the State Constitution -- an act viewed as unnecessary in light of the revered status of the privilege from the earliest of days in New Jersey. State v. Fary, 19 N.J. 431, 434-35, 117 A.2d 499 (1955); see also State v. Zdanowicz, 69 N.J.L. 619, 622, 55 A. 743 (E. & A. 1903). [6]

***504** Under our present Rules of Evidence and their counterparts codified in law, the protection against self-incrimination provides: "Every person has in any criminal action in which he is an accused a right not to be called as a witness and not to testify." N.J.S.A. 2A:84A-17(1); N.J.R.E. 501. New Jersey's privilege applies "in any ... proceeding ... where the answers might tend to [be] incriminat[ing]." State v. P.Z., 152 N.J. 86, 101, 703 A.2d 901 (1997) (quoting Minnesota v. Murphy, 465 U.S. 420, 426, 104 S.Ct. 1136, 79 L.Ed.2d 409 (1984)). Under N.J.S.A 2A:84A-18, "a matter will incriminate," if, in relevant part,

> (a) ... it constitutes an element of a crime ... , or (b) is a circumstance which with other circumstances would be a basis for a reasonable inference of the commission of such a crime, or (c) is a clue to the discovery of a matter which is within clauses (a) or (b) above; provided, a matter will not be held to incriminate if it clearly appears that the witness has no reasonable cause to apprehend a criminal prosecution.

The history of New Jersey's common law protection against self-incrimination dates back to colonial times, as has been summarized by this Court before.

> The privilege of a witness against being compelled to incriminate himself, of ancient origin, is precious to free men as a restraint against high-handed and arrogant inquisitorial practices. 8 Wigmore, Evidence 276 et seq. (3d ed. 1940); Edwin S. Corwin, The Supreme Court's Construction of the Self-Incrimination Clause, 29 Mich. L. Rev. 1, 3-9 (1930). It has survived centuries of hot controversy periodically rekindled when there is popular impatience that its protection sometimes allows the guilty to escape. It has endured as a wise and necessary protection of the individual against arbitrary power; the price of occasional failures of justice under its protection is paid in the larger interest of the general personal security. "The wisdom of the exemption has never been universally assented to since the days of Bentham, ****1290** many doubt it today, and it is best defended not as an unchangeable principle of universal justice, but a law proved by experience to be expedient." Twining v. New Jersey, 211 U.S. 78, 113, 29 S.Ct. 14, 53 L.Ed. 97 (1908). Although not written into our State Constitution (as it is in the Fifth ***505** Amendment to the Federal Constitution and in the constitutions of all our sister states except Iowa), and not given even statutory expression until it appeared as section 4 of the Evidence Act of 1855, L. 1855, c. 136, § 4, ¶ 668, now N.J.S.[A.] 2A:81-5, the privilege has been firmly established in New Jersey since our beginnings as a State. Zdanowicz, 69 N.J.L. 619, 55 A. 743; State v. Miller, 71 N.J.L. 527, 60 A. 202 (E. & A. 1905); Fries v. Brugler, 12 N.J.L. 79 (Sup. Ct. 1830); In re Vince, 2 N.J. 443, 67 A.2d 141 (1949); In re Pillo, 11 N.J. 8, 93 A.2d 176 (1952).
>
> [Fary, 19 N.J. at 434-35, 117 A.2d 499.]

The right has always been regarded as critical. State v. Vincenty, 237 N.J. 122, 132, 202 A.3d 1273 (2019) ("The importance of the common law right 'is not diminished by the lack of specific constitutional articulation.' " (quoting P.Z., 152 N.J. at 101, 703 A.2d 901)). Our State's broad embrace of providing robust protection against self-incrimination traces back to the early founders' repugnance to any practice that compelled an individual to cooperate with the authorities in securing his or her own conviction. In an oft-quoted passage from an opinion Justice Brennan wrote for this Court, he explained the underlying rationale for the common law privilege developed in New Jersey:

> In modern concept its wide acceptance and broad interpretation rest on the view that compelling a person to convict himself of crime is "contrary to the principles of a free government" and "abhorrent to the instincts of an American," that while such a coercive practice "may suit the purposes of despotic power, ... it cannot abide the pure atmosphere of political liberty and personal freedom."
>
> [In re Pillo, 11 N.J. 8, 15-16, 93 A.2d 176 (1952) (quoting Boyd, 116 U.S. at 632, 6 S.Ct. 524).]

Tellingly, Justice Brennan's Pillo opinion incorporated Boyd's themes in the fulsome enforcement of the right against self-incrimination. That emphasis on the importance of the privacy themes of the privilege was repeated by Justice Brennan while a member of the United States Supreme Court. When the Supreme Court's majority opinion in Fisher, written by Justice White, distanced itself from Boyd and moved to its act-of-production analysis, Justice Brennan voiced concern about the new direction, specifically his worry that the approach would not do justice to privacy. 425 U.S. at 416-17, 96 S.Ct. 1569 (Brennan, J., concurring) (emphasizing that "precedent[ ] and history teach" that personal privacy is "a factor controlling in part ... the scope of the ***506** privilege," not a "byproduct," and that "the scope of the privilege ... [must have] the reach necessary to protect the cherished value of privacy which it safeguards").

That backdrop is important to how I believe this Court should consider Boyd's significance in this matter. According to our last word on the subject, this Court never let loose its embrace of Boyd, which I believe should continue to guide us in the present matter.

B.

In ****1291** In re Grand Jury Proceedings of Guarino, 104 N.J. 218, 516 A.2d 1063 (1986), this Court surveyed the Supreme Court's newly developed act-of-production case law in Fisher and Doe I and, although our Court's outcome

in that matter was split, this Court's view of the new case law was not. Both the majority and dissenting opinions said that the common law of New Jersey embraced Boyd's approach and declared that Boyd was most in keeping with the underlying rationale for our state's common law privilege against self-incrimination. In fact, both specifically said that Fisher and Doe I were not consistent with our jurisprudence that provided a higher protection against government compelled self-incrimination and would not be adopted for use in this State. Then, as noted, the two opinions differed in their outcomes.

The majority stated that it was hewing to an assessment of the privacy interest in the ultimate contents of the produced documents, reinforcing its commitment to Boyd's protection of private documents. Id. at 231, 516 A.2d 1063. Focusing on the contents of the documents sought by the government, the majority opinion concluded that the business records of a sole proprietor were not in a specific zone of privacy that deserved protection. Id. at 232, 516 A.2d 1063. The Court noted that the documents had been disclosed to third parties and were not an extension of private or intimate aspects of one's life, which were, in the majority's view, the type of document that the privilege protected. Id. at 232-33, 516 A.2d 1063.

***507** The dissent disagreed with the majority's analysis as not properly adhering to Boyd's principles, which the majority was expressly reinforcing as the doctrine of this State. And, importantly, the dissent took the occasion to deconstruct the analytic structure of the new federal paradigm, criticizing it for ignoring the privacy roots of Boyd that had been "sedulously adhered to" for decades and factored into the "determin[ation] whether individuals could withhold the production, as well as the contents, of incriminating personal documents." Id. at 239-40, 516 A.2d 1063 (Handler, J., dissenting). For the dissent, the federal law's turn was out of sync with the history and import of the Fifth Amendment's protection against compelled incrimination, and the dissent explained in detail why adherence to our common law's approach required adherence to Boyd's recognition of privacy and personal autonomy. Id. at 243, 516 A.2d 1063.

In sum, both opinions in Guarino espoused fidelity to Boyd's acknowledgment that the privilege against self-incrimination must protect the integrity and privacy of the individual. Yet, I believe that my colleagues in the majority misconstrue Guarino's import when concluding that the Court's holding today stays true to its principles.

In continuing New Jersey's steadfast protection of personal privacy and autonomy, Guarino stands for the proposition that Boyd remains valid in that respect in our jurisdiction. Indeed, it is one of many proud decisions in New Jersey that have adhered to our belief, in self-incrimination settings, that New Jersey provides enhanced protections for personal privacy and autonomy. See, e.g., State v. Muhammad, 182 N.J. 551, 568-69, 868 A.2d 302 (2005) (holding that a suspect's silence, while in custody, at or near time of arrest, cannot be used against him); State v. Strong, 110 N.J. 583, 593-595, 542 A.2d 866 (1988) (concluding that New Jersey law not only protects against improper conduct to obtain compelled testimony, but also protects against its improper use because ****1292** such use "is the difference between the constitutional right in not being compelled to incriminate oneself and the right in not having one's ***508** privacy unreasonably invaded"); Hartley, 103 N.J. at 285-86, 511 A.2d 80 (recognizing that the state law privilege against self-incrimination exceeds the protections provided under the Fifth Amendment); State v. Deatore, 70 N.J. 100, 112-14, 358 A.2d 163 (1976) (same). [7]

To the extent that the Guarino Court split on the application of those personal privacy principles when it came to documents already in the possession of third parties, that does not support the invasion of private thoughts, as we have here. Defendant is being compelled to disgorge a memorized passcode to allow access to other information on his secure smartphone. In other words, he is being forced to disclose inner thoughts so as to assist law enforcement in his own prosecution. That is contrary to Boyd's tenets about personal freedom and privacy. And it is contrary to all previous decisions from this Court with respect to our state recognized law on the privilege against self-incrimination.

This Court has never before permitted law enforcement to compel from a defendant's lips inner thoughts to assist in his own prosecution. I cannot join in taking our state law in that direction. Therefore, for the same reasons that I would not extend federal law to require what the Supreme Court has not expressly held, so too I would not turn our jurisprudence from the guiding principles it has followed to date.

***509** This intrusive use of compelled cooperation forcing self-incrimination through disclosure of the contents of one's mind is not consistent with our law. It should be rejected as a step backwards from the storied history in this State of protective law concerning personal autonomy and the privacy of one's inner thoughts with respect to the privilege against self-incrimination.

C.

Finally, for completeness, I note that the Appellate Division erred in reading a basis for foregone conclusion into our statute governing what is an incriminating statement. The majority's reasons for similarly adopting that approach are not persuasive and take our law in a direction that is a mistake, in my view. To be clear, I believe that foregone conclusion, as a notion in federal law, has shaky lineage. We should not perpetuate a questionable doctrine.

Further, examination of our statutory provision yields no fertile ground for finding the concept consistent with state law.

New Jersey has enacted statutory protections and an evidentiary rule against self-incrimination, both of which use identical ****1293** language. See N.J.S.A. 2A:84A-17(1); N.J.R.E. 501. Under both N.J.S.A. 2A:84A-17(1) and N.J.R.E. 501, "[e]very person has in any criminal action in which he is an accused a right not to be called as a witness and not to testify." Further, "every natural person has a right to refuse to disclose in an action or to a police officer or other official any matter that will incriminate him or expose him to a penalty." N.J.S.A. 2A:84A-19; N.J.R.E. 503. There are four applicable exceptions to this rule. Most relevant is N.J.S.A. 2A:84A-19(b), which provides that

> no person has the privilege to refuse to obey an order made by a court to produce for use as evidence or otherwise a document, chattel or other thing under his control if some other person or a corporation or other association has a superior right to the possession of the thing ordered to be produced.

In this part of its analysis, the majority views narrowly what is turned over: only the passcodes, which the majority opinion describes ***510** as having "minimal evidentiary significance, do not themselves support an inference that a crime has been committed, nor do they constitute 'clues' " because the passcode is "not substantive information, is not a clue to an element of or the commission of a crime, and does not reveal an inference that a crime has been committed." Ante at ——, —— A.3d at ——. The majority sees no privacy interest being violated because the State has a search warrant for the physical phone. In essence the majority adheres to the Appellate Division's conclusion that

> defendant is not conveying any important facts that the State does not already possess, he is not being required to disclose any 'matter' that would incriminate him or expose him to a penalty. Furthermore, the State has a "superior right of possession" to defendant's passcodes because the trial court has issued two search warrants for defendant's iPhones, which allow the State to obtain the passcodes that may be necessary to access information on the phones.
>
> [State v. Andrews, 457 N.J. Super. 14, 32-33, 197 A.3d 200 (App. Div. 2018).]

In so concluding, the Appellate Division first, and now the majority, improperly, in my view, read the foregone conclusion doctrine into New Jersey jurisprudence in a manner that is both inconsistent with the spirit of our law and not grounded in precedent.

First, the State cannot claim a superior right of access to the passcodes. While the State can claim a legal right to review internal information on the phone pursuant to a warrant, the

State cannot have a superior right to the contents of one's mind -- which here, is the passcode. Both the Appellate Division and the majority's opinion conflate the State's Fourth Amendment right to obtain a valid warrant based on probable cause with defendant's Fifth Amendment right not to be compelled to assist in his own prosecution by being ordered to provide information contained in his mind that can be used to obtain undetermined and unspecified information in the hope it will incriminate him.

Second, the Appellate Division did not properly consider the State's long-codified protections that uphold a person's refusal to disclose incriminating information. Pursuant to N.J.S.A. 2A:84A-18's clear definition of incrimination, something is incriminating

> (a) if it constitutes an element of a crime against this State, or another State or ****1294** the United States, or (b) is a circumstance which with other circumstances would be a ***511** basis for a reasonable inference of the commission of such a crime, or (c) is a clue to the discovery of a matter which is within clauses (a) or (b) above; provided, a matter will not be held to incriminate if it clearly appears that the witness has no reasonable cause to apprehend a criminal prosecution. In determining whether a matter is incriminating under clauses (a), (b) or (c) and whether a criminal prosecution is to be apprehended, other matters in evidence, or disclosed in argument, the implications of the question, the setting in which it is asked, the applicable statute of limitations and all other factors, shall be taken into consideration.
>
> [N.J.S.A. 2A:84A-18 (emphasis added).]

The majority cannot support the claim that the State has a superior right of access to the phone's passcode. And the majority does not properly consider what the passcode would reveal. The majority opinion at times focuses on the passcode, and at others equates the passcode with the evidentiary information the government hopes to find somewhere in the encrypted device's phone and message icons. For this part of its analysis, the majority chooses to isolate the passcode from the hopefully incriminating contents the government wants.

The majority cannot have it both ways -- focusing solely on the passcode sometimes and on the phones and their contents at other times. In my view, the Appellate Division and the majority fail to acknowledge that compelling defendant's participation in obtaining passcodes giving access to the phone would certainly provide more than just a clue to an underlying crime: defendant is being compelled to essentially turn over what is presumed to be incriminating information, in direct violation of his right not to testify against himself.

IV.

For the foregoing reasons, I respectfully dissent from the judgment of the Court. I would hold that the judicial order compelling defendant to disclose the passcode to his smartphone by requiring him to reveal the contents of his mind is a violation of the Fifth Amendment protection against self-incrimination and a violation of our state law protecting the same.

***512** Law enforcement must find another means of obtaining access to the encrypted substantive information on two cell phones whose contents it wishes to search and for which the government has a search warrant. Technological barriers must be overcome without sacrificing constitutional, deep-seated historical protections against governmental intrusions forcing individuals to become assistants in their own prosecutions. Modern technology continues to evolve, bringing new problems; but it also may bring new solutions. The resolution to the present problem must be found in those new technological solutions -- at least until the Supreme Court addresses whether it is now willing to permit forced disclosure of mental thoughts because, in my view, to date, its case law on accessing physical documents, respectfully, does not support the steps being taken here.

CHIEF JUSTICE RABNER and JUSTICES PATTERSON and FERNANDEZ-VINA join in JUSTICE SOLOMON's opinion. JUSTICE LaVECCHIA filed a dissent, in which JUSTICES ALBIN and TIMPONE join.

All Citations

243 N.J. 447, 234 A.3d 1254

Footnotes

1 Lowery also informed the detectives that Andrews had self-identified as a member of the Grape Street Crips.

2 "Apple manufactures smartphones, named iPhones, which run an operating system named iOS. Numerical names designate different versions of the operating system (e.g., iOS 8). Apple adopted full-disk encryption by default in September 2014 with iOS 8." Kristen M. Jacobsen, Note, Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and its Chilling Effect on Law Enforcement, 85 Geo. Wash. L. Rev. 566, 574 (2017) (footnotes omitted). "Full-disk encryption automatically converts everything on a hard drive, including the operating system, into an unreadable form until the proper key (i.e., passcode) is entered." Id. at 573 (internal quotation marks omitted).

3 The panel noted that the parties had not raised the issue of the authenticity of the electronically stored information. Id. at 30, 197 A.3d 200.

4 Encryption keys, like a PIN or passcode, are "essentially a string of numbers or characters" that are applied "to the encrypted data using the algorithm of the given encryption program. By funneling the encrypted data through the algorithm, the data is rendered 'readable' again." Gelfgatt, 11 N.E.3d at 610 n.9.

5 We give deference to the trial court's factual findings and view them as binding upon appeal to the extent that they are "supported by adequate, substantial and credible evidence." Rova Farms Resort, Inc. v. Inv'rs Ins. Co. of Am., 65 N.J. 474, 484, 323 A.2d 495 (1974).

6 In addition to providing four enumerated exceptions to the right to refuse disclosure, see N.J.S.A. 2A:84A-19(a) to (d); N.J.RE. 503(a) to (d), both the statute and the rule specify, through reference to "Rule 37" (renumbered in 1993 as N.J.R.E. 503), that the right may be waived.

7 Defendant does not claim that the amalgamations of numbers, letters, or symbols constituting his passcodes have independent evidentiary significance. Such a claim would not, in any event, change the outcome here in light of the limitations set forth in the trial court's disclosure order.

1 Hereinafter, we refer either to a passcode or personal identification number (PIN) as the means to unlock and decrypt these smartphones' security systems.

2 In a separate opinion, Justice Thomas questioned whether the act-of-production doctrine originating in Fisher is itself consistent with the original meaning of the self-incrimination protection enshrined in the Fifth Amendment. Hubbell, 530 U.S. at 49, 120 S.Ct. 2037 (Thomas, J., concurring). He expressed, joined by the late Justice Scalia, a willingness to reconsider that decision's narrowing of the protection against compelled evidence in light of the Fifth Amendment's historical meaning and scope. Ibid. However, because the issue was not raised by the parties, the concurring Justices declined to address at that time whether the Fifth Amendment has "a broader reach than Fisher holds," although suggesting that it may. Id. at 56, 120 S.Ct. 2037.

3 Decisions splintering over the testimonial nature of the compelled disclosure of passcodes have fostered further splits concerning compelled use of biometrics to decrypt devices, with courts' views about the testimonial nature of compelled disclosure of a passcode informing the analysis regarding biometrics. Compare In re Search of a Residence in Oakland, Cal., 354 F. Supp. 3d 1010, 1015-16 (N.D. Cal. 2019) (finding that compelled production of biometric data was testimonial for Fifth Amendment purposes in the context of a warrant application seeking permission to compel fingerprint or facial recognition device unlocking), and In re Application for a Search Warrant, 236 F. Supp. 3d 1066, 1073-74 (N.D. Ill. 2017) (same as to forced fingerprint device unlocking), with In re the Search of: A White Google Pixel 3 XL Cellphone in a Black Incipio Case, 398 F. Supp. 3d 785, 793-94 (D. Idaho 2019) (finding that a forced

application of a fingerprint to unlock a device was not testimonial for Fifth Amendment purposes), and In re Search of [Redacted] Washington, D.C., 317 F. Supp. 3d 523, 539 (D.D.C. 2018) (same).

4 The Indiana Supreme Court gave sound reasons for being wary about the exception's viability, let alone expanding it.

> The limited, and questionable, application of the foregone conclusion exception also cautions against extending it further. Indeed, Fisher was decided over forty-four years ago, and it remains the lone U.S. Supreme Court decision to find that the exception applied. In the intervening years, the Court has discussed it twice and in only one context: in grand jury proceedings when a subpoena compelled the production of business and financial records. During this same time period, legal scholars -- including three current members of the Supreme Court -- have wondered whether Fisher interpreted the Fifth Amendment too narrowly, calling into question the viability of the foregone conclusion exception itself. See Hubbell, 530 U.S. at 49-56, 120 S.Ct. 2037 (Thomas, J., concurring); Carpenter v. United States, 585 U.S. ——, 138 S. Ct. 2206, 2271, 201 L.Ed.2d 507 (2018) (Gorsuch, J., dissenting); Samuel A. Alito, Jr., Documents and the Privilege Against Self-Incrimination, 48 U. Pitt. L. Rev. 27, 45-51 (1986); see also, e.g., Bryan H. Choi, The Privilege Against Cellphone Incrimination, 97 Tex. L. Rev. Online 73, 74 n.6 (2019); Richard A. Nagareda, Compulsion "To Be a Witness" and the Resurrection of Boyd, 74 N.Y.U. L. Rev. 1575, 1606 & nn.124-25 (1999); Robert Heidt, The Fifth Amendment Privilege and Documents -- Cutting Fisher's Tangled Line, 49 Mo. L. Rev. 439, 443 (1984). Regardless of the foregone conclusion exception's viability, it seems imprudent to extend it beyond its one-time application. Cf. Silverman v. United States, 365 U.S. 505, 510, 512, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961) (deciding not to extend the rationale of a factually distinct case "by even a fraction of an inch").
>
> [Seo, 148 N.E.3d at 961-62.]

5 See, e.g., United States v. Jimenez, 419 F. Supp. 3d 232, 233 (D. Mass. 2020) (denying the government's motion to compel the defendant to disclose his smartphone passcode because it "would force defendant to 'disclose the contents of his own mind' "); In re Search of a Residence in Oakland, Cal., 354 F. Supp. 3d at 1016-18 (relying on the Supreme Court's proposition in Riley v. California, 573 U.S. 373, 393-97, 134 S.Ct. 2473, 189 L.Ed.2d 430 (2014), that phones are entitled to greater privacy protection in concluding that the foregone conclusion doctrine should not be applied in the context of mobile phones).

6 In making an observation about the uncertainty of the Fifth Amendment's reach, our predecessor Court observed:

> It is not deemed necessary to consider whether this [Fifth Amendment] constitutional provision will operate to prevent any state, if it is conceivable that any state should desire to do so, from enacting laws establishing a practice in criminal cases such as is in vogue in countries not following the course of the common law, or permitting an accused person to be subject to such compulsion as may be exerted by harassing examination or other means, forcible or practically forcible, compelling him to testify against himself, or to prevent the adoption by any state of a practice which might produce that effect.
>
> Although we have not deemed it necessary to insert in our constitution this prohibitive provision, the common law doctrine, unaltered by legislation or by lax practice, is by us deemed to have its full force. In New Jersey, no person can be compelled to be a witness against himself.
>
> [Zdanowicz, 69 N.J.L. at 622, 55 A. 743.]

7 Similarly, State law exceeds federal protections for privacy in Fourth Amendment searches and seizures as well. See, e.g., State v. Earls, 214 N.J. 564, 584-89, 70 A.3d 630 (2013) (finding a reasonable expectation of privacy in a person's cell phone location information prior to later federal court case development); State

v. Reid, 194 N.J. 386, 396-99, 945 A.2d 26 (2008) (holding that, regardless of the federal government's failure to find an expectation of privacy, under New Jersey's heightened protections there is a reasonable expectation of privacy in Internet subscriber information, which can reveal intimate details about a person's life); State v. McAllister, 184 N.J. 17, 26-33, 875 A.2d 866 (2005) (holding that, although the federal government does not recognize an expectation of privacy in bank records, New Jersey recognizes that expectation because the revealing information contained in a bank record "provides a virtual current biography" (quoting Burrows v. Superior Court, 13 Cal.3d 238, 118 Cal.Rptr. 166, 529 P.2d 590, 596 (1974))).

851 F.3d 238
United States Court of Appeals, Third Circuit.

UNITED STATES of America
v.
APPLE MACPRO COMPUTER, Apple Mac Mini Computer, Apple i Phone 6 Plus, Ellular Telephone Western Digital My Book For Mac External Hard Drive, Western Digital My Book Velociraptor Duo External Hard Drive
*John Doe, Appellant
*(Pursuant to Rule 12(a), Fed. R. App. P.)

No. 15-3537
|
Argued September 7, 2016
|
(Filed: March 20, 2017)

Synopsis

Background: Government filed motion for order to show cause why suspect in investigation of child pornography accessed through the internet should not be held in civil contempt for refusing to comply with decryption order issued pursuant to All Writs Act requiring him to produce passwords for encrypted digital devices that government had seized pursuant to valid search warrant. The United States District Court for the Eastern District of Pennsylvania, No. 15-mj-00850-001, L. Felipe Restrepo, J., granted the motion. Suspect appealed.

Holdings: The Court of Appeals, Vanaskie, Circuit Judge, held that:

[1] District Court had subject matter jurisdiction to issue the decryption order;

[2] decryption order was a necessary and appropriate means of effectuating the original search warrant; and

[3] there was no clear or obvious error, and therefore no plain error, as to determination that decryption order did not violate suspect's Fifth Amendment protection against self-incrimination.

Affirmed.

Procedural Posture(s): On Appeal.

West Headnotes (21)

[1] **Federal Courts** Injunction

The Court of Appeals ordinarily exercises plenary review over the District Court's authority to issue an order pursuant to the All Writs Act. 28 U.S.C.A. § 1651.

1 Cases that cite this headnote

[2] **Contempt** Review

The Court of Appeals reviews a District Court's decision on a motion for contempt for abuse of discretion.

[3] **Federal Courts** Plain error

When the party seeking review has failed to preserve the issue in the trial court, the appellate court reviews only for plain error.

[4] **Federal Courts** Jurisdiction

The Court of Appeals exercises plenary review over challenges concerning subject matter jurisdiction.

1 Cases that cite this headnote

[5] **Federal Courts** Writs in general

The All Writs Act does not itself confer any subject matter jurisdiction, but rather only allows a federal court to issue writs in aid of its existing jurisdiction, and thus, a federal court has subject matter jurisdiction over an application for an All Writs Act order only when it has subject matter jurisdiction over the underlying order that the All Writs Act order is intended to effectuate. 28 U.S.C.A. § 1651(a).

2 Cases that cite this headnote

[6] **Federal Courts** Writs in general

A federal court may issue an All Writs Act order only as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained. 28 U.S.C.A. § 1651(a).

2 Cases that cite this headnote

[7] **Searches and Seizures** Execution and Return of Warrants

Based on subject matter jurisdiction to issue the search warrant, United States Magistrate Judge had subject matter jurisdiction to issue decryption order, under All Writs Act, requiring suspect in investigation of child pornography accessed through the internet to produce passwords for encrypted digital devices that government had seized pursuant to valid search warrant issued by the Magistrate Judge. 28 U.S.C.A. § 1651(a); Fed. R. Crim. P. 41.

2 Cases that cite this headnote

[8] **Contempt** Matters determined on hearing

A civil contempt proceeding generally does not open to reconsideration the legal or factual basis of the order alleged to have been disobeyed.

[9] **Contempt** Nature and form of remedy and jurisdiction

Judicial review of a grand jury subpoena may be obtained only by refusal to comply with the subpoena, with the validity of the subpoena being litigated in the ensuing contempt proceeding.

[10] **Federal Courts** Plain error

To obtain reversal on appellate review for plain error, an appellant must show four elements: (1) there is an error; (2) the error is clear or obvious, rather than subject to reasonable dispute; (3) the error affected the appellant's substantial rights, which in the ordinary case means it affected the outcome of the District Court proceedings; and (4) the error seriously affects the fairness, integrity, or public reputation of judicial proceedings.

1 Cases that cite this headnote

[11] **Searches and Seizures** Execution and Return of Warrants

Decryption order issued under All Writs Act, requiring suspect in investigation of child pornography accessed through the internet to produce passwords for encrypted digital devices that government had seized pursuant to valid search warrant, was a necessary and appropriate means of effectuating the original search warrant; suspect was not far removed from the underlying controversy, compliance with the order required minimal effort, and without suspect's assistance there was no conceivable way in which the search warrant authorized by the District Court could be successfully accomplished. 28 U.S.C.A. § 1651(a); Fed. R. Crim. P. 41.

3 Cases that cite this headnote

[12] **Federal Courts** Writs in general

The All Writs Act extends to anyone in a position to frustrate the implementation of a court order or the proper administration of justice as long as there are appropriate circumstances for doing so. 28 U.S.C.A. § 1651.

1 Cases that cite this headnote

[13] **Contempt** Review

On appeal, by suspect in investigation of child pornography accessed through the internet, of District Court's order finding him in civil contempt of decryption order issued under All Writs Act, which required him to produce passwords for encrypted digital devices that government had seized pursuant to valid search warrant, the Court of Appeals could not reconsider whether the decryption order violated

the suspect's Fifth Amendment protection against self-incrimination. U.S. Const. Amend. 5; 28 U.S.C.A. § 1651(a); Fed. R. Crim. P. 41.

2 Cases that cite this headnote

[14] **Witnesses** Privilege of Accused in Criminal Prosecution

The Fifth Amendment protection against self-incrimination does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a testimonial communication that is incriminating. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[15] **Witnesses** Self-Incrimination

To be "testimonial," for purposes of Fifth Amendment protection against incriminating testimonial communications, a communication must either explicitly or implicitly relate a factual assertion or disclose information. U.S. Const. Amend. 5.

1 Cases that cite this headnote

[16] **Witnesses** Privilege as to production of documents

When the production of evidence concedes the existence, custody, and authenticity of that evidence, the Fifth Amendment privilege against self-incrimination applies because that production constitutes compelled testimony. U.S. Const. Amend. 5.

5 Cases that cite this headnote

[17] **Witnesses** Privilege as to production of documents

The "foregone conclusion rule," which acts as an exception to the otherwise applicable act-of-production doctrine, provides that the Fifth Amendment protection against self-incrimination does not apply to an act of production when any potentially testimonial component of the act of production, such as the existence, custody, and authenticity of evidence, is a foregone conclusion that adds little or nothing to the sum total of the Government's information. U.S. Const. Amend. 5.

17 Cases that cite this headnote

[18] **Witnesses** Privilege as to production of documents

For the foregone conclusion rule to apply as an exception to the otherwise applicable act-of-production doctrine, under which doctrine Fifth Amendment protection against self-incrimination applies to production of evidence that concedes the existence, custody, and authenticity of that evidence, the Government must be able to describe with reasonable particularity the documents or evidence it seeks to compel. U.S. Const. Amend. 5.

10 Cases that cite this headnote

[19] **Criminal Law** In Preliminary Proceedings

There was no clear or obvious error, and therefore no plain error, as to determination that decryption order issued under All Writs Act, which required suspect in investigation of child pornography accessed through the internet to produce passwords for encrypted digital devices that government had seized pursuant to valid search warrant, did not violate suspect's Fifth Amendment protection against self-incrimination because foregone conclusion rule was applicable as exception to otherwise applicable act-of-production doctrine; Government provided evidence to show both that files existed on encrypted portions of devices and that suspect could access the files. U.S. Const. Amend. 5; 28 U.S.C.A. § 1651(a); Fed. R. Crim. P. 41.

10 Cases that cite this headnote

[20] **Contempt** Presumptions and burden of proof

In a civil contempt proceeding, when a defendant raises a challenge of impossibility of compliance, the defendant bears the burden of production.

[21] Contempt Ability to obey

Suspect in investigation of child pornography did not satisfy his burden of production with respect to impossibility of compliance, at civil contempt hearing regarding suspect's failure to comply with decryption order issued under All Writs Act, which required suspect to produce passwords for encrypted digital devices that government had seized pursuant to valid search warrant; suspect did not assert that he had been unable to remember the passwords for decryption when the police had asked him to enter those passwords. U.S. Const. Amend. 5; 28 U.S.C.A. § 1651(a); Fed. R. Crim. P. 41.

***241** On Appeal from the United States District Court for the Eastern District of Pennsylvania (D.C. No. 15-mj-00850-001) District Judge: Hon. L. Felipe Restrepo

Attorneys and Law Firms

Keith M. Donoghue [ARGUED], Brett G. Sweitzer, Leigh M. Skipper, Federal Community Defender Office for the Eastern District of Pennsylvania, 601 Walnut Street, Suite 540 West Philadelphia, PA 19106, Counsel for Defendant-Appellant

Christopher C. Walsh, Adam Schwartz, Mark Rumold [ARGUED], Andrew Crocker, Electronic Frontier Foundation, 815 Eddy Street, San Francisco, CA 94109, Counsel for Amicus Curiae

Leslie Caldwell, Nathan Judish [ARGUED], Bernadette McKeon, Michelle Rotella, Office of the United States Attorney, 615 Chestnut Street, Suite 1250, Philadelphia, PA 19106, Counsel for Plaintiff-Appellee

Before: JORDAN, VANASKIE, and NYGAARD, Circuit Judges.

OPINION

VANASKIE, Circuit Judge.

This appeal concerns the Government's ability to compel the decryption of digital devices when the Government seizes those devices pursuant to a valid search warrant. The District Court found Appellant John Doe in civil contempt for refusing to comply with an order issued pursuant to the All Writs Act, 28 U.S.C. § 1651, which required him to produce several seized ***242** devices in a fully unencrypted state. Doe contends that the court did not have subject matter jurisdiction to issue the order and that the order itself violates his Fifth Amendment privilege against self-incrimination. For the reasons that follow, we will affirm the District Court's order.

I.

During an investigation into Doe's access to child pornography over the internet, the Delaware County Criminal Investigations Unit executed a valid search warrant at Doe's residence. During the search, officers seized an Apple iPhone 5S and an Apple Mac Pro Computer with two attached Western Digital External Hard Drives, all of which had been protected with encryption software.[1] Police subsequently seized a password-protected Apple iPhone 6 Plus as well.

Agents from the Department of Homeland Security then applied for a federal search warrant to examine the seized devices. Doe voluntarily provided the password for the Apple iPhone 5S, but refused to provide the passwords to decrypt the Apple Mac Pro computer or the external hard drives. Despite Doe's refusal, forensic analysts discovered the password to decrypt the Mac Pro Computer, but could not decrypt the external hard drives. Forensic examination of the Mac Pro revealed an image of a pubescent girl in a sexually provocative position and logs showing that the Mac Pro had been used to visit sites with titles common in child exploitation, such as "toddler_cp," "lolicam," "tor-childporn," and "pthc."[2] (App. 39.) The Forensic examination also disclosed that Doe had downloaded thousands of files known by their "hash" values to be child pornography.[3] The files, however, were not on the Mac Pro, but instead had been stored on the encrypted external hard drives. Accordingly, the files themselves could not be accessed.

As part of their investigation, the Delaware County law enforcement officers also interviewed Doe's sister, who had lived with Doe during 2015. She related that Doe had shown her hundreds of images of child pornography on the encrypted external hard drives. She told the investigators ***243** that the

external hard drives included "videos of children who were nude and engaged in sex acts with other children." (App. 40.) Doe provided the password to access the iPhone 6 Plus, but did not grant access to an application on the phone which contained additional encrypted information. Forensic analysts concluded that the phone's encrypted database contained approximately 2,015 image and video files.

On August 3, 2015, upon application of the Government, a Magistrate Judge issued an order pursuant to the All Writs Act requiring Doe to produce his iPhone 6 Plus, his Mac Pro computer, and his two attached external hard drives in a fully unencrypted state (the "Decryption Order"). Doe did not appeal the Decryption Order. Instead, he filed with the Magistrate Judge a motion to quash the Government's application to compel decryption, arguing that his act of decrypting the devices would violate his Fifth Amendment privilege against self-incrimination.

On August 27, 2015, the Magistrate Judge denied Doe's Motion to Quash and directed Doe to fully comply with the Decryption Order (the "Quashal Denial"). The Magistrate Judge acknowledged Doe's Fifth Amendment objection but held that, because the Government possessed Doe's devices and knew that their contents included child pornography, the act of decrypting the devices would not be testimonial for purposes of the Fifth Amendment privilege against self-incrimination. The Quashal Denial stated that a failure to file timely objections could result in the waiver of appellate rights. Doe did not file any objections to the Quashal Denial and did not seek review by way of appeal, writ of mandamus, or otherwise.

Approximately one week after the Quashal Denial, Doe and his counsel appeared at the Delaware County Police Department for the forensic examination of his devices. Doe produced the Apple iPhone 6 Plus, including the files on the secret application, in a fully unencrypted state by entering three separate passwords on the device. The phone contained adult pornography, a video of Doe's four-year-old niece in which she was wearing only her underwear, and approximately twenty photographs which focused on the genitals of Doe's six-year-old niece. Doe, however, stated that he could not remember the passwords necessary to decrypt the hard drives and entered several incorrect passwords during the forensic examination. The Government remains unable to view the decrypted content of the hard drives without his assistance.

Following the forensic examination, the Magistrate Judge granted the Government's Motion for Order to Show Cause Why Doe Should Not Be Held in Contempt, finding that Doe willfully disobeyed and resisted the Decryption Order. Based on the evidence presented at the hearing, the Magistrate Judge found that Doe remembered the passwords needed to decrypt the hard drives but chose not to reveal them because of the devices' contents. The Magistrate Judge ordered Doe to appear before the District Court to show cause as to why he should not be held in civil contempt.

On September 30, 2015, after a hearing, the District Court granted the Government's motion to hold Doe in civil contempt. On October 5, 2015, the District Court issued a "Supplemental Order to articulate the reasons for its September 30th Order." (App. at 12.) The District Court noted that the Government's prima facie case of contempt was largely, if not entirely, uncontested. While the Government presented several witnesses to support its motion, Doe neither testified nor called witnesses. He offered no physical or ***244** documentary evidence into the record and provided no explanation for his failure to comply with the Decryption Order. The District Court remanded Doe to the custody of the United States Marshals to be incarcerated until he fully complies with the Decryption Order. This timely appeal followed.

II.

[1] **[2]** **[3]** **[4]** We have appellate jurisdiction under 28 U.S.C. § 1291. We ordinarily exercise plenary review over the District Court's authority to issue an order pursuant to the All Writs Act, *Grider v. Keystone Health Plan Cent., Inc.*, 500 F.3d 322, 327 (3d Cir. 2007), and "review a district court's decision on a motion for contempt for abuse of discretion." *Marshak v. Treadwell*, 595 F.3d 478, 485 (3d Cir. 2009). However, when the party seeking review has failed to preserve the issue in the trial court, we review only for plain error. *See Brightwell v. Lehman,* 637 F.3d 187, 193 (3d Cir. 2011); *Nara v. Frank*, 488 F.3d 187, 194 (3d Cir. 2007). We nonetheless exercise plenary review over challenges concerning subject matter jurisdiction. *United States v. Merlino*, 785 F.3d 79, 82 (3d Cir. 2015).

III.

Doe raises two primary arguments as to why he should not be held in contempt. First, he asserts that the District Court lacked subject matter jurisdiction to issue the Decryption Order under the All Writs Act. Thus, he argues that he is not in contempt of any valid order and the judgment of contempt must be vacated. Second, Doe contends that the Decryption Order violates his Fifth Amendment privilege against self-incrimination.

A.

[5] **[6]** Doe's first challenge concerns the All Writs Act, which permits federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a). The All Writs Act does not itself confer any subject matter jurisdiction, but rather only allows a federal court to issue writs "in aid of" its existing jurisdiction. *Clinton v. Goldsmith*, 526 U.S. 529, 534, 119 S.Ct. 1538, 143 L.Ed.2d 720 (1999); *Syngenta Crop Prot., Inc. v. Henson*, 537 U.S. 28, 31, 123 S.Ct. 366, 154 L.Ed.2d 368 (2002); *see also In re Arunachalam*, 812 F.3d 290, 292 (3d Cir. 2016) (per curiam). Therefore, a court has subject matter jurisdiction over an application for an All Writs Act order only when it has subject matter jurisdiction over the underlying order that the All Writs Act order is intended to effectuate. Additionally, a federal court may only issue an All Writs Act order "as may be necessary or appropriate to effectuate and prevent the frustration of orders it has previously issued in its exercise of jurisdiction otherwise obtained." *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977).

[7] Doe contends that the Magistrate Judge did not have subject matter jurisdiction to issue the Decryption Order because the Government should have compelled his compliance by means of the grand jury procedure and not the All Writs Act. The grand jury process, however, is not the exclusive means by which the Government may collect evidence prior to indictment. *See* *Zurcher v. Stanford Daily*, 436 U.S. 547, 559, 98 S.Ct. 1970, 56 L.Ed.2d 525 (1978) (allowing the Government to proceed by search warrant despite insistence that the investigation should proceed by subpoena); ***245** *United States v. Educ. Dev. Network Corp.*, 884 F.2d 737, 743 (3d Cir. 1989) (rejecting the argument that the Government could not obtain evidence by means of a search warrant and must proceed solely by grand jury). Here, the Magistrate Judge had subject matter jurisdiction under Federal Rule of Criminal Procedure 41 to issue a search warrant [4] and therefore had jurisdiction to issue an order under the All Writs Act that sought "to effectuate and prevent the frustration" of that warrant. *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 172, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977).

[8] **[9]** **[10]** In arguing that the Magistrate Judge did not have subject matter jurisdiction to issue the Decryption Order, Doe also challenges the merits of that order, contending that it was not a "necessary and appropriate means" of effectuating the original warrant as required by the Supreme Court in *New York Telephone*. A contempt proceeding, however, generally " 'does not open to reconsideration the legal or factual basis of the order alleged to have been disobeyed.' " [5] *United States v. Rylander*, 460 U.S. 752, 756, 103 S.Ct. 1548, 75 L.Ed.2d 521 (1983) (quoting *Maggio v. Zeitz*, 333 U.S. 56, 69, 68 S.Ct. 401, 92 L.Ed. 476 (1948)); *In re Contemporary Apparel, Inc.*, 488 F.2d 794, 798 (3d Cir. 1973) (same). Furthermore, Doe did not argue in the District Court that the Decryption Order was not an appropriate exercise of authority under the All Writs Act. Thus, even if the propriety of the Decryption Order was before us, our review would be limited to plain error. *Brightwell*, 637 F.3d at 193. Under this framework, an appellant must show four elements: "(1) there is an 'error'; (2) the error is 'clear or obvious, rather than subject to reasonable dispute'; (3) the error 'affected the appellant's substantial rights, which in the ordinary case means' it 'affected the outcome of the district court proceedings'; and (4) 'the error seriously affect[s] the fairness, integrity or public reputation of judicial proceedings.' " *United States v. Marcus*, 560 U.S. 258, 262, 130 S.Ct. 2159, 176 L.Ed.2d 1012 (2010) (quoting *Puckett v. United States*, 556 U.S. 129, 135, 129 S.Ct. 1423, 173 L.Ed.2d 266 (2009)).

In *New York Telephone*, the district court had issued an order authorizing federal agents to install pen registers in two telephones and directed the New York Telephone Company to furnish "all information, facilities and technical assistance" necessary to accomplish the installation. *N.Y. Tel. Co.*, 434 U.S. at 161, 98 S.Ct. 364. The Company argued that neither Fed. R. Crim. P. 41 nor the All Writs Act "provided any basis for such an order." *Id.* at 163, 98 S.Ct. 364. The Supreme

Court, however, found that this order was "clearly authorized by the All Writs Act" as a necessary and appropriate means of effectuating ***246** the installation of the pen registers. *Id.* at 172, 98 S.Ct. 364.

[11] Here, the Magistrate Judge issued a search warrant for the devices seized at Doe's residence. When law enforcement could not decrypt the contents of those devices, and Doe refused to comply, the Magistrate Judge issued the Decryption Order pursuant to the All Writs Act. The Decryption Order required Doe to "assist the Government in the execution of the ... search warrant" by producing his devices in "a fully unencrypted state." As was the case in *New York Telephone*, the Decryption Order here was a necessary and appropriate means of effectuating the original search warrant.

[12] Doe asserts that *New York Telephone* should not apply because the All Writs Act order in that case compelled a third party to assist in the execution of that warrant, and not the target of the government investigation. The Supreme Court explained, however, that the Act extends to anyone "in a position to frustrate the implementation of a court order or the proper administration of justice" as long as there are "appropriate circumstances" for doing so. *Id.* at 174, 98 S.Ct. 364. Here, as in *New York Telephone*: (1) Doe is not "far removed from the underlying controversy;" (2) "compliance with [the Decryption Order] require[s] minimal effort;" and (3) "without [Doe's] assistance there is no conceivable way in which the [search warrant] authorized by the District Court could [be] successfully accomplished." *Id.* at 174-175, 98 S.Ct. 364. Accordingly, the Magistrate Judge did not plainly err in issuing the Decryption Order.

B.

Doe also contends that the Decryption Order violates his Fifth Amendment privilege against self-incrimination and that this challenge is subject to plenary review. Doe raised a Fifth Amendment challenge in his Motion to Quash the Decryption Order. The Magistrate Judge denied that challenge, rejecting the argument that Doe's Fifth Amendment privilege would be violated. Doe did not file objections to that order, nor did he seek review by way of appeal, writ of mandamus or otherwise, despite the Quashal Denial order informing Doe that failure to file a timely objection may constitute a waiver of appellate rights. Doe also did not renew this self-incrimination claim during the contempt proceedings before the Magistrate Judge and the District Judge. [6] Instead, Doe only reasserted his Fifth Amendment claim in this appeal.

[13] While Doe persists that his challenge to the contempt order entitles him to plenary consideration of the Fifth Amendment issue, we disagree. As noted above, it is generally the case that "a contempt proceeding does not open to reconsideration the legal or factual basis of the order alleged to have been disobeyed." *Rylander*, 460 U.S. at 756, 103 S.Ct. 1548 (internal quotation marks and citation omitted).

Even if we could assess the Fifth Amendment decision of the Magistrate Judge, our review would be limited to plain error. *See United States v. Chaney*, 446 F.2d 571, 576 (3d Cir. 1971) (applying plain ***247** error review to unpreserved claim of violation of privilege against self-incrimination). Doe's arguments fail under this deferential standard of review.

[14] **[15]** The Fifth Amendment states that "[n]o person ... shall be compelled in any criminal case to be a witness against himself." U.S. CONST. amend. V. The Fifth Amendment, however, "does not independently proscribe the compelled production of every sort of incriminating evidence but applies only when the accused is compelled to make a Testimonial Communication that is incriminating." *Fisher v. United States*, 425 U.S. 391, 408, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). To be testimonial, a communication must either "explicitly or implicitly ... relate a factual assertion or disclose information." *Doe v. United States*, 487 U.S. 201, 210, 108 S.Ct. 2341, 101 L.Ed.2d 184 (1988).

[16] The Supreme Court has recognized that in some instances, the production of evidence can implicate the Fifth Amendment. In *Fisher*, the Court stated that "[t]he act of producing evidence in response to a subpoena ... has communicative aspects of its own, wholly aside from the contents of the papers produced." 425 U.S. at 410, 96 S.Ct. 1569. The Court reasoned that compliance with a request for evidence may "tacitly concede[ ] the existence of the documents demanded and their possession and control by the [defendant]." *Id.* By "producing documents, one acknowledges that the documents exist, admits that the documents are in one's custody, and concedes that the documents are those that the [Government] requests."

United States v. Chabot, 793 F.3d 338, 342 (3d Cir.), *cert. denied*, —— U.S. ——, 136 S.Ct. 559, 193 L.Ed.2d 430 (2015). When the production of evidence does concede the existence, custody, and authenticity of that evidence, the Fifth Amendment privilege against self-incrimination applies because that production constitutes compelled testimony.

[17] **[18]** In *Fisher*, however, the Court also articulated the "foregone conclusion" rule, which acts as an exception to the otherwise applicable act-of-production doctrine. *Fisher*, 425 U.S. at 411, 96 S.Ct. 1569. Under this rule, the Fifth Amendment does not protect an act of production when any potentially testimonial component of the act of production—such as the existence, custody, and authenticity of evidence—is a "foregone conclusion" that "adds little or nothing to the sum total of the Government's information." *Id.* For the rule to apply, the Government must be able to "describe with reasonable particularity" the documents or evidence it seeks to compel. *U.S. v. Hubbell*, 530 U.S. 27, 30, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000).

Although we have not confronted the Fifth Amendment implications of compelled decryption, the Eleventh Circuit has addressed the issue and found that the privilege against self-incrimination should apply. In that case, a suspect appealed a judgment of contempt entered after he refused to produce the unencrypted contents of his laptop and hard drives. *In re Grand Jury Subpoena Duces Tecum Dated Mar. 25, 2011*, 670 F.3d 1335, 1337 (11th Cir. 2012). The court found that "(1) [the suspect's] decryption and production of the contents of the drives would be testimonial, not merely a physical act; and (2) the explicit and implicit factual communications associated with the decryption and production are not foregone conclusions." *Id.* at 1346. The court reached this decision after noting that the Government did not show whether any files existed on the hard drives and could not show with any reasonable particularity that the suspect could access the encrypted portions of the drives. *Id.* Although the court did not require the Government to identify exactly ***248** the documents it sought, it did require that, at the very least, the Government be able to demonstrate some knowledge that files do exist on the encrypted devices. *Id.* at 1348–49.

Despite Doe's argument to the contrary, the Eleventh Circuit's reasoning in *In re Grand Jury Subpoena* does not compel a similar result here. In the Quashal Denial, the Magistrate Judge found that, though the Fifth Amendment may be implicated by Doe's decryption of the devices, any testimonial aspects of that production were a foregone conclusion. According to the Magistrate Judge, the affidavit supporting the application for the search warrant established that (1) the Government had custody of the devices; (2) prior to the seizure, Doe possessed, accessed, and owned all devices; and (3) there are images on the electronic devices that constitute child pornography. Thus, the Magistrate Judge concluded that the Decryption Order did not violate Doe's Fifth Amendment privilege against self-incrimination.

[19] Unlike *In re Grand Jury Subpoena*, the Government has provided evidence to show both that files exist on the encrypted portions of the devices and that Doe can access them. The affidavit supporting the search warrant states that an investigation led to the identification of Doe as a user of an internet file sharing network that was used to access child pornography. When executing a search of Doe's residence, forensic analysts found the encrypted devices, and Doe does not dispute their existence or his ownership of them. Once the analysts accessed Doe's Mac Pro Computer, they found one image depicting a pubescent girl in a sexually suggestive position and logs that suggested the user had visited groups with titles common in child exploitation. Doe's sister then reported that she had witnessed Doe unlock his Mac Pro while connected to the hard drives to show her hundreds of pictures and videos of child pornography. Forensic analysts also found an additional 2,015 videos and photographs in an encrypted application on Doe's phone, which Doe had opened for the police by entering a password. Based on these facts, the Magistrate Judge found that, for the purposes of the Fifth Amendment, any testimonial component of the production of decrypted devices added little or nothing to the information already obtained by the Government. The Magistrate Judge determined that any testimonial component would be a foregone conclusion. The Magistrate Judge did not commit a clear or obvious error in his application of the foregone conclusion doctrine. In this regard, the Magistrate Judge rested his decision rejecting the Fifth Amendment challenge on factual findings that are amply supported by the record. [7] Accordingly, Doe's challenges to the Decryption Order and Quashal Denial fail.

***249** **[20]** **[21]** So, too, does Doe's challenge to the contempt order. At the hearing on the contempt motion, Doe maintained that he could not remember the passwords to decrypt the hard drives. In a civil contempt proceeding, when a defendant raises a challenge of impossibility of compliance, "the defendant bears the burden of production." *United States v. Rylander*, 460 U.S. 752, 757, 103 S.Ct. 1548, 75 L.Ed.2d 521 (1983). At the contempt hearing, the Government presented several witnesses to support its prima facie case of contempt. Doe's sister testified to the fact that, while in her presence, Doe accessed child pornography files on his Mac Pro computer by means of entering passwords from memory. Further, a detective who executed the original search warrant stated that Doe did not provide his password at the time because he wanted to prevent the police from accessing his computer. Doe never asserted an inability to remember the passwords at that time. Doe presented no evidence to explain his failure to comply or to challenge the evidence brought by the Government. The District Court thus found Doe in contempt and ordered he be held in custody until he complies with the Decryption Order. The District Court did not abuse its discretion in finding Doe to be in contempt of the Decryption Order.

IV.

For the foregoing reasons, we will affirm the District Court's order of September 30, 2015 holding Appellant John Doe in civil contempt.

All Citations

851 F.3d 238

Footnotes

1 Encryption technology allows a person to transform plain, understandable information into unreadable letters, numbers, or symbols using a fixed formula or process. Only those who possess a corresponding "key" can return the information into its original form, *i.e.* decrypt that information. Encrypted information remains on the device in which it is stored, but exists only in its transformed, unintelligible format. Although encryption may be used to hide illegal material, it also assists individuals and businesses in lawfully safeguarding the privacy and security of information. Many new devices include encryption tools as standard features, and many federal and state laws either require or encourage encryption to protect sensitive information.

2 According to the affidavit submitted in support of the federal Government's search warrant application, "cp" stands for "child pornography" and "pthc" stands for "pre-teen hard core." (App. 39.)

3 A "hash" is "[a] mathematical algorithm that calculates a unique value for a given set of data, similar to a digital fingerprint, representing the binary content of the data to assist in subsequently ensuring that data has not been modified." *The Sedona Conference Glossary for E-Discovery and Digital Information Management* 21 (Cheryl B. Harris, et al. eds., 4th ed. 2014). Hash values are commonly used in child pornography investigations. *See, e.g.*, *United States v. Ross*, 837 F.3d 85, 87 (1st Cir. 2016), *United States v. Ackerman*, 831 F.3d 1292, 1294 (10th Cir. 2016); *United States v. Thomas*, 788 F.3d 345, 348 n. 5 (2nd Cir. 2015); *United States v. Brown*, 701 F.3d 120, 122 (4th Cir. 2012); *United States v. Cunningham*, 694 F.3d 372, 376 (3d Cir. 2012); *United States v. Cartier*, 543 F.3d 442, 444-45 (8th Cir. 2008).

4 Doe does not dispute the validity of the underlying search warrant issued by a Magistrate Judge under Fed. R. Crim. P. 41.

5 There are, of course, instances when a contempt proceeding may be the only avenue for challenging the underlying order to produce information. For example, judicial review of a grand jury subpoena may be obtained only by refusal to comply with the subpoena, with the validity of the subpoena being litigated in the ensuing contempt proceeding. *See, e.g.*, *United States v. Ryan*, 402 U.S. 530, 532-33, 91 S.Ct. 1580, 29 L.Ed.2d 85 (1971) ("[W]e have consistently held that the necessity for expedition in the administration of the criminal law justifies putting one who seeks to resist the production [to a grand jury] of desired information

to a choice between compliance with a trial court's order to produce prior to any review of that order, and resistance to that order with the concomitant possibility of an adjudication of contempt if his claims are rejected on appeal."); *In re Grand Jury Subpoena*, 709 F.3d 1027, 1029 (10th Cir. 2013) ("A protesting [grand jury] witness may seek appellate review only after he refuses to obey the subpoena and is held in contempt.").

6 In its Order explaining the contempt ruling, the District Judge observed that Doe had failed to object to the Magistrate Judge's determination that Doe's Fifth Amendment rights were not violated by the Decryption Order despite being warned that such failure "may constitute a waiver of appellate rights." (App. at 15) (citing *United States v. Polishan*, 336 F.3d 234, 240 (3d Cir. 2003).) Thus, the District Court did not address the Fifth Amendment issue.

7 It is important to note that we are not concluding that the Government's knowledge of the content of the devices is necessarily the correct focus of the "foregone conclusion" inquiry in the context of a compelled decryption order. Instead, a very sound argument can be made that the foregone conclusion doctrine properly focuses on whether the Government already knows the testimony that is implicit in the act of production. In this case, the fact known to the government that is implicit in the act of providing the password for the devices is "I, John Doe, know the password for these devices." Based upon the testimony presented at the contempt proceeding, that fact is a foregone conclusion. However, because our review is limited to plain error, and no plain error was committed by the District Court in finding that the Government established that the contents of the encrypted hard drives are known to it, we need not decide here that the inquiry can be limited to the question of whether Doe's knowledge of the password itself is sufficient to support application of the foregone conclusion doctrine.

End of Document

No. 12-240-cr
United States Court of Appeals, Second Circuit.

United States v. Ganias

824 F.3d 199 (2d Cir. 2016)
Decided May 27, 2016

No. 12-240-cr August Term 2015

05-27-2016

United States of America, Appellee, v. Stavros M. Ganias, Defendant–Appellant.

Sandra S. Glover (Sarala V. Nagala, Anastasia Enos King, Jonathan N. Francis, Assistant United States Attorneys; Wendy R. Waldron, Senior Counsel, U.S. Dep't of Justice, on the brief), for Deirdre M. Daly, United States Attorney for the District of Connecticut, for Appellee United States of America. Stanley A. Twardy, Jr., Day Pitney LLP, Stamford, CT (Daniel E. Wenner, John W. Cerreta, Day Pitney LLP, Hartford, CT, on the brief), for Defendant–Appellant Stavros Ganias. (Counsel for amici curiae are listed in Appendix A.)

Debra Ann Livingston and Gerard E. Lynch, Circuit Judges

Sandra S. Glover (Sarala V. Nagala, Anastasia Enos King, Jonathan N. Francis, Assistant United States Attorneys; Wendy R. Waldron, Senior Counsel, U.S. Dep't of Justice, on the brief), for Deirdre M. Daly, United States Attorney for the District of Connecticut, for Appellee United States of America.

Stanley A. Twardy, Jr., Day Pitney LLP, Stamford, CT (Daniel E. Wenner, John W. Cerreta, Day Pitney LLP, Hartford, CT, on the brief), for Defendant–Appellant Stavros Ganias.

(Counsel for amici curiae are listed in Appendix A.)

Before: Katzmann, Chief Circuit Judge, Jacobs, Cabranes, Pooler, Raggi, Wesley, Hall, Livingston, Lynch, Chin, Lohier, Carney, and Droney, Circuit Judges.

Livingston and Lynch, JJ., filed the majority opinion in which Katzmann, C.J., Jacobs, Cabranes, Raggi, Wesley, Hall, Carney, and Droney, JJ., joined in full, and Pooler and Lohier, JJ., joined in full as to Parts I and III and in part as to Part II.

Lohier, J., filed a concurring opinion in which Pooler, J., joined.

Chin, J., filed a dissenting opinion.

Debra Ann Livingston and Gerard E. Lynch, Circuit Judges:

Defendant-Appellant Stavros Ganias appeals from a judgment of the United States District Court for the District of Connecticut (Thompson, *J.*) convicting him, after a jury trial, of two counts of tax evasion in violation of 26 U.S.C. § 7201. He challenges his conviction on the ground that the Government violated his Fourth Amendment rights when, after lawfully copying three of his hard drives for off-site review pursuant to a 2003 search warrant, it retained these full forensic copies (or "mirrors"), which included data both responsive

and non-responsive to the 2003 warrant, while its investigation continued, and ultimately searched the non-responsive data pursuant to a second warrant in 2006. Ganias contends that the Government had successfully sorted the data on the mirrors responsive to the 2003 warrant from the non-responsive data by January 2005, and that the retention of the mirrors thereafter (and, by extension, the 2006 search, which would not have been possible but for that retention) violated the Fourth Amendment. He argues that evidence obtained in executing the 2006 search warrant should therefore have been suppressed.

We conclude that the Government relied in good faith on the 2006 warrant, and that this reliance was objectively reasonable. Accordingly, we need not decide whether retention of the forensic mirrors violated the Fourth Amendment, and we AFFIRM the judgment of the district court.

201 **I** *201 **A. Background** [1]

[1] These facts are drawn from the district court decision denying Ganias's motion to suppress and from testimony at the suppression hearing and at Ganias's jury trial. With few exceptions noted herein, the facts in this case are not in dispute.

In August 2003, agents of the U.S. Army Criminal Investigation Division ("Army CID") received an anonymous tip that Industrial Property Management ("IPM"), a company providing security for and otherwise maintaining a government-owned property in Stratford, Connecticut, pursuant to an Army contract, had engaged in misconduct in connection with that work. In particular, the informant alleged that IPM, owned by James McCarthy, had billed the Army for work that IPM employees had done for one of McCarthy's other businesses, American Boiler, Inc. ("AB"), and for construction work performed for IPM's operations manager at his home residence. The informant told the agents, including Special Agent Michael Conner, that IPM and AB's financial books were maintained by Stavros Ganias, a former Internal Revenue Service ("IRS") agent, who conducted business as Taxes International. On the basis of the informant's information, as well as extensive additional corroboration, Agent Conner prepared an affidavit seeking three warrants to search the offices of IPM, AB, and Taxes International for evidence of criminal activity.[2] Nothing in the record suggests that Ganias himself was suspected of any crimes at that time.

[2] Specifically, Agent Conner sought evidence relating to violations of 18 U.S.C. § 287 (making false claims) and § 641 (stealing government property).

In a warrant dated November 17, 2003, U.S. Magistrate Judge William I. Garfinkel authorized the search of Taxes International. The warrant authorized agents to seize, *inter alia* , "[a]ll books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and [AB]." J.A. 433. It further authorized seizure of "[a]ny of the items described [in the warrant] ... which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including ... fixed hard disks, or removable hard disk cartridges, software or memory in any form." *Id.* The warrant also specifically authorized a number of digital search protocols, though it did not state that *only* these protocols
202 were permitted.[3] The warrant authorized seizure of all hardware relevant to the alleged crimes.[4] *202 On November 19, 2003, Army CID agents executed the search warrants. Because the warrants authorized the seizure of computer hardware and software, in addition to paper documents, Agent Conner sought the help, in executing the warrants, of agents from the Army CID's Computer Crimes Investigation Unit ("CCIU"), a unit with specialized expertise in digital forensics and imaging. At Ganias's office, the CCIU agents—and in

particular Special Agent David Shaver—located three computers. Rather than take the physical hard drives, which would have significantly impaired Ganias's ability to conduct his business, Agent Shaver created mirror images: exact copies of all of the data stored thereon, down to the bit.[5] Ganias was present at his office during the creation of the mirrors, spoke with the agents, and was aware that mirrored copies of his three hard drives had been created and taken off-site.[6] There is no dispute that the forensic mirrors taken from Ganias's office contained all of the computerized data maintained by Ganias's business, including not only material related to IPM or AB, but also Ganias's own personal *203 financial records, and the records of "many other" accounting clients of Ganias: businesses of various sorts having no connection to the Government's criminal investigation.[7] J.A. 464, ¶ 14.

203

3 The warrant specified as follows:

> The search procedure of the electronic data contained in computer operating software or memory devices may include the following techniques:
>
> (a) surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
>
> (b) "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;
>
> (c) "scanning" storage areas to discover and possibly recover recently deleted files;
>
> (d) "scanning" storage areas for deliberately hidden files; or
>
> (e) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

J.A. 433-34.

4 In his attached affidavit, Agent Conner offered three reasons why it was necessary for the agents to take entire hard drives off-site for subsequent search rather than search the hard drives on-site: First, he stated that computer searches had to be conducted by computer forensics experts, who "us[ed] ... investigative techniques" to both "protect the integrity of the evidence ... [and] detect hidden, disguised, erased, compressed, password protected, or encrypted files." J.A. 448-49. Because of "[t]he vast array" of software and hardware available, it would not always be possible "to know before a search which expert is qualified to analyze the [particular] system and its data." J.A. 450. Thus, the appropriate experts could not be expected, in all cases, to accompany agents to the relevant site to be searched. Second, Agent Conner affirmed that such searches often must occur in "a laboratory or other controlled environment" given the sensitivity of the digital storage media. J.A. 449-50. And third, he stated that "[t]he search process can take weeks or months, depending on the particulars of the hard drive to be searched." J.A. 449. The district court found, in denying Ganias's motion to suppress, that, as a result of technological limitations in 2003 and the complexities of searching

digital data, "[a] full [on-site] search would have taken months to complete." *United States v. Ganias* , No. 3:08CR00224, 2011 WL 2532396, at *2 D. Conn. June 24, 2011.

[5] Hard drives are storage media comprising numerous bits—units of data that may be expressed as ones or zeros. Mirroring involves using a commercially available digital software (in the present case, though not always, EnCase) to obtain a perfect, forensic replica of the sequence of ones and zeros written onto the original hard drive. During the mirroring, EnCase acquires metadata about the mirroring process, writing an unalterable record of who creates the copy and when the copy is created. It also assigns the mirror a "hash value"—a unique code that can be used to verify whether, upon subsequent examination of the mirror at any later date, even a single one or zero has been altered from the original reproduction.

[6] Testifying at the suppression hearing, Agent Conner explained that the decision to take mirrors, rather than the hard drives themselves, reflected a desire to mitigate the burden on Ganias and his business. *See* J.A. 140-41. The district court credited this testimony, concluding that the agents "used a means less intrusive to the individual whose possessions were seized than other means they were authorized to use." *Ganias* , 2011 WL 2532396, at *8. The district court, further, explicitly found that the 2003 warrant authorized the Government to take these mirrors, *id.* at *10, a position Ganias has not challenged on appeal, and that runs directly counter to the dissent's seeming suggestions that the Government somehow acted improperly when it mirrored Ganias's hard drives or that this initial seizure went beyond the scope of the 2003 warrant, *see, e.g.* , Dissent at 227 (noting that "although the Government had a warrant for documents relating to only two of defendant-appellant Stavros Ganias's accounting clients, it seized *all* the data from three of his computers"); *id.* at 227 (stating that "the Government ... entered Ganias's premises with a warrant to seize certain papers and indiscriminately seized—and *retained* —all papers instead").

[7] Ganias claimed before the district court that when he expressed some concern about the scope of the data being seized, an agent assured him that the agents were only looking for files related to AB and IPM, and that irrelevant files "would be purged once they completed their search" for such files. J.A. 428. The district court made no finding to this effect, however. It is undisputed, moreover, that Ganias became aware in February 2006 that the Government retained the mirrors and sought to search them in connection with Ganias's own tax reporting. At no time thereafter did Ganias seek return of the mirrors pursuant to Federal Rule of Criminal Procedure 41(g) or otherwise contact a case agent to seek their return or destruction.

The next day, Agent Shaver consolidated the eleven mirrored hard drives from all three searches (including the three from Ganias's office) onto a single external hard drive which he provided to Agent Conner. Agent Conner, in turn, provided this hard drive to the evidence custodian of the Army CID, who stored it at Fort Devens, Massachusetts. There the consolidated drive remained, unaltered and untouched, throughout the events relevant to this case. Around the same time, Agent Shaver created two additional copies of the mirrored drives on two sets of nineteen DVDs. After providing these DVD sets to Agent Conner, Agent Shaver then purged the external hard drives onto which he had originally written the mirrors. At this point, a week after the search, three complete copies of the mirrors of Ganias's hard drives existed: an untouched copy stowed away in an evidence locker and two copies available for forensic analysis.[8]

[8] These copies were identical digital replicas of Ganias's hard drives as mirrored on November 19, 2003. Notably, the original hard drives in Ganias's computers had already been significantly altered since the Government mirrored them. Ganias explains in his brief before this Court that "[t]wo days after the execution of the November 2003 warrant, [he]

reviewed his personal QuickBooks file and.... *corrected over 90 errors in earlier journal entries* ." Appellant Br. at 15 n.7 (emphasis added).

Though internal protocols required that specialized digital forensic analysts search the mirrored hard drives, the paper files were not subject to such limitations. Thus, shortly after the November 19 seizure, the Army CID agents began to analyze the non-digital files seized pursuant to the warrant. These files suggested that IPM had made payments to a third company whose owner, according to the Connecticut Department of Labor, was a full-time employee of an insurance company who received no wages from any source other than that insurance company. This and other red flags spurred Agent Conner to contact the Criminal Investigation Division of the IRS, which subsequently joined the investigation.

In early February 2004, as he and his fellow agents continued to follow leads from the paper files, Agent Conner sent one of the two DVD sets containing the forensic mirrors to the Army Criminal Investigation Laboratory ("ACIL") in Forest Park, Georgia, accompanied by a copy of one of the three search warrants. In early June, the ACIL assigned Gregory Norman, a digital evidence examiner, to perform a forensic analysis. Around the same time, Special Agent Michelle Chowaniec, who replaced Agent Conner as the primary case agent for the Army CID in late March, provided the second set of DVDs to the IRS agent assigned to the case, Special Agent Paul Holowczyk. Agent Holowczyk in turn, passed it on, by way of intermediaries, to Special
204 Agent Vita Paukstelis, a computer investigative specialist. *204 By the end of June 2004, computer experts for the Army CID and the IRS—Norman and Agent Paukstelis, respectively—had received copies of the digital evidence (which, as the district court found, were "encoded so that only agents with forensic software not directly available to the case agents could view [them]," *Ganias* , 2011 WL 2532396, at *7), and forensic examination began.

Norman commenced his analysis in late June by loading the eleven mirrored drives into EnCase—the same software with which Agent Shaver initially created the mirrors—so that he could search the data thereon. After looking at the search warrants, he created a number of keywords, with which he searched for potentially relevant data. Initially, the search returned far too many results for practicable review (more than 17,000 hits); thus, Norman requested new keywords from Agent Chowaniec. On the basis of these new keywords, he was able to narrow his search and ultimately identify several files he thought might be of interest to the investigation, all of which he put on a single CD.[9] Some of these files he was able personally to examine, to determine whether they were responsive to the warrant; a few (including the QuickBooks file labeled "Steve_ga.qbw," which was ultimately searched pursuant to the 2006 warrant, J.A. 467) Norman could not open without a specific software edition of QuickBooks to which he did not have immediate access. However, as these files (like the others) contained keywords that were taken from the narrower list and generated on the basis of the warrant, Norman included the QuickBooks files in the CD he ultimately sent to Agent Chowaniec along with a report.[10] On July 23, 2004, Chowaniec received this CD. Norman, in turn, returned the nineteen DVDs to Army CID's evidence custodian in Boston for safekeeping.

9 The rest of the data remained on the DVDs, where agents would not be able to access it without specific forensic software. *See Ganias* , 2011 WL 2532396, at *7.

10 Norman describes the storage device he sent to Chowaniec as a "DVD," J.A. 218; the district court described it as a "CD," *Ganias* , 2011 WL 2532396, at *4. The distinction is immaterial.

Norman's counterpart in the IRS, Agent Paukstelis—who, in addition to receiving the search warrant with her set of DVDs, also received a list of companies, addresses, and key individuals relating to the investigation, along with "a handwritten notation next to the name 'Taxes International' that stated '(return preparer) do not search,' " *Ganias* , 2011 WL 2532396, at *3 —conducted her analysis over a period of about four months. Because she worked for the IRS, she limited her search to the three mirrored drives from Taxes International. Though Agent Paukstelis used ILook, a different software program, to review the mirrored hard drives, she too could not open QuickBooks files without the relevant proprietary software. Still, though she could not open these files, she believed, based on the information to which she had access, that they were within the scope of the warrant; thus, in October 2004, she copied this data, in concert with other responsive data, onto a CD, three copies of which she sent to Agent Holowczyk and Special Agent Amy Hosney, also with the IRS. In light of the note she had received with her DVD set as well as the list of relevant entities, Agent Paukstelis avoided, to the degree she could, searching any files of Taxes International that did not appear to be directly relevant to that list. On November 30, 2004, Paukstelis also provided a "restoration" of the mirrors of the Taxes International
205 hard drives to Special Agent *205 George Francischelli, an IRS computer specialist assigned to the case.[11]

[11] A "restoration" is a software interface that enables a user (potentially a jury) to view data on a mirror as such data would have appeared to a person accessing the data on the original storage device at the time the mirror was created. *Ganias* , 2011 WL 2532396, at *4.

Agents Chowaniec and Conner, after receiving Norman's CD and report in late July, conducted initial reviews of the data. Like Norman and Agent Paukstelis, however, they could not open the QuickBooks files. At the same time, the agents were busy, in the words of Agent Chowaniec, "tracking down other leads [,] ... [issuing] grand jury subpoenas, ... doing interviews of subcontractors and identifying subcontractors from the papers that [the agents had] received from the search warrants." J.A. 294-95. In October, Agents Hosney and Chowaniec attempted, together, to review the QuickBooks files, but again lacked the relevant software to do so. Finally, in November 2004, Agent Chowaniec, having acquired the appropriate software, opened two IPM QuickBooks files on her office computer, and then in December, Agents Hosney and Chowaniec, using the restoration provided by Agent Paukstelis, looked at additional IPM QuickBooks files. Though they had the entirety of the mirrored data before them (the only time throughout the investigation that the case agents had direct access to a software interface permitting them to view essentially all of the data stored on the mirrors), they carefully limited their search: Agent Hosney testified that they "only looked at the QuickBooks files for Industrial Property Management and American Boiler ... [b]ecause those were the only two companies named in the search warrant attachment." J.A. 340. They did, however, observe that other files existed—both on the CD Norman had provided and on the restoration—in particular, the files Agent Hosney ultimately searched in 2006.

Ganias contends that there is no dispute that by this point, the agents had finished "identifying and segregating the files within the November 2003 warrant's scope." Appellant Reply Br. at 5. In actuality, the record is unclear as to whether the forensic examination of the mirrored computers pursuant to the initial search warrant had indeed concluded as a forward-looking matter, rather than from the perspective of hindsight.[12] The district court did not find any facts decisive to this question. It is, further, undisputed that the investigation into McCarthy, IPM, and AB was ongoing at this time, and that this investigation would culminate in an indictment
206 of McCarthy in 2008 secured in large part *206 through reliance on evidence responsive to the 2003 warrant and located on the mirrored copies of Ganias's hard drives. *See* Indictment, *United States v. McCarthy* , No. 3:08cr224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 1. When asked why, at this time or any time later, Agent

Conner did not return or destroy the data stored on the mirrors that did not appear directly to relate to the crimes alleged in the warrant, Agent Conner explained that "[the] investigation was still ... open" and that, generally, items would be "released back to the owner" once an investigation was closed. J.A. 123. He further noted that the Army CID "would not routinely go into DVDs to delete data, as we're altering the original data that was seized." J.A. 122.[13]

12 At the suppression hearing, Agent Chowaniec testified, in response to the question whether "as of mid-December, [her] forensic analysis was completed": "That's correct, of the computers." J.A. 322. But when asked later, "[D]id you know [in December 2004] you wouldn't need to look at any information that had been provided by Greg Norman on that CD anymore in the course of this investigation," Agent Chowaniec responded, "No," and when further asked, "Did you know you wouldn't require further analysis by Greg Norman or any other examiner at the Army lab in Georgia after December of 2004," Agent Chowaniec again responded, "No." J.A. 324. Agent Conner similarly answered with uncertainty when asked a related question. *See* J.A. 145 ("I didn't know the entire universe of information that was contained within the DVDs that were sent to [Norman] for analysis. I knew only what he sent back to me saying this is what I found off your keyword search."). The dissent disputes our conclusion that the record was unclear on this point, arguing, through citation to Agent Chowaniec's testimony, that "the record ... shows otherwise." Dissent at 233. The district court found no facts on this issue, and the record, as demonstrated above, is indeed unclear.

13 Agent Conner's explanation for why the Government did not, as a matter of policy in this or other cases, delete mirrored drives or otherwise require segregation or deletion of non-responsive data, is not a model of clarity: in addition to citing concerns of evidentiary integrity and suggesting a policy of non-deletion or return prior to the end of an investigation, he noted that "you never know what data you may need in the future," J.A. 122, and at one point referred to the DVDs as "the government's property, not Mr. Ganias'[s] property," J.A. 146. The dissent seizes on this single sentence during Agent Conner's cross-examination as the smoking gun of the Government's bad faith, citing it on no fewer than four occasions. *See* Dissent at 227, 229, 238, 240. The district court, however, did not find facts explicating Agent Conner's testimony or placing it within the context of the explanations that he and other agents offered for retention of the mirrors. The court did note in its legal analysis that "[a] copy of the evidence was preserved in the form in which it was taken." *Ganias* , 2011 WL 2532396, at *8. Further, the Government on appeal provides numerous rationales—many echoing those articulated by Agent Conner *throughout* his testimony—for why retention of a forensic mirror may be necessary during the pendency of an investigation, none of which amounts to the argument that the mirror is simply "government [ ] property."

Over the next year, the agents continued to investigate IPM and AB. Analysis of the paper files taken pursuant to the November 2003 search warrant revealed potential errors in AB's tax returns that seemed to omit income reflected in checks deposited into IPM's account. Aware that Ganias had prepared these tax returns and deposited the majority of these checks, Agent Hosney came to suspect that Ganias was engaged in tax-related crimes.[14] She did not, however, return to the restoration or otherwise open any of Ganias's digital financial
207 documents or files associated with *207 Taxes International.[15] Instead, Agent Hosney subpoenaed Ganias's bank records from 1999 to 2003 and accessed his income tax returns for the same period. On July 28, 2005, the IRS —believing Ganias to be involved both personally and as an accomplice or co-conspirator in tax evasion— officially expanded the investigation to include him.

14 The dissent suggests that "[w]hat began nearly thirteen years ago as an investigation by the Army into two of Ganias's business clients *somehow* evolved into an unrelated investigation by the IRS into Ganias's personal affairs, largely because" the Government retained the mirrored copies of Ganias's hard drives. Dissent at 241 (emphasis added). In fact, Agent Hosney's affidavit in support of the 2006 warrant explains that the Government suspected Ganias of

underreporting his income because of evidence that Ganias had assisted McCarthy in underreporting income from *McCarthy's* companies—evidence which led to an indictment of *both* McCarthy and Ganias for conspiracy to commit tax fraud. Further, when Agent Hosney developed this suspicion—which was hardly "unrelated" to the initial investigation—she did not turn to the mirrors, but instead engaged in old-fashioned investigatory work, "examin[ing Ganias's tax returns] more closely to determine if his own income was underreported." J.A. 465, ¶ 18. She then reviewed deposits in his bank account, cross-referenced bank records and tax returns, and finally presented this evidence in a proffer session to Ganias—all without once looking at any non-responsive information on the mirrors. Only after she had acquired independent probable cause—and only after extensive evidence suggested Ganias may have committed a crime—did Agent Hosney seek a second warrant to search the mirrors. It is, in short, no mystery how the investigation of McCarthy, IPM, and AB came to include Ganias, and, further, an inaccurate statement of the record to suggest that this "evolution" had anything to do with the retention of the mirrors.

15 Agent Hosney explained in her testimony: "[W]e couldn't look at that file because it wasn't—Steve Ganias and Taxes International were not listed on the original Attachment B, items to be seized." J.A. 348.

On February 14, 2006, Ganias, accompanied by his lawyer, met in a proffer session with Agent Hosney and others involved in the investigation.[16] That day or shortly thereafter, Agent Hosney asked Ganias for consent to access his personal QuickBooks files and those of his business, Taxes International—data Agent Hosney knew to be present on the forensic mirrors but which she had not accessed. When, by April 24, 2006 (two and a half months later), Ganias had failed to respond (either by consenting, objecting, or filing a motion under Federal Rule of Criminal Procedure 41(g) for return of seized property), Agent Hosney sought a search warrant to search the mirrored drives again.[17] In her search warrant affidavit, Agent Hosney pointed to bank records, income tax forms, and additional evidence to demonstrate that she had probable cause to believe that Ganias had violated 26 U.S.C. § 7201 (by committing tax evasion) and § 7206(1) (by making false declarations).[18] She further noted that the items to be searched were "mirror images of computers seized on November 19, 2003 from the offices of Taxes International," J.A. 461, ¶ 7; that information material to the initial investigation had been located on these mirrors and that, "[d]uring th[at] investigation," such information had been "analyzed in detail," J.A. 464, ¶ 15; that Ganias was not, at the time of the initial seizure, under investigation, J.A. 461, ¶ 3 ("On July 28, 2005, the Government's investigation was expanded to include an examination of whether Ganias, McCarthy's accountant and former IRS Revenue Agent, violated the federal tax laws."); and thus that, though Agent Hosney believed that the second mirrored drive, called TaxInt_2, was "the primary computer for Taxes International," J.A. 463, ¶ 13, she could not search Ganias's personal or business files as "[p]ursuant to the 2003 search warrant, only files for [AB] and IPM could be viewed," J.A. 464, ¶ 14. The magistrate judge issued the warrant, Agent Hosney searched the referenced data, and ultimately the Government indicted Ganias for tax evasion.

16 According to Agent Hosney, in that proffer session Ganias claimed "that he failed to record income from his own business [to his QuickBook files] as a result of a computer flaw in the QuickBooks software ... [but that,] ... although he attempted to duplicate the software error, he was unable to do so." J.A. 467, ¶ 28. Agent Hosney contacted Intuit, Inc., which released QuickBooks, to determine whether such an error might have affected, generally, the pertinent version of the software, and was told that the company was aware of no such "widespread malfunction." J.A. 469, ¶ 35.

17 U.S. Magistrate Judge William I. Garfinkel, who had authorized the 2003 warrant, authorized this 2006 warrant as well. J.A. 430, 454.

18 Ganias did not contest before the district court, and does not contest on appeal, that this evidence—none of which was acquired through search of non-responsive data on the mirrors—created sufficient probable cause for the 2006 warrant.

B. Procedural History

In February 2010, Ganias moved to suppress the evidence Agent Hosney acquired pursuant to the 2006 warrant. After a two- *208 day hearing, the district court denied the motion on April 14, 2010, and issued a written decision on June 24, 2011. In that decision, the district court found, *inter alia* , that the forensic examination of the mirrored drives "was conducted within the limitations imposed by the [2003] warrant" and that "[a] copy of the evidence was preserved in the form in which it was taken." *Ganias* , 2011 WL 2532396, at *8. Judge Thompson observed that Ganias "never moved for destruction or return of the data, which could have led to the seized pertinent data being preserved by other means." *Id.* The district court concluded that the Government's retention of the mirrored drives—and thus its subsequent search of those drives pursuant to a warrant—did not violate the Fourth Amendment. Having found no Fourth Amendment violation, the district court did not reach the question of good faith. *Id.* at *9.

At trial, the Government introduced information in Ganias's QuickBooks files as evidence against him, in particular highlighting the fact that payments made to him by clients such as IPM were characterized as "owner's contributions," which prevented QuickBooks from recognizing them as income.[19] On the basis of this and other evidence, the jury convicted Ganias of two counts of tax evasion, and the district court sentenced him to two terms of 24 months' incarceration, to be served concurrently.

19 Many of these entries existed *only* on the QuickBooks files that the Government had accessed on the mirrors, as a result of Ganias's amendments to the entries on his hard drives days after the execution of the 2003 warrant. At trial, Ganias testified that his characterization of the payments as "owner's contributions" was simply a good faith mistake, and not evidence of intent to commit tax evasion, a claim that the Government labeled implausible in light of Ganias's extensive experience as an IRS agent and accountant.

Ganias appealed. On review of his conviction, a panel of this Court concluded, unanimously, that the Government had violated the Fourth Amendment; in a divided decision, the panel then ordered suppression of the evidence obtained in executing the 2006 warrant and vacated the jury verdict. We subsequently ordered this rehearing *en banc* in regards to, first, the existence of a Fourth Amendment violation and, second, the appropriateness of suppression.[20]

20 Specifically, we asked the parties to brief the following two issues:

> (1) Whether the Fourth Amendment was violated when, pursuant to a warrant, the government seized and cloned three computer hard drives containing both responsive and non-responsive files, retained the cloned hard drives for some two-and-a-half years, and then searched the nonresponsive files pursuant to a subsequently issued warrant; and
>
> (2) Considering all relevant factors, whether the government agents in this case acted reasonably and in good faith such that the files obtained from the cloned hard drives should not be suppressed.

United States v. Ganias , 791 F.3d 290 (2d Cir. 2015) (mem.).

II

"On appeal from a district court's ruling on a motion to suppress evidence, 'we review legal conclusions de novo and findings of fact for clear error.' " *United States v. Bershchansky* , 788 F.3d 102, 108 (2d Cir. 2015) (quoting *United States v. Freeman* , 735 F.3d 92, 95 (2d Cir. 2013)). We may uphold the validity of a judgment "on any ground that finds support in the record." *Headley v. Tilghman* , 53 F.3d 472, 476 (2d Cir. 1995).

The district court concluded that the conduct of the agents in this case comported fully with the Fourth
209 Amendment, and *209 thus did not reach the question whether they also acted in good faith. Because we conclude that the agents acted in good faith, we need not decide whether a Fourth Amendment violation occurred. We thus affirm the district court on an alternate ground. Nevertheless, though we offer no opinion on the existence of a Fourth Amendment violation in this case, we make some observations bearing on the reasonableness of the agents' actions, both to illustrate the complexity of the questions in this significant Fourth Amendment context and to highlight the importance of careful consideration of the technological contours of digital search and seizure for future cases.

"The touchstone of the Fourth Amendment is reasonableness...." *United States v. Miller* , 430 F.3d 93, 97 (2d Cir. 2005) (alteration omitted) (quoting *United States v. Knights* , 534 U.S. 112, 118, 122 S.Ct. 587, 151 L.Ed.2d 497 (2001)). As relevant here, "searches pursuant to a warrant will rarely require any deep inquiry into reasonableness." *United States v. Leon* , 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984) (alteration omitted) (quoting *Illinois v. Gates* , 462 U.S. 213, 267, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983) (White, J., concurring in judgment)). Nevertheless, both the scope of a seizure permitted by a warrant,[21] and the
210 reasonableness of government conduct in executing a valid warrant,[22] can present Fourth *210 Amendment issues. Ganias thus argues that the Government violated the Fourth Amendment in this case, notwithstanding the two warrants that issued, by retaining complete forensic copies of his three hard drives during the pendency of its investigation.

21 Specifically, courts have long recognized that a prohibition on "general warrants"—warrants completely lacking in particularity—was a central impetus for the ratification of the Fourth Amendment. *See, e.g.* , *Riley v. California* , —— U.S. ——, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014) (noting, in the context of evaluating the reasonableness of a warrantless search of a cell phone, that "[o]ur cases have recognized that the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity" and that "opposition to such searches was in fact one of the driving forces behind the Revolution itself"); *Marshall v. Barlow's, Inc* ., 436 U.S. 307, 311, 98 S.Ct. 1816, 56 L.Ed.2d 305 (1978) (noting, in the context of evaluating the reasonableness of warrantless inspections of business premises, that "[t]he particular offensiveness" of general warrants "was acutely felt by the merchants and businessmen whose premises and products were inspected" under them); *Stanford v. Texas* , 379 U.S. 476, 486, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965) ("[T]he Fourth ... Amendment[ ] guarantee[s] ... that no official ... shall ransack [a person's] home and seize his books and papers under the unbridled authority of a general warrant...."); *United States v. Galpin* , 720 F.3d 436, 445 (2d Cir. 2013) ("The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of "general warrants." ' " (quoting *Payton v. New York* , 445 U.S. 573, 583, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980))).

We agree with the dissent that "the precedents are absolutely clear that general warrants are unconstitutional." Dissent

at 237. To the degree that the dissent would go further, however, and find it "absolutely clear" to a reasonable government agent in 2005 that the retention of a lawfully acquired mirror during the pendency of an investigation and the subsequent search of data on that mirror pursuant to a second warrant would implicate the ban on general warrants, we respectfully disagree.

22 *See, e.g.* , *L.A. Cty. v. Rettele* , 550 U.S. 609, 614–16, 127 S.Ct. 1989, 167 L.Ed.2d 974 (2007) (applying the reasonableness standard to evaluate whether police officers' manner of executing a valid warrant violated the Fourth Amendment); *Wilson v. Layne* , 526 U.S. 603, 611, 119 S.Ct. 1692, 143 L.Ed.2d 818 (1999) ("[T]he Fourth Amendment does require that police actions in execution of a warrant be related to the objectives of the authorized intrusion...."); *Dalia v. United States* , 441 U.S. 238, 258, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979) ("[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness."); *Terebesi v. Torreso* , 764 F.3d 217, 235 (2d Cir. 2014) ("[T]he method used to execute a search warrant ... [is] as a matter of clearly established constitutional law, subject to Fourth Amendment protections...."), *cert. denied sub nom. Torresso v. Terebesi* , ——U.S. ——, 135 S.Ct. 1842, 191 L.Ed.2d 723 (2015) (mem.); *Lauro v. Charles* , 219 F.3d 202, 209 (2d Cir. 2000) ("[T]he Fourth Amendment's proscription of unreasonable searches and seizures 'not only ... prevent[s] searches and seizures that would be unreasonable if conducted at all, but also ... ensure[s] reasonableness in the manner and scope of searches and seizures that are carried out.' " (all but first alteration in original) (quoting *Ayeni v. Mottola* , 35 F.3d 680, 684 (2d Cir. 1994))).

According to Ganias, when law enforcement officers execute a warrant for a hard drive or forensic mirror that contains data that, as here, cannot feasibly be sorted into responsive and non-responsive categories on-site, "the Fourth Amendment demands, at the very least, that the officers expeditiously complete their off-site search and then promptly return (or destroy) files outside the warrant's scope."[23] Appellant Br. at 18. Arguing that a culling process took place here and that it had concluded by, at the latest, January 2005, Ganias faults the Government for retaining the mirrored drives—including storing one forensic copy in an evidence locker for safekeeping.[24] It was this retention, he argues, that constituted the Fourth Amendment violation—a violation that, in turn, made the 2006 search of the data itself unconstitutional as, but for this retention, the search could never have occurred.

23 On appeal, Ganias does not question the scope or validity of the 2003 warrant. The district court found that the 2003 warrant authorized the Government to mirror Ganias's hard drives for off-site review, *Ganias* , 2011 WL 2532396, at *10 ; that the warrant, though authorizing such seizure, was sufficiently particularized and not a "general warrant," *id.* ; that, absent mirroring for off-site review, on-site review would have taken months, *id.* at *2 ; and that mirroring thus minimized any intrusion on Ganias's business, *id.* at *8 ; *cf.* Fed. R. Crim. P. 41(e)(2)(B) (which, as amended in 2009, permits a warrant to "authorize the seizure of electronic storage media or the seizure or copying of electronically stored information," and notes that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant"); Fed. R. Crim. P. 41(e)(2)(B) advisory committee's note to 2009 amendments (explaining that, because "[c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location[, t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant"). Ganias does not contest these conclusions on appeal but contends, instead, that considerations *underlying* the prohibition on general warrants may require that, if the government lawfully mirrors an entire hard drive containing non-responsive as well as responsive information for off-site review, it may not then retain the mirror throughout the pendency of its investigation.

24 As already noted, the district court made no finding as to when or whether forensic examination of the mirrors pursuant to the 2003 warrant was completed.

To support this argument, Ganias relies principally on *United States v. Tamura* , 694 F.2d 591 (9th Cir. 1982), a Ninth Circuit case involving the search and seizure of physical records. In *Tamura* (unlike the present case, in which a warrant specifically authorized the agents to seize hard drives and to search them off-site) officers armed only with a warrant authorizing them to seize specific "records" instead seized numerous boxes of
211 printouts, file *211 drawers, and cancelled checks for off-site search and sorting. *Id.* at 594–95. After the officers had clearly sorted the responsive paper documents from the non-responsive ones, they refused—despite request—to return the non-responsive paper files. *Id.* at 596–97. The Ninth Circuit concluded that both the unauthorized seizure of voluminous material not specified in the warrant and the retention of the seized documents violated the Fourth Amendment.[25] *Id.* at 595, 597 ; *see also Andresen v. Maryland* , 427 U.S. 463, 482 n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976) ("[W]e observe that to the extent [seized] papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily and the trial judge was correct in suppressing others.... In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.... [R]esponsible officials [conducting such searches], including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy."); *cf. United States v. Matias* , 836 F.2d 744, 747 (2d Cir. 1988) ("[W]hen items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items....").

25 The Ninth Circuit declined to reverse the defendant's conviction, as no improperly seized document was admitted at trial, and as blanket suppression was not warranted. *See Tamura* , 694 F.2d at 597.

Because we resolve this case on good faith grounds, we need not decide the relevance, if any, of *Tamura* (or, more broadly, the validity of Ganias's Fourth Amendment claim). We note, however, that there are reasons to doubt whether *Tamura* (to the extent we would indeed follow it) answers the questions before us. First, on its facts, *Tamura* is distinguishable from this case, insofar as the officers there seized for off-site review records that the warrant did not authorize them to seize,[26] and retained those records even after their return was requested. Here, in contrast, the warrant authorized the seizure of the hard drives, not merely particular records, and Ganias did not request return or destruction of the mirrors (even after he was indisputably alerted to the Government's continued retention of them) by, for instance, filing a motion for such return pursuant to Federal Rule of Criminal Procedure 41(g). Second, and more broadly, even if the facts of *Tamura* were otherwise on point, Ganias's invocation of *Tamura* 's reasoning rests on an analogy between paper files intermingled in a file cabinet and digital data on a hard drive. Though we do not take any position on the ultimate disposition of the constitutional questions herein, we nevertheless pause to address the appropriateness of this analogy, which is often invoked (including by the dissent) and bears examination.

26 The fact that the officers in *Tamura* lacked a warrant for the initial seizure was not incidental to the decision: the *Tamura* court explicitly found that it was the lack of a warrant that made the initial seizure—even if otherwise understandable in light of the voluminous material to be reviewed—a violation of the Fourth Amendment. *See* 694 F.2d at 596.

The central premise of Ganias's reliance on *Tamura* is that the search of a digital storage medium is analogous to the search of a file cabinet. The analogy has some force, particularly as seen from the perspective of the affected computer user. Computer users—or at least, average users (in contrast to, say, digital forensics experts)
212 —typically experience computers as filing cabinets, as that is precisely how *212 user interfaces are designed to be perceived by such users.[27] Given that the file cabinet analogy (at least largely) thus captures an average person's subjective experience with a computer interface, the analogy may shed light on a user's subjective expectations of privacy regarding data maintained on a digital storage device. Because we experience digital files as discrete items, and because we navigate through a computer as through a virtual storage space, we may expect the law similarly to treat data on a storage device as comprised of distinct, severable files, even if, in fact, "[s]torage media do not naturally divide into parts." Josh Goldfoot, *The Physical Computer and the Fourth Amendment* , 16 Berkeley J. Crim. L. 112, 131 (2011). In this case, for example, a person in Ganias's situation could well understand the "files" on his hard drives containing information relating to IPM and AB as separate from the "files" containing his personal financial information and that of other clients. Indeed, the very fact that the Government sought additional search authorization via the 2006 warrant when it established probable cause to search Ganias's personal files indicates that the Government too understood—and credited—this distinction.

27 *See* Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 8-14 (2015) (contrasting "operating systems ... [which] hide the hardware resources behind abstractions to provide an environment that is more user-friendly," *id.* at 13, with machine language, assembly language, high-level languages, data structures, and algorithms); Josh Goldfoot, *The Physical Computer and the Fourth Amendment* , 16 Berkeley J. Crim. L. 112, 117 (2011) (contrasting two perspectives on digital storage media—the "internal perspective," or how "the user experiences [such media,] as parcels of information, grouped into files, or even into smaller units such as spreadsheet rows" and the "external perspective," or how the actual computer functions, in which "files are not ... 'things' at all," but "groupings of data ... inseparably tied to the storage medium," created by the computer by manipulating "chunks of physical matter [such as regions on a hard drive] whose state is altered to record information").

That said, though it may have some relevance to our inquiry, the file cabinet analogy is only that—an analogy, and an imperfect one. *Cf.* James Boyle, *The Public Domain* 107 (2008) ("Analogies are only bad when they ignore the key difference between the two things being analyzed."). Though to a user a hard drive may seem like a file cabinet, a digital forensics expert reasonably perceives the hard drive simply as a coherent physical storage medium for digital data—data that is interspersed *throughout* the medium, which itself must be
213 maintained and accessed with care, lest this data be altered or destroyed.[28] *See* *213 Goldfoot, *supra* , at 114 (arguing digital storage media are physical objects like "drugs, blood, or clothing"); Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement* , 7 U. Pitt. J. Tech. L. & Pol'y, art. 5, at 1, 30 (2007) ("[A] computer does not simply hold data, it is *composed* of data."). Even the most conventional "files"—word documents and spreadsheets such as those the Government searched in this case—are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact "fragmented" on a storage device, potentially across physical locations. Jekot, *supra* , at 13. "Because of the manner in which data is written to the hard drive, rarely will one file be stored intact in one place on a hard drive," *id* .; so-called "files" are stored in multiple locations and in multiple forms, *see* Goldfoot, *supra* , at 127-28.[29] And as a corollary to this fragmentation, the computer stores unseen information about any given "file"—not only metadata about when the file was created or who created it, *see* Michael W. Graves, *Digital Archaeology: The Art and Science of Digital Forensics* 94-95 (2014), but also prior versions or

edits that may still exist "in the document or associated temporary files on [the] disk"—further interspersing the data corresponding to that "file" across the physical storage medium, Eoghan Casey, *Digital Evidence and Computer Crime* 507 (3d ed. 2011).

28 *See* Eoghan Casey, *Digital Evidence and Computer Crime* 472, 474-96 (3d ed. 2011) (highlighting the fact that forensic examination of storage media can create tiny alterations, which necessitates care on the part of examiners in acquiring, searching, and preserving that data); *id.* at 477-78 (describing the importance of protecting digital storage media from "dirt, fluids, humidity, impact, excessive heat and cold, strong magnetic fields, and static electricity"); Michael W. Graves, *Digital Archaeology: The Art and Science of Digital Forensics* 95 (2014) ("Computer data is extremely volatile and easily deleted, and can be destroyed, either intentionally or accidentally, with a few mouse clicks."); Bill Nelson et al., *Guide to Computer Forensics and Investigations* 160 (5th ed. 2015) (emphasizing the importance of "maintain[ing] the integrity of digital evidence in the lab" by creating a read-only copy prior to analysis); Jonathan L. Moore, *Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation* , 50 Jurimetrics J. 147, 153 (2010) ("[All electronically stored information is] prone to manipulation[;] ... [such] alteration can occur intentionally or inadvertently."); Int'l Org. for Standardization & Int'l Electrotechnical Comm'n, *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence* 17 (2012) [hereinafter ISO/IEC, *Guidelines*] (emphasizing the importance of careful storage and transport techniques and noting that "[s]poliation can result from magnetic degradation, electrical degradation, heat, high or low humidity exposure, as well as shock and vibration").

29 *See* Goldfoot, *supra* ("Storage media do not naturally divide into parts," *id.* at 131; "it is difficult to agree ... on where the subcontainers begin and end," *id.* at 113.); Orin S. Kerr, *Searches and Seizures in a Digital World* , 119 Harv. L. Rev. 531, 557 (2005) ("[V]irtual files are not robust concepts. Files are contingent creations assembled by operating systems and software."); *see also* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data* , 48 Tex. Tech L. Rev. 1, 32 (2015) ("What does it mean to 'delete' data?").

"Files," in short, are not as discrete as they may appear to a user. Their interspersion throughout a digital storage medium, moreover, may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data. To be clear, we do not suggest that it is impossible to do so in any particular or in every case; we emphasize only that in assessing the reasonableness, for Fourth Amendment purposes, of the search and seizure of digital evidence, we must be attuned to the technological features unique to digital media as a whole and to those relevant in a particular case—features that simply do not exist in the context of paper files.

These features include an additional complication affecting the validity of the file cabinet analogy: namely, that a good deal of the information that a forensic examiner may seek on a digital storage device (again, because it is a coherent and complex forensic object and not a file cabinet) does not even remotely fit into the typical user's conception of a "file." *See* Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 39 (2015) ("Forensic software gives a forensic examiner access to electronically stored information (ESI) that is otherwise unavailable to a typical computer user."). Forensic investigators may, *inter alia* , search for and discover evidence that a file was
214 *214 deleted as well as evidence sufficient to reconstruct a deleted file—evidence that can exist in so-called "unallocated" space on a hard drive. *See* Casey, *supra* , at 496; Orin S. Kerr, *Searches and Seizures in a Digital World* , 119 Harv. L. Rev. 531, 542, 545 (2005) ; Fed. Judicial Ctr., *supra* , at 40 ("A host of information can lie in the interstices between the allocated spaces."). They may seek responsive metadata about a user's activities, or the manner in which information has been stored, to show such things as knowledge or intent, or to create

timelines as to when information was created or accessed.[30] Forensic examiners will sometimes seek evidence on a storage medium that something *did not happen* : "If a defendant claims he is innocent because a computer virus committed the crime, the absence of a virus on his hard drive is 'dog that did not bark' negative evidence that disproves his story.... To prove something is not on a hard drive, it is necessary to look at every place on the drive where it might be found and confirm it is not there."[31] Goldfoot, *supra* , at 141; *see also United States v. O'Keefe* , 461 F.3d 1338, 1341 (11th Cir. 2006) ("[The government's expert] testified that the two viruses he found on [the defendant's] computer were not capable of 'downloading and uploading child pornography and
215 sending out advertisements.' ").[32] *215 Finally, because of the complexity of the data thereon and the manner in which it is stored, the nature of digital storage presents potential challenges to parties seeking to preserve digital evidence, authenticate it at trial, and establish its integrity for a fact-finder—challenges that materially differ from those in the paper file context. First, the extraction of specific data files to some other medium can alter, omit, or even destroy portions of the information contained in the original storage medium. Preservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial. Graves, *supra* , at 95-96 ("[The investigator] must be able to prove that the information presented came from where he or she claims and was not altered in any way during examination, and that there was no opportunity for it to have been replaced or altered in the interim."); *see also* Casey, *supra* , at 480 ("Even after copying data from a computer or piece of storage media, digital investigators generally retain the original evidential item in a secure location for future reference.").[33] The preservation of data, moreover, is not simply a concern for law enforcement. Retention of the original storage medium or its mirror may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved. *See, e.g.* , *United States v. Kimoto* , 588 F.3d 464, 480 (7th Cir. 2009) (quoting the defendant's motion as stating: "Upon beginning their work, [digital analysis experts] advised [the defendant's] Counsel that the discovery provided to the defense did not appear to be a complete forensic copy, and that such was necessary to verify the data as accurate and unaltered.").[34] Defendants may also require access to a forensic copy to conduct an independent analysis of precisely what the government's forensic expert did—potentially altering evidence in a manner material to the case—or to locate
216 exculpatory evidence that the government missed.[35] *216 Notwithstanding any other distinctions between this case and *Tamura*, then, the Government plausibly argues that, because digital storage media constitute coherent forensic objects with contours more complex than—and materially distinct from—file cabinets containing interspersed paper documents, a digital storage medium or its forensic copy may need to be retained, during the course of an investigation and prosecution, to permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant; to secure metadata and other probative evidence stored in the interstices of the storage medium; and to preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained. To be clear, we do not decide the ultimate merit of this argument as applied to the circumstances of
217 this case.[36] Nor do we gainsay the *217 privacy concerns implicated when the government retains a hard drive or forensic mirror containing personal information irrelevant to the ongoing investigation, even if such information is never viewed. We discuss the aptness and limitations of Ganias's analogy and the Government's response simply to highlight the complexity of the relevant questions for future cases and to underscore the importance, in answering such questions, of engaging with the technological specifics.[37]

30 *See Fharmacy Records v. Nassar* , 379 Fed.Appx. 522, 525 (6th Cir. 2010) (describing testimony of a digital forensics expert in a copyright case that the number and physical location of a file on an Apple Macintosh—which saves files sequentially on its storage medium—demonstrated that the file had been back-dated).

31 Indeed, in this very case, as already noted, *see supra* note 16, Ganias at one point claimed that a "software error" or "computer flaw" prevented him from recording certain income in his QuickBooks files. J.A. 467, ¶ 28. Data confirming the existence, or non-existence, of an error affecting the particular installation of a program on a given digital storage device could be, in a hypothetical case, relevant to the probity of information otherwise located thereupon.

32 We note that some of these inferences may be limited to—or at least of more relevance to—traditional magnetic disk drives, which have long been the primary digital storage technology. "Generally when data is deleted from a [traditional hard disk drive], the data is retained until new data is written onto the same location. If no new data is written over the deleted data, then the forensic investigator can recover the deleted data, albeit in fragments." Alastair Nisbet et al., *A Forensic Analysis and Comparison of Solid State Drive Data Retention with TRIM Enabled File Systems* , Proceedings of the 11th Australian Digital Forensics Conference 103 (2013). In contrast, the technology used in solid state drives "requires a cell to be completely erased or zeroed-out before a further write can be committed," *id.* at 104, and in part because such erasure can be time consuming, solid state drives incorporate protocols which "zero-delete data locations ... as a matter of course," thereby "reduc[ing] the data that can be retrieved from the drive by [a] forensic investigator," *id.* at 103. *See also* Graeme B. Bell & Richard Boddington, *Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?* , 5 J. Digital Forensics, Sec. & L., no. 3, 2010, at 1, 12 (stating that, in connection with such storage devices, "evidence indicating 'no data' does not authoritatively prove that data did not exist at the time of capture"). That is not to say that studies indicate that deleted information is *never* recoverable from any model of solid state drive. *See, e.g.* , Christopher King & Timothy Vidas, *Empirical Analysis of Solid State Disk Data Retention When Used with Contemporary Operating Systems* , 8 Digital Investigation 111, 113 (2011) (citing a study suggesting that data deleted from a particular solid state drive was recoverable in certain contexts); Gabriele Bonetti et al., *A Comprehensive Black–Box Methodology for Testing the Forensic Characteristics of Solid-State Drives* , Proceedings of the 29th Annual Computer Security Applications Conference 277 (2013) (observing that, though several tested solid state drives contained no recoverable deleted data, one model contained "high[ly] recoverab[le]" quantities of such data). The point is simply that there may be material differences among different varieties of storage media that, in turn, make certain factors cited herein more or less relevant to a given inquiry.

33 We do not suggest that authentication of evidence from computerized records is impossible absent retention of an entire hard drive or mirror. Authentication is governed by Federal Rule of Evidence 901, which requires only that "the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is." Fed. R. Evid. 901(a). As we have stated, "[t]his requirement is satisfied 'if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.' " *United States v. Pluta* , 176 F.3d 43, 49 (2d Cir. 1999) (citation omitted) (quoting *United States v. Ruggiero* , 928 F.2d 1289, 1303 (2d Cir. 1991)). "[T]he burden of authentication does not require the proponent of the evidence to rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication, and hence for admissibility, is one of reasonable likelihood." *Id.* (alteration omitted) (quoting *United States. v. Holmquist* , 36 F.3d 154, 168 (1st Cir. 1994)). The weight of digital evidence admitted at trial, however, may be undermined by challenges to its integrity—challenges which proper preservation might have otherwise avoided.

34 Where, as in this case, a mirror containing responsive data has been lawfully seized from a third-party custodian, this concern cannot be avoided simply by returning the original medium to the party from whom it was seized. A third-party custodian may need to utilize a hard drive in ways that will alter the data, and will likely have no incentive to retain a mirrored copy of drives as they once existed but that are of no further use to the custodian.

35 *See Kimoto* , 588 F.3d at 480–81 ("[The defendant] argued that the failure to provide him with a complete forensic copy of all digital files impaired his ability to prepare a defense.... [The defendant] submitted that he should not be punished 'because the Government failed to properly preserve or maintain a digital forensic copy of the data.' "); Casey, *supra* , at 510-11 (discussing a case study in which, due to forensic investigators' own mistakes, discovery of digital evidence confirming a murder suspect's alibi was greatly delayed); *see also id.* at 508-510 (detailing the importance of experts reporting their processes); Fed. Judicial Ctr., *supra* , at 41 ("The forensic examiner ... generate[s] reports, detailing the protocols and processes that he or she followed.... The forensic reports must provide enough data to allow an independent third-party examiner to recreate the exact environment that yielded the report's findings and observations."); Darren R. Hayes, *A Practical Guide to Computer Forensics Investigations* 116 (2015) ("[B]ecause forensics is a science, the process by which the evidence was acquired must be repeatable, with the same results."); ISO/IEC, *Guidelines* , *supra* , at 7 (emphasizing the importance of repeatability and reproducibility).

36 That said, it is important to correct a misunderstanding in the dissent's analysis, as it pertains to these factors and their application here. The dissent suggests that the Government can have had no interest in retention, as "[t]he agents could not have been keeping non-responsive files [in order to authenticate and defend the probity of responsive files] for the purpose of proceeding against Ganias, as [in December 2004] they did not yet suspect [him] of criminal wrongdoing." Dissent at 234. This argument misunderstands the Government's position: the Government was not retaining the mirrors in late 2004 and 2005 in the hopes of proceeding against Ganias; it was retaining the mirrors as part of its ongoing investigation of James McCarthy and his two companies, AB and IPM—an investigation that would culminate in an indictment of McCarthy in 2008 secured through extensive reliance on responsive data recovered from the mirrored copies of Ganias's hard drives. The dissent's focus on Ganias, the owner of the hard drives the Government mirrored, and not McCarthy, a third-party defendant, thus permits the dissent to dismiss out-of-hand Government interests that, properly viewed, are significant—whether or not ultimately dispositive. *See* Dissent at 235 ("As a practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image."); *id.* at 235–36 (dismissing the Government's *Brady* concern by noting that "[t]he Government is essentially arguing that it must hold on to the materials so that it can give them back to the defendant," a concern that the dissent argues "can be obviated simply by returning the non-responsive files to the defendant in the first place"). Perhaps in some situations, in which the owner of computerized data seized pursuant to a search warrant is the expected defendant in a criminal proceeding, problems of authentication or probity could be handled by stipulations, and *Brady* issues might be mooted by the return of the data to the defendant—though we express no view on those questions. As this case illustrates, however, when the owner of hard drives mirrored by the government is a third party who is not the expected target of the investigation, the government's interests in retention take on an additional layer of complexity. A stipulation with Ganias about the authenticity or probity of data extracted from his computers would not have affected the ability of the original targets of the investigation to raise challenges to authenticity or probity. Nor would returning the mirrors to Ganias—who at that point, absent a stipulation to the contrary, could presumably have destroyed or altered them, intentionally or accidentally—have protected the interests of those anticipated defendants in conducting their own forensic examination of the data in search of exculpatory evidence or to replicate and criticize the Government's inspection procedures.

37 Of course, engaging with the specifics requires acknowledging and emphasizing that technologies rapidly evolve, and that the specifics change. *See* John Sammons, *The Basics of Digital Forensics* 170 (2012) (commenting that digital forensics faces the "blinding speed of technology [and] new game-changing technologies such as cloud computing and solid state hard drives ... just to name a few"). In discussing the technological specifics of computer hard drives, we have primarily addressed a particular form of electronic storage that has become conventional. *See supra* note 32. Newer forms of emerging storage technology, or future developments, may work differently and thus present different challenges. *See, e.g.* , Bell & Boddington, *supra* , at 3, 6, 14 (observing that "the peculiarity of 'deleted, but not

forgotten' data which so often comes back to haunt defendants in court is in many ways a bizarre artefact of hard drive technology" and that increasingly popular solid state drives can "modify themselves very substantially without receiving instructions to do so from a computer," and thus predicting that "recovery of deleted files and old metadata will become extremely difficult, if not impossible" as solid state storage devices utilizing a particular deletion protocol called "TRIM" become more prevalent); King & Vidas, *supra* , at 111 ("We show that on a TRIM-enabled [solid state drive], using an Operating System (OS) that supports TRIM, ... in most cases no data can be recovered."); *id.* at 113 ("[M]ost [solid state drive] manufacturers have a TRIM-enabled drive model currently on the market."). *But see* Bonetti et al., *supra* , at 270-71, 278 (making clear that solid state drives, which differ considerably among models and vendors, may yield differing levels of deleted-file recoverability, depending upon their utilization of TRIM and other deletion protocols, erasing patterns, compression, and wear leveling protocols). Solid state drives, of course, are just one example. *Cf.* Bell & Boddington, *supra* , at 3 ("It is ... in the nature of computing that we perceive regular paradigm shifts in the ways that we store and process information."). The important point is that considerations discussed in this opinion may well become obsolete at some future point, the challenges facing forensic examiners and affected parties may change, and courts dealing with these problems will need to become conversant with the particular forms of technology involved in a given case and the evidentiary challenges presented by those forms.

In emphasizing such specifics, we reiterate that we do not mean to thereby minimize or ignore the privacy concerns implicated when a hard drive or forensic mirror is retained, even pursuant to a warrant. The seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure. Indeed, another weakness of the file cabinet analogy is that no file cabinet has the capacity to contain as much information as the typical computer hard drive. In 2005, Professor Orin Kerr noted that the typical personal computer hard drive had a storage capacity of about eighty gigabytes, which he estimated could hold text files equivalent to the "information
218 contained in the books on one floor of a typical academic library." Kerr, *218 *Searches and Seizures in a Digital World* , *supra* , at 542. By 2011, computers were being sold with one terabyte of capacity—about twelve times the size of Professor Kerr's library floor. Paul Ohm, Response, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges* , 97 Va. L. Rev. In Brief 1, 6 (2011). The *New York Times* recently reported that commercially available storage devices can hold "16 petabytes of data, roughly equal to 16 billion thick books." Quentin Hardy, *As a Data Deluge Grows, Companies Rethink Storage* , N.Y. Times, Mar. 15, 2016, at B3.

Moreover, quantitative measures fail to capture the significance of the data kept by many individuals on their computers. Tax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, banking and shopping information—all may be kept in the same device, interspersed among the evidentiary material that justifies the seizure or search. *Cf. Riley v. California* , —— U.S. ——, 134 S.Ct. 2473, 2489–90, 189 L.Ed.2d 430 (2014) (explaining that even microcomputers, such as cellphones, have "immense storage capacity" that may contain "every piece of mail [people] have received for the past several months, every picture they have taken, or every book or article they have read," which can allow the "sum of an individual's private life [to] be reconstructed"); *United States v. Galpin* , 720 F.3d 436, 446 (2d Cir. 2013) ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."). While physical searches for paper records or other evidence may require agents to rummage at least cursorily through much private material, the reasonableness of seizure and subsequent retention by the government of such vast quantities of irrelevant private material was rarely if ever presented in

cases prior to the age of digital storage, and has never before been considered justified, or even practicable, in such cases. Even as we recognize that search and seizure of digital media is, in some ways, distinct from what has come before, we must remain mindful of the privacy interests that necessarily inform our analysis.[38]

38 The dissent extensively addresses these privacy interests. As this opinion makes clear, we do not disagree with the proposition that the seizure and retention of computer hard drives or mirrored copies of those drives implicate such concerns and raise significant Fourth Amendment questions. We do not agree, however, for reasons we have also discussed at length, with the dissent's dismissal of the countervailing government concerns. However these issues are ultimately resolved, we believe that the Government's arguments are, at a minimum, sufficiently forceful that it is unwise to try to reach definitive conclusions about the constitutional issues in a case that can be decided on other grounds.

We note, however, that parties with an interest in retained storage media are not without recourse. As noted above, Ganias never sought the return of any seized material, either by negotiating with the Government or by motion to the court. Though negotiated stipulations regarding the admissibility or integrity of evidence may not always suffice to satisfy reasonable interests of the government in retention during the pendency of an
219 investigation,[39] such *219 stipulations may make return feasible in a proper case, and can be explored.

39 For instance, as we have previously noted, where, as here, the owner of the records is not (at least at the time of the seizure) the target of the investigation, a stipulation from that party may not serve the government's need to establish the authenticity or integrity of evidence it may seek to use, and access to the records by that party will not necessarily satisfy the need of potential future defendants to test the processes used by the government to extract or accurately characterize data culled from a hard drive. In some cases, however, negotiated solutions may be practicable.

A person from whom property is seized by law enforcement may move for its return under Federal Rule of Criminal Procedure 41(g).[40] Rule 41(g) permits a defendant or any "person aggrieved" by either an unlawful or *lawful* deprivation of property, *see United States v. Comprehensive Drug Testing, Inc.* , 621 F.3d 1162, 1173 (9th Cir. 2010) (en banc) (per curiam), to move for its return, Fed. R. Crim. P. 41(g). Evaluating such a motion, a district court "must receive evidence on any factual issue necessary to decide the motion," and, in the event that the motion is granted, may "impose reasonable conditions to protect access to the property and its use in later proceedings." *Id.* Since we resolve this case on other grounds, we need not address whether Ganias's failure to make such a motion forfeited any Fourth Amendment objection he might otherwise have had to the Government's retention of the mirrors. But we agree with the district court that, as a pragmatic matter, such a motion "would have given a court the opportunity to consider 'whether the government's interest could be served by an alternative to retaining the property,' and perhaps to order the [mirrors] returned to Ganias, all while enabling the court to 'impose reasonable conditions to protect access to the property and its use in later proceedings.' " *Ganias* , 2011 WL 2532396, at *8 (citation omitted) (first quoting *In re Smith* , 888 F.2d 167, 168 (D.C. Cir. 1989) (per curiam); then quoting Fed. R. Crim. P. 41(g)).

40 Rule 41(g) provides as follows:

> **Motion to Return Property.** A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

Rule 41(g) thus provides a potential mechanism, in at least some contexts, for dealing with the question of retention at a time when the government may be expected to have greater information about the data it seeks and the best process through which to search and present that data in court. It is worth observing, then, that Rule 41(g) constitutes a statutory solution (as opposed to a purely judicially constructed one) to at least one facet of the retention problem.[41] Statutory approaches, of course, do not relieve courts from their obligation to interpret the Constitution; nevertheless, such approaches have, historically, provided one mechanism for safeguarding privacy interests while, at the same time, addressing the needs of law enforcement in the face of
220 technological change. Indeed, when Congress addressed wiretapping in the Omnibus Crime Control *220 and Safe Streets Act of 1968, the Senate Judiciary Committee issued a report reflecting precisely this ambition—to provide a framework through which law enforcement might comport with the demands of the Constitution and meet important law enforcement interests. *See* S. Rep. No. 90-1097, at 66-76 (1968) (describing the construction of the then-Omnibus Crime Control and Safe Streets of Act of 1967, which laid out comprehensive rules for when and how law enforcement could intercept wire and oral communications through electronic surveillance, as a Congressional attempt to respond to and synthesize, first, technological change, *id.* at 67, second, ineffective or unclear state statutory regimes, *id.* at 69, third, evolving Supreme Court precedent, *id.* at 74-75, and fourth, law enforcement concerns, *id.* at 70); *see also id.* at 66 ("Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized."). The Act did not seek to supplant the role of the courts, nor could it have done so, but it did demonstrate the intuitive proposition that Congress can and should be a partner in the process of fleshing out the contours of law-enforcement policy in a shifting technological landscape. In acknowledging the role of Rule 41(g), then, we seek also to suggest that search and seizure of electronic media may, no less than wiretapping, merit not only judicial review but also legislative analysis; courts need not act alone.

41 The advisory committee notes to the 2009 amendments to Federal Rule of Criminal Procedure 41(e)(2)(B) contemplate that Rule 41(g) may indeed constitute such a solution. Regarding specifically the seizure of electronic storage media or the search of electronically stored information, the advisory committee notes observe that though the rule does not create

> a presumptive national or uniform time period within which ... off-site copying or review of ... electronically stored information would take place, ... [i]t was not the intent of the amendment to leave the property owner without ... a remedy[:] ... Rule 41(g) ... provides a process for the "person aggrieved" to seek an order from the court for a return of the property, including storage media or electronically stored information, under reasonable circumstances.

As we have said, we need not resolve the ultimate question whether the Government's retention of forensic copies of Ganias's hard drives during the pendency of its investigation violated the Fourth Amendment. We conclude, moreover, that we should not decide this question on the present record, which does not permit a full assessment of the complex and rapidly evolving technological issues, and the significant privacy concerns,
221 relevant to its consideration.[42] Having noted Ganias's argument, *221 we do not decide its merits. We instead turn to the question of good faith.

42 The dissent faults us for our caution in this regard, suggesting that "the prevailing scholarly consensus has been that the [original *Ganias*] panel largely got it right." Dissent at 228 n. 5. With respect, the dissent mischaracterizes the scholarly response. As an initial matter, the dissent cites Professor Kerr as having concluded that the panel "largely got it right." *Id.* In fact, Kerr's analysis of the original panel opinion is generally critical, not complimentary. *See* Kerr, *Executing Warrants for Digital Evidence* , *supra* , at 32 (critiquing the panel for going too far and thus offering a "particularly strong version" of Kerr's approach). Assessing the original panel's analysis, Kerr first concludes that, given the technological contours of electronic media, an affirmative obligation to delete could be "difficult to implement," just as it could be difficult to ascertain at what point in the process such a "duty [would be] triggered." *Id.* Second, Kerr concludes that—to the degree that restrictions should be placed upon what the government may do with non-responsive data that must, for pragmatic reasons, be retained—a restriction preventing the government from viewing data pursuant to a search warrant acquired with independent probable cause is unnecessary "to restore the basic limits of search warrants in a world of digital evidence." *Id.* at 33.

Apart from this citation to Kerr and to two student notes (which reach differing conclusions about the merits of the panel opinion), the articles the dissent cites (as is evident from the carefully worded parentheticals the dissent itself provides) are not evaluations of the original panel opinion, but instead provide largely descriptive accounts of the opinion and its relation to other case law in the context of making other points. The signed article that comes the closest to providing a normative critique of the panel's opinion concludes that "*perhaps* the panel's answer is broadly the right answer," but rejects the panel's—and the dissent's—reasoning. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)* , 18 U. Pa. J. Const. L. 933, 948 (2016) (emphasis added); *see id.* at 947 (concluding that, because "in 2003 and in 2006 the government obtained a warrant demonstrating particularized suspicion towards Ganias's data, and in each instance agents thereafter only looked for the responsive data," it was inapt for the original panel to conclude that the Government's position would transform a warrant for electronic data into a "general warrant"). We do not opine on these issues here, but we see no scholarly consensus on the complicated questions implicated in this case that would suggest caution is ill-advised in a matter where these questions need not be answered to reach a resolution. Caution, although not always satisfying, is sometimes the most appropriate approach.

III

The Government argues that, because it acted in good faith throughout the pendency of this case, any potential violation of the Fourth Amendment does not justify the extraordinary remedy of suppression. *See Davis v. United States* , 564 U.S. 229, 237, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011) (noting the "heavy toll" exacted by suppression, which "requires courts to ignore reliable, trustworthy evidence," and characterizing suppression as a "bitter pill," to be taken "only as a 'last resort' " (quoting *Hudson v. Michigan* , 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006))); *accord United States v. Clark* , 638 F.3d 89, 99 (2d Cir. 2011). In particular, the Government urges that its "reliance on the 2006 warrant," which it obtained after disclosing to the magistrate judge all relevant facts regarding its retention of the mirrored files, "fits squarely within the traditional *Leon* exception for conduct taken in reliance on a search warrant issued by a neutral and detached magistrate judge."[43] Government Br. at 59; *see Leon* , 468 U.S. at 922, 104 S.Ct. 3405. For the following reasons, we agree.

43 The Government also contends: (1) that it relied in good faith on the 2003 warrant in retaining the mirrors; and (2) that its behavior was in no way culpable, rendering exclusion inappropriate, *see* Government Br. at 51; *see also Herring v. United States* , 555 U.S. 135, 144, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009) ("[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence."); *accord*

Davis , 564 U.S. at 237, 131 S.Ct. 2419. Given our conclusion that the Government relied in good faith on the 2006 warrant, we need not address these additional arguments.

In *Leon*, the Supreme Court determined that the exclusion of evidence is inappropriate when the government acts "in objectively reasonable reliance" on a search warrant, even when the warrant is subsequently invalidated. 468 U.S. at 922, 104 S.Ct. 3405 ; *see also Clark* , 638 F.3d at 100 ("[I]n *Leon*, the Supreme Court strongly signaled that most searches conducted pursuant to a warrant would likely fall within its protection."). Such reliance, however, must be *objectively reasonable* . *See Leon* , 468 U.S. at 922–23, 104 S.Ct. 3405 ("[I]t is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." (footnote omitted)). Thus, to assert good faith reliance successfully, officers must, *inter alia* , disclose all potentially adverse information to the issuing judge. *See United States v. Reilly* , 76 F.3d 1271, 1280 (2d Cir.) ("The good faith exception to the exclusionary rule does not protect searches by officers who fail to provide all potentially adverse information to the issuing judge...."), *aff'd and amended* , 91 F.3d 331 (2d Cir. 1996) (per curiam); *see also United States v. Thomas* , 757 F.2d 1359, 1368 (2d Cir. 1985) (finding good faith reliance on a warrant, under *Leon*, where officers, first, committed a constitutional violation they did not *222 reasonably know, at the time, was unconstitutional—a warrantless canine sniff—and second, in relying on evidence from this sniff in a warrant application, fully revealed the fact of the canine sniff to a magistrate judge), *cert. denied by Fisher v. United States* , 474 U.S. 819, 106 S.Ct. 66, 88 L.Ed.2d 54 (1985) *and Rice v. United States* , 479 U.S. 818, 107 S.Ct. 78, 93 L.Ed.2d 34 (1986).

222

Ganias argues that reliance on the 2006 warrant is misplaced for two reasons. First, he urges that the alleged constitutional violation here (unlawful retention of the mirrored drives) had "long since" ripened into a violation by April 2006, when the second warrant was obtained, Appellant Br. at 55-56, and attests that "[n]othing [in *Leon*] suggests that the police, *after* they engage in misconduct, can then 'launder their prior unconstitutional behavior by presenting the fruits of it to a magistrate,' " *id.* at 56 (quoting *State v. Hicks* , 146 Ariz. 533, 707 P.2d 331, 333 (Ariz. Ct. App. 1985)). Second, Ganias argues that, even if "a subsequent warrant can ever appropriately purge the taint of an earlier violation, the agent must, at the very least, 'provide all potentially adverse information' regarding the earlier illegality 'to the issuing [magistrate] judge,' " a requirement that he argues was not satisfied here. *Id.* at 58 (quoting *Reilly* , 76 F.3d at 1280). Ganias's arguments are unavailing.

First, Ganias relies on this Court's decision in *Reilly* to argue categorically that agents who have engaged in a predicate Fourth Amendment violation may not rely on a subsequently issued warrant to establish good faith. *Reilly*, however, stands for no such thing. In *Reilly*, officers unlawfully intruded on the defendant's curtilage, discovering about twenty marijuana plants, before they departed and obtained a search warrant based on a "bare-bones" description of their intrusion and resulting observations which this Court found "almost calculated to mislead." *Reilly* , 76 F.3d at 1280 ; *see also id.* ("[The affidavit] simply ... stated that [the officers] walked along Reilly's property until they found an area where marijuana plants were grown. It did not describe this area to the Judge[,] ... [and it] gave no description of the cottage, pond, gazebo, or other characteristics of the area.... [The omitted information] was crucial. Without it, the issuing judge could not possibly make a valid assessment of the legality of the warrant that he was asked to issue."). We rejected the government's argument that the officers were entitled to rely on the warrant, noting that the officers had "undert[aken] a search that caused them to invade what they could not fail to have known was potentially ... curtilage," and that they thereafter "failed to provide [the magistrate issuing the warrant] with an account of what they did," so that the magistrate was unable to ascertain whether the evidence on which the officers relied in seeking the warrant was

"itself obtained illegally and in bad faith." *Id.* at 1281. In such circumstances, *Leon* did not—and does not—permit good faith reliance on a warrant. *See Leon* , 468 U.S. at 923, 104 S.Ct. 3405 (observing that an officer's reliance on a warrant is not *objectively reasonable* if he "misled [the magistrate with] information in an affidavit that [he] knew was false or would have known was false except for his reckless disregard of the truth").

The present case, however, is akin not to *Reilly*, but to this Court's decision in *Thomas*, which the *Reilly* panel carefully distinguished, while reaffirming. *See Reilly* , 76 F.3d at 1281–82. In *Thomas*, an agent, acting without a warrant, used a dog trained to detect narcotics to conduct a "canine sniff" at a dwelling. 757 F.2d at 1367. The
223 agent presented evidence acquired as a result of the sniff to a "neutral *223 and detached magistrate" who, on the basis of this and other evidence, determined that the officer had probable cause to conduct a subsequent search of the dwelling in question. *Id.* at 1368. The defendant moved to suppress the evidence found in executing the search warrant, arguing that the antecedent canine sniff constituted a warrantless, unconstitutional search and that the evidence acquired from that sniff was dispositive to the magistrate judge's finding of probable cause. *See id.* at 1366. This Court agreed on both counts: first deciding, as a matter of first impression in our Circuit, that the canine sniff at issue constituted a search, *id.* at 1367, and second determining that, absent the evidence acquired from this search, the warrant was not supported by probable cause, *id.* at 1368. The *Thomas* panel nevertheless concluded that suppression was inappropriate because the agent's reliance on the warrant was objectively reasonable: "The ... agent brought his evidence, including [a factual description of the canine sniff], to a neutral and detached magistrate. That magistrate determined that probable cause to search existed, and issued a search warrant. There is nothing more the officer could have or should have done under these circumstances to be sure his search would be legal." *Id.*

Reilly carefully distinguished *Thomas*, and in a manner that makes apparent that it is *Thomas* that is dispositive here. First, the *Reilly* panel noted that *Thomas* was unlike *Reilly*, in that the agent in *Thomas* disclosed all crucial facts for the legal determination in question to the magistrate judge. *Reilly* , 76 F.3d at 1281. Then, the *Reilly* panel articulated another difference: while in *Reilly*, "the officers undertook a search that caused them to invade what they could not fail to have known was potentially Reilly's curtilage," in *Thomas*, the agent "did not have any significant reason to believe that what he had done [conducting the canine sniff] was unconstitutional." *Id* . ; *see also id.* ("[U]ntil *Thomas* was decided, no court in this Circuit had held that canine sniffs violated the Fourth Amendment."). Thus, the predicate act in *Reilly* tainted the subsequent search warrant, whereas the predicate act in *Thomas* did not. The distinction did not turn on whether the violation found was *predicate* , or prior to, the subsequent search warrant on which the officers eventually relied, but on whether the officers' reliance on the warrant was reasonable.

Contrary to Ganias's argument, then, it is not the case that good faith reliance on a warrant is never possible in circumstances in which a predicate constitutional violation has occurred. The agents in *Thomas* committed such a violation, but they had no "significant reason to believe" that their predicate act was indeed unconstitutional, *Reilly* , 76 F.3d at 1281, and the issuing magistrate was apprised of the relevant conduct, so that the magistrate was able to determine whether any predicate illegality precluded issuance of the warrant. In such circumstances, invoking the good faith doctrine does not "launder [the agents'] prior unconstitutional behavior by presenting the fruits of it to a magistrate," as Ganias suggests. Appellant Br. at 56 (quoting *Hicks* , 707 P.2d at 333). In such cases, the good faith doctrine simply reaffirms *Leon* 's basic lesson: that suppression is inappropriate where reliance on a warrant was "objectively reasonable." *Leon* , 468 U.S. at 922, 104 S.Ct.
224 3405.[44] *224 Such is the case here. First, Agent Hosney provided sufficient information in her affidavit to apprise the magistrate judge of the pertinent facts regarding the retention of the mirrored copies of Ganias's

hard drives—the alleged constitutional violation on which he relies. Agent Hosney explained that the mirror images in question had been "seized on November 19, 2003 from the offices of Taxes International," J.A. 461, ¶ 7; that information material to the initial investigation of a third party had been located on the mirrors and "analyzed in detail," J.A. 464, ¶ 15; that Ganias was not, at the time of the original seizure, under investigation, J.A. 461, ¶ 3; that, "[p]ursuant to [that initial warrant]," Agent Hosney could not search Ganias's personal or business files as the warrant authorized search only of "files for [AB] and IPM," J.A. 464, ¶ 14; and that Ganias's personal data—which Agent Hosney was not authorized to search—was *on those mirrored drives* , J.A. 467, ¶ 27, and thus, *a fortiori* , had been there for the past two and a half years. The magistrate judge was thus informed of the fact that mirrors containing data non-responsive to the 2003 warrant had been retained for several years past the initial execution of that warrant and, to the degree it was necessary, that data responsive to the 2003 warrant had been analyzed in detail. The magistrate therefore had sufficient information on which to determine whether such retention precluded issuance of the 2006 warrant. *Cf. Thomas* , 757 F.2d at 1368 ("The magistrate, whose duty it is to interpret the law, determined that the canine sniff could form the basis for probable cause....").

[44] Insofar as Ganias argues that *Thomas* 's and *Reilly* 's holdings are limited to when the alleged predicate violation is a *search* that taints the warrant, but do not extend to circumstances in which the alleged predicate violation is a seizure or unlawful retention, we discern no justification for this distinction. But for the canine search in *Thomas* —the predicate violation—there would have been no subsequent warrant pursuant to which the government searched the dwelling and on whose legality it relied in conducting that search. But for the retention in this case—the alleged predicate violation —there could have been no subsequent search warrant pursuant to which the Government searched the relevant evidence and on whose legality the Government relied in conducting that search. To credit Ganias's distinction would be to replace the underlying directive that reliance on a warrant be "objectively reasonable," *Leon* , 468 U.S. at 922, 104 S.Ct. 3405, with an arbitrary formalism.

Ganias disagrees, arguing, in particular, that, though Agent Hosney alerted the magistrate that the mirrors had been retained for several years; that data responsive to the original warrant had been both located and extensively analyzed; and that those of Ganias's QuickBooks files that Agent Hosney wanted to search were non-responsive to the original warrant, the Hosney affidavit did not go far enough in that it failed to disclose that the agents "had been retaining the non-responsive records for a full 16 months *after* the files within the November 2003 warrant's scope had been identified." Appellant Br. at 60. As an initial matter, the Government *did* alert the magistrate that it had located responsive data on the mirrors *and* conducted extensive analysis of that responsive material, and it is not clear what else the Government should have said: the district court did not determine—nor does the record show—that by January 2005, as Ganias contends, the Government had determined, as a forward-looking matter, that it had performed all forensic searches of data responsive to the 2003 warrant that might prove necessary over the course of its investigation. *Compare* J.A. 322 (Q: "So it's fair to say that as of mid-December [2004], your forensic analysis was completed at that time?" Agent Chowaniec: "That's correct, of the computers."), *with* J.A. 324 (Q: "Did you know you wouldn't require further analysis by
225 Greg Norman or any other examiner at the Army lab in Georgia after December of 2004?" Agent *225
Chowaniec: "No."); *see supra* note 12. Nor would it be reasonable to expect additional detail in the affidavit on this point, even assuming Ganias's contention to be correct that the Government had both finished its segregation *and* provided insufficient facts to alert the magistrate judge to that reality, given the dearth of precedent suggesting its relevance. *Cf. Clark* , 638 F.3d at 105 ("[W]here the need for specificity in a warrant or warrant affidavit on a particular point was not yet settled or was otherwise ambiguous, we have declined to find

that a well-trained officer could not reasonably rely on a warrant issued in the absence of such specificity."); *cf. Reilly* , 76 F.3d at 1280 (noting that the affidavit in that case, in clear contrast to the affidavit in this one, was "almost calculated to mislead").

Second, here, as in *Thomas*, it is also clear that the agents, as the panel put it in *Reilly*, "did not have any significant reason to believe that what [they] had done was unconstitutional," *Reilly* , 76 F.3d at 1281 —that their retention of the mirrored hard drives, while the investigation was ongoing, was anything but routine. At the time of the retention, no court in this Circuit had held that retention of a mirrored hard drive during the pendency of an investigation could violate the Fourth Amendment, much less that such retention would do so in the circumstances presented here. *See id.* (noting that suppression was inappropriate in *Thomas* in part because no relevant precedent established that canine sniffs of a dwelling "violated the Fourth Amendment").[45] Moreover, as noted above, the 2003 warrant authorized the lawful seizure not merely of particular records or data, but of the hard drives themselves, or in the alternative the creation of mirror images of the drives to be removed from the premises for later forensic evaluation, and set no greater limit on the Government's retention of those materials than on any other evidence whose seizure it authorized.

[45] The closest decision Ganias can locate is *United States v. Tamura* , 694 F.2d at 594–95, an out-of-circuit case that concerned intermingled paper files, the removal of which was unauthorized and the return of which had been vigorously sought by the affected parties. Whatever relevance that case may have by analogy, it is not sufficient to alert a reasonable agent to the existence of a serious Fourth Amendment problem: for to suggest that a holding applicable to retaining *intermingled paper files* specifically demanded to be returned clearly resolves a question about retention of a *physical digital storage medium* (the return of which had been neither suggested nor requested) would be "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley* , 134 S.Ct. at 2488.

Finally, the record here is clear that the agents acted reasonably throughout the investigation. They sought authorization in 2003 to seize the hard drives and search them off-site; they minimized the disruption to Ganias's business by taking full forensic mirrors; they searched the mirrors only to the extent authorized by, first, the 2003 warrant, and then the warrant issued in 2006; they were never alerted that Ganias sought the return of the mirrors; and they alerted the magistrate judge to these pertinent facts in applying for the second warrant. In short, the agents acted reasonably in relying on the 2006 warrant to search for evidence of Ganias's tax evasion. This case fits squarely within *Leon* so that, assuming, *arguendo* , that a Fourth Amendment violation occurred, suppression was not warranted.

* * *

We conclude that the Government relied in good faith on the 2006 search warrant and thus AFFIRM the
226 judgment of the *226 district court. Given this determination, we do not reach the specific Fourth Amendment question posed to us today.

LOHIER, Circuit Judge, joined by POOLER, Circuit Judge, concurring:

I concur fully in Part I of the majority opinion, which accurately recites the facts, and Part III, which affirms based on the narrow ground that the Government relied in good faith on the 2006 search warrant obtained in this case. It bears emphasizing that Part III contains the only holding in the majority opinion. I also concur insofar as the majority opinion clarifies that under appropriate circumstances it may be helpful for litigants to use the mechanism provided by Rule 41(g) of the Federal Rules of Criminal Procedure when faced with the Government's retention of electronic data.

Chin, Circuit Judge, dissenting:

I respectfully dissent.

Over two hundred fifty years ago, agents of the King of England, with warrant in hand, entered the home of John Entick. They rummaged through boxes and trunks, cabinets and bureaus. They were looking for evidence of known instances of seditious libel, but they took "all the papers and books without exception." *Entick v. Carrington* , 19 How. St. Tr. 1029, 1064 (C.P. 1765). In holding that Entick's rights were violated, the court explained:

> Papers are the owner's goods and chattels: they are his dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection; and though the eye cannot by the laws of England be guilty of a trespass, yet where private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect. Where is the written law that gives any magistrate such a power? I can safely answer, there is none; and therefore it is too much for us without such authority to pronounce a practice legal, which would be subversive of all the comforts of society.

Id. at 1066.

Entick was not lost on the Framers. As the Supreme Court has noted, "its propositions were in the minds of those who framed the fourth amendment to the constitution, and were considered as sufficiently explanatory of what was meant by unreasonable searches and seizures." *Boyd v. United States* , 116 U.S. 616, 626–27, 6 S.Ct. 524, 29 L.Ed. 746 (1886). And enshrined in the Fourth Amendment is the foundational principle that the Government cannot come into one's home looking for some papers and, without suspicion of broader criminal wrongdoing, indiscriminately take all papers instead.

In this case, the Government argues that when those papers are inside a computer, the result is different. It argues that when computers are involved, it is free to overseize files for its convenience, including files outside the scope of a warrant, and retain them until it has found a reason for their use. In essence, the Government contends that it is entitled to greater latitude in the computer age. I disagree. If anything, the protections of the Fourth Amendment are even more important in the context of modern technology, for the Government has a far
227 greater ability to intrude into a person's private affairs.[1] *227 Here, although the Government had a warrant for documents relating to only two of defendant-appellant Stavros Ganias's accounting clients, it seized *all* the data from three of his computers, including wholly unrelated personal files and files of other clients. The Government did so solely as a matter of convenience, and not because it suspected Ganias or any of his other clients of wrongdoing. The Government was able to extract the responsive files some thirteen months later. But instead of returning the non-responsive files, the investigators retained them, because, as one agent testified, they "viewed the data as the government's property, not Mr. Ganias's property." J. App. 146.[2] Some sixteen months later, almost two-and-a-half years after the files were first seized, the Government found an unrelated reason to prosecute Ganias—his personal tax evasion—and it sought judicial authorization to reexamine the data that was still in its possession. The Government contends that this conduct did not violate the Fourth Amendment, and that, even if it did, suppression was not warranted because its agents acted in good faith.

[1] *See, e.g.* , *United States v. Galpin* , 720 F.3d 436, 446 (2d Cir. 2013) ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain."); *United States v. Otero* , 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's

personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs...."); Orin S. Kerr, *Searches and Seizures in a Digital World* , 119 Harv. L. Rev. 531, 569 (2005) (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

[2] Throughout this dissent I refer as a matter of convenience to data on Ganias's hard drive as "files" or "documents." Of course, computers contain a variety of types of data, including data that we do not utilize as discrete "files" or "documents" (*e.g.* , metadata, the operating system, the BIOS).

I disagree. I would hold, as the panel held unanimously, that the Government violated Ganias's Fourth Amendment rights when it retained Ganias's non-responsive files for nearly two-and-a-half years and then reexamined the files for evidence of additional crimes. *United States v. Ganias* , 755 F.3d 125, 133–40 (2d Cir. 2014). I would also hold, as two members of the panel did, that the Government's actions are not excused by the good faith exception. *Id.* at 140–41. *But see id.* at 141 (Hall, *J.* , dissenting in part).[3] Accordingly, I dissent.

[3] The third member of the panel was the Honorable Jane A. Restani of the United States Court of International Trade, who sat by designation. Judge Restani was not eligible to participate in the *en banc* proceedings. *See* 28 U.S.C. § 46(c).

I.

I consider first whether Ganias's Fourth Amendment rights were violated. The majority addresses the question at length, with some twenty-five pages of scholarly discussion about the Fourth Amendment in the digital age, but it reaches no conclusion. *E.g.* , Maj. Op. at 200, 208, 211, 216, 219, 220–21. Although we reheard the case *en banc* (at our own request and not at the request of any party), and despite the benefit of additional briefing
228 and oral argument from the parties as well as eight *amicus* briefs,[4] the Court declines to rule *228 on the question, "offer[ing] no opinion on the existence of a Fourth Amendment violation in this case." *Id.* at 209. I would reach the question, and I would hold, as did the panel, that the Fourth Amendment was indeed violated.[5]

[4] All eight *amici* urged that we find a Fourth Amendment violation. Brief for *Amicus Curiae* Center for Constitutional Rights as *Amicus Curiae* in Support of Appellant, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4597942 ; Brief for *Amici Curiae* Center for Democracy & Technology, ACLU, et al. in Support of Defendant–Appellant, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4597943 ; Brief of *Amici Curiae* Electronic Privacy Information Center in Support of Appellant and Urging Affirmance, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4610149 ; Brief on Rehearing *En Banc* for *Amici Curiae* Federal Public Defenders Within the Second Circuit in Support of Appellant Stavros M. Ganias, No. 12-240-cr (July 29, 2015), 2015 WL 4597956 ; Brief of Google Inc. as Amicus Curiae Supporting Defendant–Appellant, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4597960 ; *Amicus Curiae* Brief of the National Ass'n of Criminal Defense Lawyers in Support of Defendant–Appellant and Urging Reversal, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4597959 ; Brief for *Amicus Curiae* New York Council of Defense Lawyers in Support of Appellant, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4597958 ; Brief of *Amicus Curiae* Restore the Fourth, Inc. in Support of Defendant–Appellant Stavros M. Ganias, *Ganias* , No. 12-240-cr (July 29, 2015), 2015 WL 4597961.

[5] I note also that the prevailing scholarly consensus has been that the panel largely got it right with its Fourth Amendment approach. *E.g.* , Stephen E. Henderson, *Fourth Amendment Time Machines (and What They May Say About Police Body Cameras)* , 18 U. Pa. J. Const. L. 933, 947 (2016) ("I agree, though I differ from the panel's

reasoning."); Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data* , 48 Tex. Tech L. Rev. 1, 30-33 (2015) (concluding that "[t]he basic approach mirrors the ongoing seizure approach recommended in this Article" and that "*Ganias* properly focuses on the reasonableness of the ongoing seizure of the nonresponsive files," while labeling the panel opinion as "a particularly strong version" that "courts could adopt"); *see also* Recent Case, *Second Circuit Creates A Potential "Right to Deletion" of Imaged Hard Drives. —* United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014)* , 128 Harv. L. Rev. 743, 747-50 (2014) (concluding that "[t]he *Ganias* court's opinion properly held that Ganias's Fourth Amendment rights were violated, and it rightly recognized the importance of the particularity requirement in the context of electronic evidence," but arguing that the panel could have "issued a narrower opinion"). *But see* Note, *Digital Duplications and the Fourth Amendment* , 129 Harv. L. Rev. 1046, 1059-64 (2016) (arguing the retention at issue should have been considered as a "search" and not a "seizure"). Others have likewise commented that the panel opinion fits with current Supreme Court jurisprudence, including, in particular, *Riley v. California* , 134 S.Ct. 2473. *E.g.* , Alan Butler, *Get a Warrant: The Supreme Court's New Course for Digital Privacy Rights After* Riley v. California, 10 Duke J. Const. L. & Pub. Pol'y 83, 112-13 (2014) ("The rule adopted in *Ganias* is consistent with the scope of privacy interests in digital data outlined in *Riley*, and other courts will be more likely to adopt the rule in light of the Supreme Court's decision."); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content* , 38 Harv. J.L. & Pub. Pol'y 117, 238-41 (2015) (commenting that, like the panel opinion, *Riley* "similarly supports a Fourth Amendment use restriction on lawfully obtained information" and concluding that "[e]ven though the government might have legally obtained the information at the front end, it could not search the information for evidence of criminal activity absent a warrant, supported by probable cause"); Paul Ohm, *The Life of* Riley *(* v. California*)* , 48 Tex. Tech L. Rev. 133, 138-39 (2015) (anticipating that future courts could find *Ganias* supportable under *Riley*).

A.

The facts are largely undisputed. Ganias was providing tax and accounting services to individuals and small businesses, including Industrial Property Management, Inc. ("IPM") and American Boiler. In November 2003, the Army, as part of an investigation of those two entities, subpoenaed from Ganias:

> All books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and American Boiler....

J. App. 433. Two Army computer specialists and another Army investigator came to Ganias's office, and they
229 saw three computers. They made identical copies of the hard drives of those computers to take *229 with them —that is, they cloned the hard drives by making exact replicas ("mirror images") on blank hard drives. In the course of doing so, they took data and files *not* "relating to the business, financial and accounting operations of [IPM] and American Boiler." *Id.* In fact, they took from those hard drives *all* of Ganias's data, including files relating to his personal affairs.

Back in their offices, the Army investigators copied the data taken from Ganias's computers onto "two sets of 19 DVDs," one of which was "maintained as evidence" while the other was kept as a "working copy." Special App. 11. It took the Army Criminal Investigation Division some seven months to begin reviewing the files, but before it began doing so, it invited the Internal Revenue Service (the "IRS") to join the investigation. The Army and the IRS thereafter proceeded separately, reviewing the mirror images for files responsive to the warrant.

By December 2004, approximately thirteen months after the seizure, some four months of which was spent locating a copy of the off-the-shelf consumer software known as QuickBooks, Army and IRS investigators were able to isolate and extract the files covered by the warrant, that is, the files relating to IPM and American

Boiler. The investigators were aware that, because of the constraints of the warrant, they were not permitted to review any other computer records. Indeed, the investigators were careful, at least until later, to review only data covered by the November 2003 warrant.

The investigators did not, however, purge or delete or return the non-responsive files. To the contrary, they retained the files because they "viewed the data as the government's property, not Mr. Ganias's property." J. App. 146.[6] Their view was that while items seized from an owner will be returned after an investigation closes, all of the electronic data here was evidence that was to be protected and preserved. As one agent testified, "[W]e would not routinely go into DVDs to delete data, as we're altering the original data that was seized. And you never know what data you may need in the future.... I don't normally go into electronic data and start deleting evidence off of DVDs stored in my evidence room." *Id.* at 122.

6 The majority suggests that I "seize[ ] on this single sentence ... as the smoking gun of the Government's bad faith." Maj. Op. at 206 n. 13. The testimony is what it is: a statement under oath by a law enforcement officer explaining the Government's actions. Moreover, as discussed below, there is more than just this single sentence to show the lack of good faith. *See infra* Part II.B.

In late 2004, IRS investigators discovered accounting irregularities regarding transactions between IPM and American Boiler in the documents taken from Ganias's office. After subpoenaing and reviewing the relevant bank records in 2005, they began to suspect that Ganias was not properly reporting American Boiler's income. Accordingly, on July 28, 2005, some twenty months after the seizure of his computer files, the Government officially expanded its investigation to include possible tax violations by Ganias. Further investigation in 2005 and early 2006 indicated that Ganias had been improperly reporting income for both his clients, leading the Government to suspect that he also might have been underreporting his own income.

At that point, the IRS case agent wanted to review Ganias's personal financial records, and she knew, from her review of the seized computer records, that they were among the files in the DVD copies of Ganias's hard
230 drives. The case agent was aware, however, that Ganias's personal financial *230 records were beyond the scope of the November 2003 warrant, and consequently she did not believe that she could review the non-responsive files, even though they were already in the Government's possession.

In February 2006, the Government asked Ganias and his counsel for permission to access certain of his personal files that were contained in the materials seized in November 2003. Ganias did not respond, and thus, on April 24, 2006, the Government obtained another warrant to search the preserved mirror images of Ganias's personal financial records taken in 2003. At that point, the mirror images had been in the Government's possession for almost two-and-a-half years.

B.

"[T]he ultimate touchstone of the Fourth Amendment is 'reasonableness.' " *Brigham City v. Stuart* , 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006). In adopting the Fourth Amendment, the Framers were principally concerned about "indiscriminate searches and seizures" conducted "under the authority of 'general warrants.' " *United States v. Galpin* , 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York* , 445 U.S. 573, 583, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980)). General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not limited in scope and application." *Maryland v. King* , —— U.S. ——, 133 S.Ct. 1958, 1980, 186 L.Ed.2d 1 (2013). The Fourth Amendment guards against

this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a specific crime; and (2) the warrant states with particularity the areas to be searched and the items to be seized. *Galpin* , 720 F.3d at 445–46.

The latter requirement, in particular, "makes general searches ... impossible" because it "prevents the seizure of one thing under a warrant describing another." *Id.* at 446 (quoting *Marron v. United States* , 275 U.S. 192, 196, 48 S.Ct. 74, 72 L.Ed. 231 (1927)). This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant. *See Horton v. California* , 496 U.S. 128, 140, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990) ; *United States v. Tamura* , 694 F.2d 591, 595 (9th Cir. 1982). Certain exceptions have been made in those "comparatively rare instances where documents [we]re so intermingled that they [could not] feasibly be sorted on site." *Tamura* , 694 F.2d at 595–96. These circumstances might occur, for example, where potentially relevant documents are interspersed through a large number of boxes or file cabinets. *See id.* at 595. But in those cases, the off-site review had to be monitored by a neutral magistrate and non-responsive documents were to be returned after the relevant items were identified. *Id.* at 596–97.

In the computer age, off-site review has become much more common. The ability of computers to store massive volumes of information presents logistical problems in the execution of search warrants, and files on a computer hard drive are often "so intermingled that they cannot feasibly be sorted on site." *Id.* at 595. Forensic analysis of electronic data may take weeks or months to complete, and it would be impractical for agents to occupy an individual's home or office, or retain an individual's computer, for such extended periods of time. It is now also unnecessary. Today, advancements in technology enable the Government to create a mirror image
231 of an individual's hard drive, which can be searched as if it were the actual hard drive *231 but without otherwise interfering with the individual's use of his home, office, computer, or files. Indeed, the Federal Rules of Criminal Procedure now provide that a warrant for computer data presumptively "authorizes a later review of the media or information consistent with the warrant." Fed. R. Crim. P. 41(e)(2)(B).

But these practical necessities must still be balanced against our possessory and privacy interests, which have become more susceptible to deprivation in the computer age. A computer does not consist simply of "papers," but now contains the quantity of information found in a person's residence or greater. *See Riley v. California* , —— U.S. ——, 134 S.Ct. 2473, 2489, 189 L.Ed.2d 430 (2014) ; *Galpin* , 720 F.3d at 446. Virtually the entirety of a person's life may be captured as data: family photographs, correspondence, medical history, intimate details about how a person spends each passing moment of each day. GPS-enabled devices reveal our whereabouts. A person's internet search history may disclose her mental deliberations, whether or not those thoughts were favored by the Government, the public at large, or even that person's own family. Smartphones "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers." *Riley* , 134 S.Ct. at 2489 ; *see also* Michael D. Shear, David E. Sanger & Katie Benner, *In the Apple Case, a Debate Over Data Hits Home* , N.Y. Times (Mar. 13, 2016) ("It is a minicomputer stuffed with every detail of a person's life: photos of children, credit card purchases, texts with spouses (and nonspouses), and records of physical movements."). From a mere data storage device, a forensic analyst could reconstruct a "considerable chunk of a person's life." Kerr, *supra* note 1, at 569. All of this information is captured when the Government, in executing a search warrant, makes a mirror image of a hard drive.

We know only general descriptions of what was in Ganias's three hard drives—"personal and financial information," including information on other tax and accounting clients (*e.g.* , social security numbers) that was private to them—but the Fourth Amendment requires us to consider broadly the ramifications of computer

seizures. J. App. 428. If Ganias were a doctor, his computer might have contained the entire medical history of hundreds of individuals. If Ganias were a teacher, his computer could have contained educational information on dozens of students and communications with their families. If Ganias were not an individual but a corporation like Apple, Dropbox, Google, or Microsoft that stores individuals' information in the "cloud," the Government would have captured an untold vastness of information on millions of individuals. *See* Jim Kerstetter, *Microsoft Goes on Offensive Against Justice Department* , N.Y. Times (Apr. 15, 2016) ("When customer information is stored in a giant data center run by companies like Google, Apple and Microsoft, investigators can go straight to the information they need, even getting a judge to order the company to keep quiet about it."); *see also* Andrew Keane Woods, *Against Data Exceptionalism* , 68 Stan. L. Rev. 729, 743 (2016) ("Twenty years ago, a kidnapper might have confessed to a crime by writing in his diary.... Today the same admission is just as likely to be stored online....").

To safeguard individuals' possessory and privacy interests, when the Government seeks to review mirror images off-site, we are careful to subject the Government's conduct to the rule of reasonableness. *See, e.g.* , *United States v. Ramirez* , 523 U.S. 65, 71, 118 S.Ct. 992, 140 L.Ed.2d 191 (1998) ("The general touchstone of
232 reasonableness *232 which governs Fourth Amendment analysis governs the method of execution of the warrant." (citation omitted)). The advisory committee's notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is "reasonable" in this context. Specifically, the committee rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." Fed. R. Crim. P. 41(e)(2)(B) advisory committee's notes to 2009 amendments. The committee noted that several variables—storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload—influence the duration of a forensic analysis and counsel against a "one size fits all" time period. *Id.* In combination, these factors might justify an off-site review lasting for a significant period of time. They do not, however, provide an "independent basis" for retaining any electronic data "other than [those] specified in the warrant." *United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1171 (9th Cir. 2010) (*en banc*) (*per curiam*).

Hence, for these practical considerations, the Government may, consistent with the Fourth Amendment, overseize electronically stored data when executing a warrant. But overseizure is exactly what it sounds like. It is a seizure that *exceeds* or *goes beyond* what is otherwise authorized by the Fourth Amendment. It is an overseizure of evidence that may be reasonable, in light of the practical considerations.

But once the Government is able to extract the responsive documents, its right to the overseizure of evidence comes to an end. This obvious principle has long been adhered to in the context of physical documents, such as when the Government seizes entire file cabinets for off-site review. *See Tamura* , 694 F.2d at 596–97 ("We likewise doubt whether the Government's refusal to return the seized documents not described in the warrant was proper."); *see also Andresen v. Maryland* , 427 U.S. 463, 482 n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976) ("[T]o the extent such papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily...."). By logical extension, at least in a situation where responsive computer files can be extracted without harming other government interests, this principle would apply with equal force. *See CDT* , 621 F.3d at 1175–76 (using "file cabinets" as a starting analogy for analyzing digital privacy issues). Once responsive files are segregated or extracted, the retention of non-responsive documents is no longer reasonable, and the Government is obliged, in my view, to return or dispose of the non-responsive files within a reasonable period of time. *See CDT* , 621 F.3d at 1179 (Kozinski, *J.* , concurring) ("Once the data has been segregated ... any remaining copies should be destroyed or ... returned...."). At that

point, the Government's overseizure of files and continued retention of non-responsive documents becomes the equivalent of an unlawful general warrant. *See CDT* , 621 F.3d at 1176 (majority opinion) (noting "serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant"); *cf. United States v. Jones* , ——U.S. ——, 132 S.Ct. 945, 955–56, 181 L.Ed.2d 911 (2012) (Sotomayor, *J.* , concurring) (warning that "Government can store ... records and efficiently mine them for information years into the future").

In the circumstances here, the Government violated Ganias's right against unreasonable searches and seizures.
233 The Government overseized Ganias's data in *233 November 2003, taking both responsive and non-responsive documents. By December 2004, the responsive documents had been segregated and extracted. Yet, instead of returning or deleting the non-responsive files, the Government retained them for another year and a half, until it finally developed a justification to search them again for unrelated reasons. Without some independent basis for retaining the non-responsive documents in the interim, however, in my view the Government clearly violated Ganias's rights under the Fourth Amendment.

The majority comments that it is "unclear" whether the Government had segregated the files relating to IPM and American Boiler from non-responsive files by December 2004. Maj. Op. at 205–06 & n. 12. But the record shows that by October 2004, the Government had placed files thought to be responsive onto a CD. Referring to this event at rehearing *en banc* , the Government stated:

> There does come a point where we often identify a subset of documents that are responsive, *and you could even call it segregating* . In this case, they put them onto a separate disc as working copies and sent [them] to the case agents.

Oral Arg. 32:12-43 (emphasis added). And as an agent then testified, "as of mid-December, [the] forensic analysis was completed." J. App. 322. In other words, the responsive files were segregated.

The majority posits that perhaps the agents did not consider the forensic analysis as to IPM and American Boiler completed "as a forward-looking matter" as of December 2004. Maj. Op. at 205, 224. The record, however, shows otherwise, and, at a minimum, it is clear that the segregation of the files was essentially complete at that point. Moreover, this factual distinction is both speculative and irrelevant. The Fourth Amendment should not be held in abeyance on the off-chance that later developments might cause agents to want to reexamine documents preliminarily determined to be non-responsive. Indeed, the Fourth Amendment recognizes that some degree of perfection must be sacrificed to safeguard liberties. By barring the Government from simply taking *everything* through the use of a general warrant, the Fourth Amendment contemplates that investigators may miss *something* . With computers, another search term can always be concocted and data can always be further crunched. But the fact that another iota of evidence might be uncovered at some point down the road does not defeat the rights protected by the Fourth Amendment. *Cf. Riley* , 134 S.Ct. at 2491 ("[T]he Founders did not fight a revolution to gain the right to government agency protocols.").

C.

I next turn to the Government's arguments as to why the Fourth Amendment was not violated. The Government offers several "legitimate governmental interests" that it contends permit it to hold onto data long after it has been seized, sorted, and segregated, even though the data includes irrelevant, personal information. *See* Gov't Br. 29. During the *en banc* process, the Government suggested that these interests permit it to retain data for the
234 duration of the prosecution. *See id.* at 17, 29; Oral Arg. 27:38-57.[7] *234 At the outset, in evaluating the legitimacy of these reasons in relation to this case, I note what is *not* implicated here. This is not a case where

the defendant's non-responsive files had independent evidentiary value—for instance, in a prosecution where the charge was that evidence had been destroyed, *e.g.* , 18 U.S.C. § 1519, it would be relevant that certain documents were *not* on the hard drive.[8] This is also not a case where the manner in which a responsive file was stored could be used to prove knowledge or intent, as might be the situation in a child pornography prosecution. And this is not a case where the physical hard drive itself is of evidentiary value—the fact that Ganias's files were actually found inside a computer did not make his guilt more or less probable. Finally, this is not a case where the Government seized Ganias's hard drive to proceed against him. Instead, the Government retained Ganias's hard drive for some two-and-a-half years without suspecting him of criminal wrongdoing, and the agency that ultimately suspected him of illicit tax activity (the IRS) was not even involved at the outset.

7 In contrast, before the original panel, the Government argued: "Where the warrant does not specify a time period in which the review must be conducted—like the November 2003 warrant—this Court has allowed the government to retain computer material indefinitely and 'without temporal limitation.' " First Gov't Br. 30 (quoting *United States v. Anson* , 304 Fed.Appx. 1, 3 (2d Cir. 2008)).

8 The majority twice relatedly suggests that the entire mirror image might be relevant here because Ganias made allusion to a "computer flaw" or "software error" in QuickBooks that did not allow him to properly split deposited checks. *See* Maj. Op. at 207 n. 16, 214 n. 31. The issue surely could be resolved by retaining only the responsive files and a copy of the pertinent version of QuickBooks. Moreover, even assuming there is some speculative value to retaining entire mirror images to prove the non-existence of a glitch, it would hardly be reasonable to rule that these practical frustrations of everyday technology provide the Government license to keep everything.

The Government argues that it has the right to retain non-responsive files so that, at trial, *responsive* files will be more easily authenticated or of greater evidentiary weight. Once again, the Government's argument obscures the issues in *this* case. The agents could not have been keeping non-responsive files for the purpose of proceeding against Ganias, as they did not yet suspect Ganias of criminal wrongdoing.

Further, even if the authentication concern is genuine, "[t]he bar for authentication of evidence is not particularly high." *United States v. Gagliardi* , 506 F.3d 140, 151 (2d Cir. 2007). Indeed, as long as *a* reasonable juror *could* find that evidence was authentic we permit that evidence to be introduced. *Id.* ; *see* Fed. R. Evid. 901(a). Meeting this minimal burden is not difficult—all the Government need do is to introduce as a trial witness one of its agents who handled the data. *See Tamura* , 694 F.2d at 597.

The Government presses the point by arguing that by keeping the hard drives, it could *more easily* preserve the chain of custody and authenticate by "calculat[ing] ... a 'hash value' for the original and th[e] [mirror] image." Gov't Br. 30. A "hash value" is an alphanumeric marker (*e.g.* , "ABC123") for data that stays the same *if and only if* the data is not altered. Thus, if a hard drive and its mirror image have the same hash value, the files in the mirror image are exact replicas; whereas if the Government purges data from the mirror image, then hash values would not match. Hash values thus make authentication easy. *See* Fed. R. Evid. 901(b)(4).

The hashing argument, however, is not persuasive. First, the Government would have to call an expert just to explain to a jury what a hash value was, as it did here. *See* Fed. R. Evid. 702(a) ; Trial Tr. 128-30. This is no less burdensome than simply having an agent testify as to the chain of custody. Second, as the Government acknowledged at rehearing *en banc* , it can hash individual files that it has segregated. *See* Oral Arg. 31:08-30.
235 This practice is not a hypothetical possibility: the Government *235 has done so before, *see, e.g.* , *United States v. Hock Chee Koo* , 770 F.Supp.2d 1115, 1123 (D. Or. 2011), and the Government did so in this very case for

Ganias's QuickBooks files, *see* Trial Tr. 147-54. *See generally* Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash* , 119 Harv. L. Rev. F. 38, 40-41 (2005) ("Many digital analysis tools can be configured to calculate separate hash values of each individual file...."). The Government's ability to authenticate individual files by hashing them undercuts its assertion that it must retain non-responsive files to authenticate responsive ones. Hashing appears to make it easier for the Government to comply with the Fourth Amendment, not harder.

Next, the Government contends that it has an interest in retaining computer evidence in its "original form" to preserve "the integrity and usefulness of computer evidence during a criminal prosecution." Gov't Br. 32. This contention is unpersuasive. The Government can always preserve a copy of the *responsive* files to protect against degradation—indeed, the Government points to no reason why a hard drive with all of Ganias's files would be less prone to degradation than a hard drive with some of his files. Moreover, even assuming there is some slight prosecutorial advantage gained by being able to show juries what a computer interface looked like in its "original form," this benefit surely does not justify a violation of basic Fourth Amendment rights.

In a similar vein, the Government argues that retention of mirror images "preserves the evidentiary value of computer evidence itself" and might "refute claims ... of data tampering." Gov't Br. 31-34. As a practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image.[9] More generally, the Government can argue in every case that overseized evidence will have some bearing on the "evidentiary value" of other, properly seized evidence at trial. When the Government makes authorized seizures of folders of financial information from a file cabinet, it could argue that it is entitled to seize the entire cabinet to demonstrate to a jury that folders were preserved in their original form. Or the Government might like to seize nearby, carefully organized folders of medical information to rebut a claim of incompleteness by showing how meticulous the defendant was. Or the Government might seek to seize a folder of children's report cards to show that the defendant normally kept information from a certain time period. Permitting the Government to keep non-responsive files merely to strengthen the evidentiary value of responsive files would eviscerate the Fourth Amendment.

9 Though the record is silent as to this point, the Government told the Court at rehearing *en banc* that it gave Ganias a copy of the forensic mirror image so that he could conduct his own analysis. *See* Oral Arg. 30:28-31:05.

Remarkably, the Government also argues that it should be allowed to hold on to overseized data for the *defendant's* benefit—so that it can comply with its discovery obligations and duty to disclose exculpatory materials under *Brady*. *See generally Brady v. Maryland* , 373 U.S. 83, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963). The Government is essentially arguing that it must hold on to the materials so that it can give them back to the defendant. Of course, this is not a genuine concern—the problem can be obviated simply by returning the non-responsive files to the defendant in the first place.

236 The Government further argues that it should be permitted to retain forensic mirror *236 images so that it may search the images for material responsive to a warrant "as the case evolves." Gov't Br. 35. At base, this is a blanket assertion that the Government can seize first and investigate later. *See CDT* , 579 F.3d at 998 (criticizing approach as: "Let's take everything back to the lab, have a good look around and see what we might stumble upon."). This is the equivalent of a general warrant, and the Fourth Amendment simply does not permit it.

Finally, the Government suggests that the availability of Federal Rule of Criminal Procedure 41(g) weighs in favor of the reasonableness of its actions. Rule 41(g) provides that a person aggrieved by an unlawful seizure "may move for the property's return." This rule, however, cannot shift the Government's burden under the Fourth Amendment onto the defendant. Pointing fingers at Ganias does not help the Government meet its *own* obligation to be reasonable.

The Government's arguments thus fail. In my view, Ganias's Fourth Amendment rights were violated when the Government unreasonably continued to hold on to his non-responsive files long after the responsive files had been extracted to reexamine when it subsequently saw need to do so.

II.

Instead of ruling on the question of whether the Government's actions violated the Fourth Amendment, the majority relies on the good faith exception to the exclusionary rule, and concludes that suppression was not warranted because the Government relied in good faith on the 2006 warrant and that this reliance was objectively reasonable. *See* Maj. Op. at 200.

A.

Even where a search or seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution. *United States v. Julius* , 610 F.3d 60, 66 (2d Cir. 2010). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States* , 555 U.S. 135, 144, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009).

To balance these interests, we have adopted the "good faith" exception, in certain circumstances, as a carve-out to the exclusionary rule. *See Davis v. United States* , 564 U.S. 229, 237–39, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011). When a warrant is present, an agent's objectively reasonable good faith reliance on and abidance by the warrant generally makes exclusion an inappropriate remedy. *See United States v. Leon* , 468 U.S. 897, 922, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984). Likewise, government agents act in good faith when they perform "searches conducted in objectively reasonable reliance on binding appellate precedent." *Davis* , 564 U.S. at 232, 131 S.Ct. 2419. When agents act in good faith, the exclusionary rule will usually not apply. *See United States v. Aguiar* , 737 F.3d 251, 259 (2d Cir. 2013). "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance." *United States v. Voustianiouk* , 685 F.3d 206, 215 (2d Cir. 2012) (quoting *United States v. George* , 975 F.2d 72, 77 (2d Cir. 1992)).

Furthermore, evidence will be suppressed only where the benefits of deterring the Government's unlawful
237 actions appreciably outweigh the costs of suppressing the evidence—"a high obstacle *237 for those urging ... application" of the rule. *Herring* , 555 U.S. at 141, 129 S.Ct. 695 (quoting *Pa. Bd. of Prob. & Parole v. Scott* , 524 U.S. 357, 364–65, 118 S.Ct. 2014, 141 L.Ed.2d 344 (1998)); *see Davis* , 564 U.S. at 232, 131 S.Ct. 2419. "When the police exhibit 'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Davis* , 564 U.S. at 238, 131 S.Ct. 2419 (quoting *Herring* , 555 U.S. at 144, 129 S.Ct. 695). "The principal cost of applying the [exclusionary] rule is, of course, letting guilty and possibly dangerous defendants go free—something that 'offends basic concepts of the criminal justice system.' " *Herring* , 555 U.S. at 141, 129 S.Ct. 695 (quoting *Leon* , 468 U.S. at 908, 104 S.Ct. 3405).

B.

The Government contends that it relied in good faith both on the 2003 warrant and the 2006 warrant. The majority, without supporting its holding with the 2003 warrant, concludes that the agents acted reasonably in relying on the 2006 warrant to search for evidence of Ganias's tax evasion, and that suppression therefore was not warranted. *See* Majority Op. at 219–23. I disagree, and would hold that neither warrant provided a good faith basis for retaining the non-responsive files long after the responsive files had been extracted.

(1)

I first turn to the 2003 warrant. The Government's retention of Ganias's non-responsive files pursuant to the 2003 warrant was hardly lawful or in good faith. The Government, in keeping the entirety of the mirror images, kept substantial amounts of "computer associated data" that did not "relat[e] to the business, financial and accounting operations of [IPM] and American Boiler." J. App. 433. This sort of retention following a "widespread seizure" was not explicitly authorized by the 2003 warrant, *United States v. Shi Yan Liu* , 239 F.3d 138, 140 (2d Cir. 2000) (quoting *United States v. Matias* , 836 F.2d 744, 748 (2d Cir. 1988)), and, as discussed, amounted to a general search. Likewise, the Government points to no binding appellate precedent that allows it to retain files outside the scope of a warrant when the responsive files can be feasibly extracted. Instead the Fourth Amendment baseline is that the Government may not take and then *keep* papers without a warrant "particularly describing ... the persons or things to be seized." U.S. Const. amend. IV.

The Government argues nonetheless that the agents had an objectively reasonable good faith belief that their post-warrant conduct was lawful, because no precedent held that they could *not* do what they did. The argument fails, in my view, for the precedents are absolutely clear that general warrants are unconstitutional and that government agents authorized to come into one's home to seize papers for a limited purpose may not indiscriminately seize and retain all papers instead. Any agent who professes to have the ability to do so merely because computers are involved is not acting in good faith.

Moreover, the Government's formulation of "the 'good faith' exception w[ould] swallow the exclusionary rule." *Davis* , 564 U.S. at 258, 131 S.Ct. 2419 (Breyer, *J.* , dissenting). The Government is essentially arguing that the absence of binding appellate precedent addressing the overseizure and retention of computer files excuses the agents' actions. But it has always been the case that agents must rely on *something* for their reliance
238 to be objective. That is, officers must "learn 'what is required of *238 them' ... and ... conform their conduct to these rules." *Davis* , 564 U.S. at 241, 131 S.Ct. 2419 (majority opinion) (quoting *Hudson v. Michigan* , 547 U.S. 586, 599, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006)); *see also id.* at 250, 131 S.Ct. 2419 (Sotomayor, *J.* , concurring) ("[W]hen police decide to conduct a search or seizure in the absence of case law (or other authority) specifically sanctioning such action, exclusion of the evidence obtained may deter Fourth Amendment violations...."). Here, the basic principles were well settled and provided ample guidance. And even if the warrant and our precedent were unclear as to what was allowed, the answer was not for agents to venture alone into uncharted constitutional territory. *See United States v. Johnson* , 457 U.S. 537, 561, 102 S.Ct. 2579, 73 L.Ed.2d 202 (1982) ("[I]n close cases, law enforcement officials would have little incentive to err on the side of constitutional behavior."). Rather, the answer was for the agents to seek out a magistrate to authorize the *continued retention* of Ganias's non-responsive files. *See CDT* , 621 F.3d at 1179 (Kozinski, *J.* , concurring). Once the responsive files were extracted, the Government could have asked to keep non-responsive files for use during a prosecution or for the purpose of trial and allowed a magistrate to balance the Government's need against Ganias's Fourth Amendment interests. *See Leon* , 468 U.S. at 916, 104 S.Ct. 3405 (noting we would not "punish the errors of judges and magistrates"). The Government did not do that, but instead retained the non-responsive files for another year and a half before seeking judicial guidance.

More troublingly, the agents here knew what they were supposed to do—their actions were "deliberate." *Davis* , 564 U.S. at 238, 131 S.Ct. 2419 (quoting *Herring* , 555 U.S. at 144, 129 S.Ct. 695). The agents *knew* they were supposed to return or delete overseized data. When asked whether he was "to return those items or destroy those items that don't pertain to your lawful authority to seize those particular items" after a "reasonable period" of off-site review, the testifying agent answered, "Yes, sir." J. App. 145-46; *see also id.* at 428 (Ganias corroborating that the agent "assured me that those materials and files not authorized under the warrant and not belonging to American Boiler and IPM would be purged once they completed their search"). Instead of following this protocol, that agent testified that the investigators "viewed the data as the government's property, not Mr. Ganias' property." *Id.* at 146; *see also id.* at 122 ("And you never know what data you may need in the future."). In other words, the agents "knew that limits of the warrant w[ere] not be[ing] honored." *United States v. Foster* , 100 F.3d 846, 852 (10th Cir. 1996). This knowledge of the need to return or delete non-responsive files compels a conclusion that the agents did not rely in good faith on the 2003 warrant or any appellate precedent (binding or non-binding) and that the deterrence value of suppression here is substantial.

(2)

I next turn to the 2006 warrant. On April 24, 2006, the Government sought a warrant—seeking to search "Images of three (3) hard drives seized on November 19, 2003 from the offices of Steve M. Ganias"—to investigate him personally. J. App. 455. A magistrate judge issued the warrant, and the Government searched the mirror images.

For the purpose of deterring Fourth Amendment violations, the relevant inquiry is whether the agents acted in good faith when they committed the violation. *See Leon* , 468 U.S. at 916, 104 S.Ct. 3405 ("[T]he exclusionary
239 rule is designed to *239 deter police misconduct...."). The agents here could not have relied in good faith on the 2006 warrant because it was issued almost two-and-a-half years after the files were first overseized, and some sixteen months after the responsive files had been extracted. That is, the agents did not rely on the 2006 warrant to retain non-responsive files because that warrant came into being only *after* the Fourth Amendment violation occurred. An agent can only rely on something that exists "at the time of the search." *Aguiar* , 737 F.3d at 259 ; *see Davis* , 131 S.Ct. at 2418 (asking if search was in "objectively reasonable reliance on binding judicial precedent" as of "the time of the search").

In other words, the later 2006 warrant could not cure the prior illegal retention of Ganias's data when agents did not rely on it to retain that data. A warrant is not a Band-Aid that the Government may seek when it realizes its Fourth Amendment violation has been discovered. *See* Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 1.3(f) (5th ed. 2015) ("When the magistrate issued the warrant, he did not endorse past activity; he only authorized future activity."). As we have previously held, "Good faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly* , 76 F.3d 1271, 1280 (2d Cir. 1996).

The Government and the majority rely on a line of cases that includes *United States v. Reilly* , 76 F.3d 1271, and its predecessor, *United States v. Thomas* , 757 F.2d 1359 (2d Cir. 1985). In *Reilly*, we affirmed the *Thomas* principle that illegally obtained evidence need not be excluded where the agents later obtained a warrant by providing a magistrate "the details of their dubious pre-warrant conduct" and where " 'there was nothing more the officer could have or should have done under the[ ] circumstances to be sure his search would be legal.' "

Reilly , 76 F.3d at 1282 (alterations omitted) (quoting *Thomas* , 757 F.2d at 1368). We required, however, that the officer "did not have any significant reason to believe that what he had done was unconstitutional." *Id.* at 1281.[10]

10 As an initial observation, the *Thomas* principle is not free from doubt. *Reilly* acknowledged that *Thomas* is difficult to square with the holdings of many of our sister circuits without attempting to reconcile conflicting case law. *See id.* at 1282 ("Other courts have criticized *Thomas*...."); *e.g.* , *United States v. McGough* , 412 F.3d 1232, 1240 (11th Cir. 2005) ; *United States v. O'Neal* , 17 F.3d 239, 243 (8th Cir. 1994) ; *United States v. Scales* , 903 F.2d 765, 768 (10th Cir. 1990) ; *United States v. Vasey* , 834 F.2d 782, 789 (9th Cir. 1987). Indeed, the language that exclusion may be avoided when the Government "did not have any significant reason to believe that what [it] had done was unconstitutional," *Reilly* , 76 F.3d at 1282, may one day prove to be too lax.

In this case, the agents did *not* present to the magistrate judge all of "the details of their dubious pre-warrant conduct." *Id.* at 1282. Though the majority points out that the agents disclosed to the magistrate judge in 2006 that the mirror images were seized in November 2003, that Ganias was not then under investigation, and that the mirror images included files outside the scope of the original warrant, this information was not sufficient on its own to permit the magistrate judge to evaluate whether the relevant constitutional violation occurred. *See* Maj. Op. at 224. The agents did not disclose that they had segregated responsive files from non-responsive files and extracted the responsive files and that for some time they did not have other, anticipated uses for the non-responsive files. Without this information relating to whether the Government still had a legitimate use for the
240 mirror image during the retention, it simply would not have been *240 feasible for a magistrate judge to consider the legitimacy of the continued retention of the mirror image. *See United States v. Vasey* , 834 F.2d 782, 789 (9th Cir. 1987) ("Typically, warrant applications are requested and authorized under severe time constraints.").

Likewise, unlike in *Thomas*, there was more that the Government could have done prior to 2006 to ensure that its conduct was legal. *See Thomas* , 757 F.2d at 1368. As noted above, it could have gone to a magistrate judge much earlier for permission to retain the non-responsive computer files.

Finally, the Government *did* have significant reason to believe that its conduct was unconstitutional. As noted, an agent testified that he knew he was supposed to "return those items or destroy those items that d[idn't] pertain to [his] lawful authority to seize those particular items." J. App. 145-46. And any reasonable law enforcement agent would have understood that it was unreasonable to "view[ ] [private property] as the government's property" or to treat the 2003 warrant as a general warrant. *Id.* at 146. Furthermore, the language of the 2003 warrant clearly set parameters for what was lawful: only data "relating to" IPM and American Boiler could be kept. *Id.* at 433.

At bottom, in holding that the Government acted with objectively reasonable reliance on the 2006 warrant, the majority condones creative uses of government power to interfere with individuals' possessory interests and to invade their privacy. Without specifically opining on whether the Government can retain overseized, non-responsive files, the majority has crafted a formula for the Government to do just that. The Government only needs to: obtain a warrant to seize computer data, overseize by claiming files are intermingled (they always will be), keep overseized data until the however distant future, and then (when probable cause one day develops)

ask for another warrant to search what it has kept. The rule that we have fashioned does nothing to deter the Government from continually retaining papers that are, though initially properly seized, not responsive to or particularly described in a warrant. Instead of deterring future violations, we have effectively endorsed them.

The Government bears the burden of proving "the objective reasonableness of the officers' good faith reliance." *Voustianiouk* , 685 F.3d at 215 (quoting *George* , 975 F.2d at 77). It has not met that burden here. To the contrary, the agents exhibited a deliberate or reckless or grossly negligent disregard for Ganias's rights, *see Davis* , 564 U.S. at 238, 131 S.Ct. 2419, and, in my view, the benefits of deterring the Government's unlawful actions here appreciably outweigh the costs of suppression, *see Herring* , 555 U.S. at 141, 129 S.Ct. 695 ; *see also Davis* , 564 U.S. at 232, 131 S.Ct. 2419 ; *Pa. Bd. of Prob. & Parole* , 524 U.S. at 364–65, 118 S.Ct. 2014.

III.

In the discussion of lofty constitutional principles, we sometimes forget the impact that our rulings and proceedings may have on individuals and their families. Here, there has been a cloud hanging over Ganias's head for nearly thirteen years, impacting every aspect of his life and the lives of those around him. The cloud is still there now.

The wheels of justice have spun ever so slowly in this case. The Government seized Ganias's files in November 2003, nearly thirteen years ago. He was indicted, in 2008, some eight years ago. He waited two-and-a-half
241 years for a trial, and after he was found guilty, he waited roughly *241 another ten months to be sentenced. He appealed his conviction, but it took another year for his appeal to be heard, and then another year for the appeal to be decided.

The panel issued its decision on June 17, 2014. The panel held that the Government violated Ganias's Fourth Amendment rights and rejected its reliance on the good faith exception. On August 15, 2014, the Government filed a petition for rehearing, seeking panel rehearing only, not rehearing *en banc* , and seeking rehearing only with respect to the good faith exception. In other words, the Government did not seek rehearing on whether the Fourth Amendment was violated, and it did not seek rehearing *en banc* on either issue.

Yet, on June 29, 2015, more than a year after the panel decision, more than a year after Ganias thought he had won a substantial victory, this Court, on its own initiative, elected to rehear the case *en banc* —with respect to *both* issues. The Court did so ostensibly to provide guidance in a novel and difficult area of law. But, after a year-long *en banc* process, no guidance has come forth. The Court took on an issue at Ganias's expense and then quickly retreated, relying instead on an issue that was not worthy of *en banc* review.

Ganias's non-responsive files are in the Government's custody still. What began nearly thirteen years ago as an investigation by the Army into two of Ganias's business clients somehow evolved into an unrelated investigation by the IRS into Ganias's personal affairs, largely because the Government did precisely what the Fourth Amendment forbids: it entered Ganias's premises with a warrant to seize certain papers and indiscriminately seized—and *retained* —all papers instead.

I respectfully dissent.

Appendix A

Amici Curiae

Alan R. Friedman (*counsel of record*), Samantha V. Ettari, Noah Hertz–Bunzl, Kramer Levin Naftalis & Frankel LLP, New York, NY, *for Amicus Curiae the Center for Constitutional Rights, in support of Defendant–Appellant* .

Tanya L. Forsheit, Baker & Hostetler LLP, Los Angeles, CA, and William W. Hellmuth, Baker & Hostetler LLP, Washington, DC (*representing Amicus Curiae Center for Democracy & Technology*); Alex Abdo, Nathan Freed Wessler, Jason D. Williamson, American Civil Liberties Union Foundation, New York, NY; Dan Barrett, American Civil Liberties Union of Connecticut, Hartford, CT; Faiza Patel, Brennan Center for Justice at NYU School of Law, New York, NY; Hanni Fakhoury, Electronic Frontier Foundation, San Francisco, CA; Laura M. Moy, Open Technology Institute/New America, Washington, DC, *for Amici Curiae Center for Democracy & Technology, American Civil Liberties Union, American Civil Liberties Union of Connecticut, Brennan Center for Justice at NYU School of Law, Electronic Frontier Foundation, and New America's Open Technology Institution, in support of Defendant–Appellant.*

Marc Rotenberg (*counsel of record*), Alan Butler, Electronic Privacy Information Center, Washington, DC, *for Amicus Curiae Electronic Privacy Information Center, in support of Defendant–Appellant* .

Colleen P. Cassidy (*of counsel*), Federal Defenders of New York, Inc., Southern District of New York, New York, NY; James Egan, Office of the Federal Public Defender, Northern District of New York, Syracuse, NY, *for Amicus Curiae Federal Public Defenders Within the*

242 *242

Second Circuit, in support of Defendant–Appellant .

Todd M. Hinnen, Perkins Coie LLP, Seattle, WA, and Amanda Andrade, Perkins Coie LLP, Washington, DC, *for Amicus Curiae Google Inc., in support of Defendant–Appellant.*

Miranda E. Fritz, Eli B. Richlin, Thompson Hine LLP, New York, NY; Richard D. Willstatter, Green & Willstatter, White Plains, NY; Joel B. Rudin, Law Offices of Joel B. Rudin, P.C., New York, NY, *for Amicus Curiae National Association of Criminal Defense Lawyers, in support of Defendant–Appellant* .

Michael L. Yaeger, Barry A. Bohrer, Schulte Roth & Zabel LLP, New York, NY, *for Amicus Curiae New York Council of Defense Lawyers, in support of Defendant–Appellant* .

Mahesha P. Subbaraman, Subbaraman PLLC, Minneapolis, MN, *for Amicus Curiae Restore the Fourth, Inc., in support of Defendant–Appellant.*

436 F.Supp.3d 707
United States District Court, S.D. New York.

UNITED STATES of America,
v.
Ali Sadr Hashemi NEJAD, Defendant.

18-cr-224 (AJN)
|
Signed 01/28/2020

Synopsis

Background: Defendant was charged with violating the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR), arising from payments allegedly routed from a Venezuelan state-owned energy company through banks in the United States to Swiss accounts of entities owned by defendant and his family. Defendant moved for a *Franks* hearing and for the suppression of search warrant evidence, moved for return of property, and moved to exclude certain documents.

Holdings: The District Court, Alison J. Nathan, J., held that:

[1] defendant's memorandum of law failed to make a substantial showing of credible and probative evidence that the alleged misstatements in affidavit in support of search warrant were designed to mislead;

[2] defendant failed to make any showing, let alone a substantial showing, that alleged omissions in affidavit in support of search warrant were designed to mislead or were made with reckless disregard for whether they would mislead issuing court;

[3] even if challenged allegations were excised from affidavit, affidavit's remaining allegations established probable cause to believe that defendant was engaged in a complex scheme designed to evade U.S. sanctions;

[4] search warrants for defendant's e-mail accounts were sufficiently particular;

[5] even assuming the search warrants for defendant's e-mail accounts were invalid, the good-faith exception to the exclusionary rule applied;

[6] responsiveness review of documents government found in defendant's e-mail accounts for documents that fell within the scope of search warrants was conducted reasonably and within the confines of the Fourth Amendment; and

[7] seizure of documents from searches conducted within data pulled by search warrants of defendant's e-mail after the responsiveness review had concluded violated the Fourth Amendment.

Ordered accordingly.

See also: 2020 WL 429422, 2019 WL 6702361.

Procedural Posture(s): Pre-Trial Hearing Motion.

West Headnotes (56)

[1] **Searches and Seizures** Probable or Reasonable Cause

Searches and Seizures Particularity or generality and overbreadth in general

A warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity. U.S. Const. Amend. 4.

[2] **Searches and Seizures** Probable or Reasonable Cause

In evaluating probable cause in any given case, a judge must make a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place. U.S. Const. Amend. 4.

[3] **Searches and Seizures** Scope of inquiry or review, in general

Due to the subjective standard used to evaluate whether probable cause exists in a given case, a reviewing court generally accords substantial deference to the finding of an issuing judicial officer that probable cause exists, limiting the inquiry to whether the officer had a substantial basis for his determination. U.S. Const. Amend. 4.

[4] **Searches and Seizures** Scope of inquiry or review, in general

A court may properly conclude that a warrant was invalid because the judge's probable-cause determination reflected an improper analysis of the totality of circumstances. U.S. Const. Amend. 4.

[5] **Searches and Seizures** In general; conclusiveness of warrant in general

Searches and Seizures Hearing; in camera inspection

Although a search or seizure pursuant to a warrant is presumed valid, a defendant may, in certain circumstances, challenge the truthfulness of factual statements made in the affidavit, and thereby undermine the validity of the warrant and the resulting search or seizure.

1 Cases that cite this headnote

[6] **Searches and Seizures** Hearing; in camera inspection

To obtain a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a search warrant affidavit, a defendant must make a substantial preliminary showing that (1) there were intentional misrepresentations or omissions in the warrant affidavit, or, in other words the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth, and (2) those misrepresentations or omissions were material, or necessary to the issuing judge's probable cause finding. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[7] **Searches and Seizures** Hearing; in camera inspection

To satisfy the test to obtain a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit, a defendant must point out specifically the portion of the warrant affidavit that is claimed to be false. U.S. Const. Amend. 4.

[8] **Searches and Seizures** Hearing; in camera inspection

With respect to the intentionality prong of the test for obtaining a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit, the reviewing court must be presented with credible and probative evidence that a misstatement or omission in a warrant application was designed to mislead or was made in reckless disregard of whether it would mislead. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[9] **Searches and Seizures** Hearing; in camera inspection

For purposes of obtaining a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit, reckless disregard for the truth may be established by demonstrating that an affiant made statements which failed to take account of the facts as he knew them, or which he seriously doubted were true. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[10] **Searches and Seizures** Hearing; in camera inspection

Where omissions are concerned, for purposes of obtaining a *Franks* hearing on a motion to suppress on the basis of alleged omissions in a warrant affidavit, recklessness may be inferred where the omitted information was clearly critical to the probable cause determination, however, such an inference is not to be automatically drawn simply because a reasonable person would have included the omitted information, and the inference is particularly inappropriate where the government comes forward with evidence indicating that the omission resulted from nothing more than negligence, or that the omission was the result of a considered and reasonable judgment that the information was not necessary to the warrant application. U.S. Const. Amend. 4.

[11] **Searches and Seizures** Hearing; in camera inspection

With respect to the materiality prong in the test for determining whether *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit was required, courts gauge materiality by a process of subtraction or addition depending on whether misstatements or omissions are at issue. U.S. Const. Amend. 4.

[12] **Searches and Seizures** Hearing; in camera inspection

To determine materiality element of test for obtaining a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit, courts should disregard the allegedly false statements, insert the omitted truths, and determine whether there remains a residue of independent and lawful information sufficient to support probable cause; if, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a *Franks* hearing. U.S. Const. Amend. 4.

[13] **Searches and Seizures** Hearing; in camera inspection

The *Franks* standard for invalidating a warrant due to alleged misstatements or omissions in a warrant affidavit is a high one; to be entitled to a hearing under this standard, a defendant must make a substantial preliminary showing of each of the prongs. U.S. Const. Amend. 4.

[14] **Searches and Seizures** Hearing; in camera inspection

The substantial preliminary showing to obtain a *Franks* hearing, challenging a search warrant on the basis of alleged misstatements or omissions in a warrant affidavit, must consist of specific allegations accompanied by an offer of proof, unsupported conclusory allegations of falsehood or material omission cannot support a *Franks* challenge. U.S. Const. Amend. 4.

[15] **Searches and Seizures** Hearing; in camera inspection

Reckless disregard for the truth, for purposes of obtaining a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit cannot be inferred unless circumstances evince obvious reasons to doubt the veracity of the allegedly misstated information. U.S. Const. Amend. 4.

[16] **Searches and Seizures** Factual showing, in general

An affiant cannot be expected to include in an affidavit in support of a search warrant every piece of information gathered in the course of an investigation. U.S. Const. Amend. 4.

[17] **Searches and Seizures** False, inaccurate or perjured information; disclosure

Searches and Seizures Hearing; in camera inspection

Defendant's memorandum of law in support of request for *Franks* hearing failed to make a substantial showing of credible and probative evidence that the alleged misstatements in affidavit in support of search warrant were designed to mislead, for purposes of determining whether a *Franks* hearing was required to determine whether warrant was valid; alleged lack of further support or evidence for an allegation did not constitute an obvious reason to doubt the veracity of that allegation, suggestion that falsity of allegation itself constituted an obvious reason to doubt its veracity was circular reasoning, and fact that alleged misstatements appeared in earlier warrant affidavits but were excised from later warrant affidavits demonstrated a willingness of affiant to strike the allegations. U.S. Const. Amend. 4.

[18] **Searches and Seizures** False, inaccurate or perjured information; disclosure

Searches and Seizures Hearing; in camera inspection

Defendant failed to make any showing, let alone a substantial showing, that alleged omissions in affidavit in support of search warrant for defendant's email accounts for evidence of involvement in money laundering, offering a false instrument for filing, or falsifying business records were designed to mislead or were made with reckless disregard for whether they would mislead the issuing court, for purposes of determining whether a *Franks* hearing was warranted. U.S. Const. Amend. 4.

[19] **Searches and Seizures** False, inaccurate or perjured information; disclosure

Searches and Seizures Hearing; in camera inspection

To determine if misrepresentations or omissions in affidavit in support of a search warrant are material for purposes of obtaining a *Franks* hearing, a court corrects the errors and then resolves de novo whether the hypothetical corrected affidavit still establishes probable cause. U.S. Const. Amend. 4.

[20] **Searches and Seizures** Particular concrete applications

Even if challenged allegations were excised from affidavit in support in support of search warrant for defendant's e-mail accounts, affidavit's remaining allegations established probable cause to believe that defendant was engaged in a complex scheme designed to evade U.S. sanctions and that business records were falsified or false instruments were offered for filing as part of this complex scheme, and therefore all challenged allegations were not material for purposes of defendant obtaining a *Franks* hearing; affidavit alleged, amongst other things, that contract provided that payments for project-related transactions would be made in U.S. dollars and that payments in favor of corporation owned by defendant's family were to be made through a U.S. bank to defendant's Swiss bank account. U.S. Const. Amend. 4.

[21] **Searches and Seizures** Hearing; in camera inspection

On a request for a *Franks* hearing, a defendant must point out specifically all portions of the warrant affidavit he claims to be

false; this is necessary to allow the court to gauge materiality, which involves deleting any alleged misstatements from the original warrant affidavit, adding to it any relevant omitted information, and determining whether probable cause still exists after such a correction. U.S. Const. Amend. 4.

[22] **Searches and Seizures** Objects or information sought

A warrant can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries. U.S. Const. Amend. 4.

[23] **Searches and Seizures** Particularity or generality and overbreadth in general

The Fourth Amendment's particularity requirement targets the specific evil of the general warrant abhorred by the colonists, and is thus meant to prevent the general, exploratory rummaging in a person's belongings that such general warrants allowed. U.S. Const. Amend. 4.

[24] **Searches and Seizures** Objects or information sought

A sufficiently particular warrant under the Fourth Amendment is one that enables the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize. U.S. Const. Amend. 4.

[25] **Searches and Seizures** Particularity or generality and overbreadth in general

To be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements: (1) a warrant must identify the specific offense for which the police have established probable cause, (2) a warrant must describe the place to be searched, and (3) the warrant must specify the items to be seized by their relation to designated crimes. U.S. Const. Amend. 4.

[26] **Searches and Seizures** Objects or information sought

A warrant is overbroad under the Fourth Amendment if its description of the objects to be seized is broader than can be justified by the probable cause upon which the warrant is based. U.S. Const. Amend. 4.

[27] **Searches and Seizures** Particularity or generality and overbreadth in general

Breadth and particularity are related but distinct concepts when analyzing a search warrant under the Fourth Amendment, the two are related in that a warrant's unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause, however, they are distinct in that a broad warrant does not necessarily lack particularity: a warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without necessarily violating the particularity requirement. U.S. Const. Amend. 4.

[28] **Searches and Seizures** Particularity or generality and overbreadth in general

In determining whether a warrant is overbroad, courts must focus on whether there exists probable cause to support the breadth of the search that was authorized. U.S. Const. Amend. 4.

[29] **Searches and Seizures** Particularity or generality and overbreadth in general

Search warrants for defendant's e-mail accounts for evidence of involvement in money laundering, offering a false instrument for filing, or falsifying business records, were sufficiently particular under Fourth Amendment; although warrants did not reference suspected crimes within paragraphs authorizing seizure and allowed for an initial seizure of all e-mails in the target accounts; warrants identified specific offenses for which police established probable cause, described places to be searched, and specified items to be seized by their relation to designated crimes, and affiant noted that personal e-mails were frequently used to transmit messages and documents amongst individuals involved in projects at issue. U.S. Const. Amend. 4.

[30] **Searches and Seizures** Objects or information sought

There is no settled formula for determining whether a warrant lacks particularity, rather a warrant must be sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize. U.S. Const. Amend. 4.

[31] **Searches and Seizures** Objects or information sought

A warrant is lacking in particularity if it leaves to the unguided discretion of the officers executing the warrant the decision as to what items may be seized. U.S. Const. Amend. 4.

[32] **Searches and Seizures** Particularity or generality and overbreadth in general

Generic terms may be used in a search warrant so long as the warrant identifies a specific illegal activity to which the item sought related. U.S. Const. Amend. 4.

[33] **Searches and Seizures** Particularity or generality and overbreadth in general

The type of evidence sought is relevant to the level of specificity the Fourth Amendment requires in a search warrant affidavit. U.S. Const. Amend. 4.

[34] **Searches and Seizures** Particularity or generality and overbreadth in general

A temporal limitation is one indicia of particularity for a search warrant under Fourth Amendment. U.S. Const. Amend. 4.

[35] **Searches and Seizures** Objects or information sought

A warrant is overbroad if its description of the objects to be seized is broader than can be justified by the probable cause upon which the warrant is based. U.S. Const. Amend. 4.

[36] **Criminal Law** Searches, seizures, and arrests

A violation of the Fourth Amendment does not necessarily result in the application of the exclusionary rule. U.S. Const. Amend. 4.

[37] **Criminal Law** Searches, seizures, and arrests

Criminal Law Exclusionary rule as a personal or individual right

The exclusionary rule is not a personal constitutional right of the party aggrieved, but rather is a judicially created rule designed to safeguard Fourth Amendment rights generally through its deterrent effect. U.S. Const. Amend. 4.

[38] **Criminal Law** Exclusionary Rule in General

In order for the exclusionary rule to apply, the benefits of deterrence must outweigh the often substantial social costs of letting guilty and possibly dangerous defendants go free.

[39] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Good-faith exception to the exclusionary rule allows the government to introduce evidence obtained in violation of the Fourth Amendment unless the police conduct was sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system. U.S. Const. Amend. 4.

[40] **Criminal Law** Searches, seizures, and arrests

Criminal Law Good Faith or Objectively Reasonable Conduct Doctrine

The deterrence benefits of exclusion will naturally vary with the culpability of the law enforcement conduct at issue, when the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs, conversely, when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force. U.S. Const. Amend. 4.

[41] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

Under the good-faith exception to the exclusionary rule, the pertinent analysis of deterrence and culpability is objective and the court's good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances. U.S. Const. Amend. 4.

[42] **Criminal Law** Exceptions Relating to Defects in Warrant

Good-faith exception to the exclusionary rule applies when the government acts in objectively reasonable reliance on a subsequently invalidated search warrant. U.S. Const. Amend. 4.

[43] **Criminal Law** Exceptions Relating to Defects in Warrant

Good faith exception to the exclusionary rule does not apply (1) where the issuing magistrate has been knowingly misled, (2) where the issuing magistrate wholly abandoned his or her judicial role, (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable, and (4) where the warrant is so facially deficient that reliance upon it is unreasonable. U.S. Const. Amend. 4.

[44] **Criminal Law** Particular cases

Even assuming the search warrants for defendant's e-mail accounts for evidence of involvement in money laundering, offering a false instrument for filing, or falsifying business records were invalid, the good-faith exception to the exclusionary rule applied, where the government acted in objectively reasonable reliance on them, the judge was not misled, there was no suggestion that the issuing judge had wholly abandoned his judicial role in granting the search warrant applications, there was no consensus in the circuit as to when temporal limitations in a search warrant were required or when the lack thereof alone may invalidate an otherwise valid search warrant, and the warrants

were not so facially deficient that reliance upon them was unreasonable. U.S. Const. Amend. 4.

[45] **Criminal Law** Good Faith or Objectively Reasonable Conduct Doctrine

For purposes of application of the good faith exception to the exclusionary rule, the standard of reasonableness in the context of suppression of evidence mirrors that in the context of qualified immunity.

[46] **Criminal Law** Exceptions Relating to Defects in Warrant

Where denial of qualified immunity would be appropriate in the civil context because clearly established law establishes a warrant's invalidity, so too must a court conclude that an officer's conduct was objectively unreasonable for purposes of the good faith inquiry under exception to the exclusionary rule.

[47] **Searches and Seizures** Execution and Return of Warrants

The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant. U.S. Const. Amend. 4.

[48] **Searches and Seizures** Scope of Search

A search must be confined to the terms and limitations of the warrant authorizing it. U.S. Const. Amend. 4.

2 Cases that cite this headnote

[49] **Criminal Law** Execution and return of warrant

Searches and Seizures Disposition of property seized

When items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items. U.S. Const. Amend. 4.

[50] **Searches and Seizures** Scope of Search

The retention of items outside the scope of the warrant can be justified only if the government meets its burden of demonstrating that those items fall within an exception to the warrant requirement. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[51] **Criminal Law** Execution and return of warrant

The drastic remedy of the suppression of all evidence seized is not justified unless those executing the warrant acted in flagrant disregard of the warrant's terms; executing agents are considered to have flagrantly disregarded the warrant's terms where (1) they effect a widespread seizure of items that were not within the scope of the warrant and (2) do not act in good faith. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[52] **Criminal Law** Execution and return of warrant

The extreme remedy of blanket suppression of all evidence seized pursuant to warrant should only be imposed in the most extraordinary of cases. U.S. Const. Amend. 4.

[53] **Searches and Seizures** Places, persons, and things within scope of warrant

Responsiveness review of documents government found in defendant's e-mail accounts for documents that fell within the scope of search warrants was conducted reasonably and within the confines of the Fourth Amendment, even though the reviewers did not agree on a comprehensive set of search terms

or consistently remove documents tagged as responsive from the review population, the review took approximately three years from first search warrant, and irrelevant documents were labeled responsive; reviewers were district attorney employees who in many instances were quite familiar with the investigation and had met and discussed the review of the search warrant returns, and the search warrants returned over one million documents in three different languages. U.S. Const. Amend. 4; Fed. R. Crim. P. 41(e)(2)(B).

1 Cases that cite this headnote

[54] **Searches and Seizures** Places, persons, and things within scope of warrant

Responsiveness review of documents found pursuant to a search warrant must be completed in a reasonable amount of time to comply with the Fourth Amendment and rule governing search and seizure requirements governing the execution of search warrants. U.S. Const. Amend. 4; Fed. R. Crim. P. 41.

[55] **Criminal Law** Motions

Defendant's request to suppress certain documents in prosecution for violations of the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR) was moot, where government represented that it would not use the documents at trial. 50 U.S.C.A. § 1701 et seq.

[56] **Searches and Seizures** Places, persons, and things within scope of warrant

Seizure of documents from searches conducted within data pulled by search warrants of defendant's e-mail after the responsiveness review had concluded violated the Fourth Amendment, where searches were conducted following the conclusion of the responsiveness review and thus the execution of the search warrants, exceeding the scope of the warrants' authority. U.S. Const. Amend. 4.

Attorneys and Law Firms

***714** Andrew James DeFilippis, Jane Kim, Michael Kim Krouse, Rebekah Allen Donaleski, Stephanie Lindsay Lake, David William Denton, Jr., United States Attorney's Office, Matthew Joseph Laroche, Assistant U.S. Attorney, New York, NY, for United States of America.

Brian Matthew Heberlig, Bruce C. Bishop, David Matthew Fragale, Nicholas Paul Silverman, Steptoe & Johnson, LLP, Washington, DC, Michelle Lynn Levin, Reid Weingarten, Steptoe & Johnson, LLP, New York, NY, for Defendants

OPINION & ORDER

ALISON J. NATHAN, District Judge:

***715** Defendant Ali Sadr Hashemi Nejad is charged in a six-count Indictment. Dkt. No. 2. Before the Court are Sadr's motion for a *Franks* hearing and for suppression of search warrant evidence, motion for return of property, and motion to exclude. For the reasons that follow, the Court GRANTS in part, DENIES in part, and RESERVES JUDGMENT in part on Sadr's motion to suppress search warrant evidence, DENIES his corollary requests for a *Franks* hearing, RESERVES JUDGMENT on his motion for return of property, and DENIES as moot his motion to exclude.

I. BACKGROUND

A. Factual Background

The Court assumes familiarity with the factual background in this matter as set forth in its December 6, 2019 Opinion and Order deciding Sadr's first seven pretrial motions. *See* Dkt. No. 164. In brief, the Indictment alleges that an Iranian-incorporated entity controlled by Sadr and his family was involved in a housing construction project in Venezuela. Ind. ¶ 8. The charges in the Indictment stem from payments

for the construction of low-income housing in Venezuela that were allegedly routed from a Venezuelan state-owned energy company through banks in the United States to the Swiss accounts of entities owned by Sadr and his family. *See id.* ¶¶ 11–13. The Government alleges that this transaction structure violated the International Emergency Economic Powers Act ("IEEPA") and the Iranian Transactions and Sanctions Regulations ("ITSR"). [1]

B. Procedural Background

This case originated as an investigation by the New York County District Attorney's Office. On April 16, 2014, June 16, 2014, and October 21, 2015, the DA's Office obtained search warrants from the Honorable Michael Obus, a justice of the New York County Supreme Court, to search certain of Sadr's email accounts for evidence of involvement in money laundering, offering a false instrument for filing, or falsifying business records. *See* Dkt. 108 at 56–59; *see also* Dkt. 96-1–4. These search warrants generally provide that "there is reasonable and probable cause to believe that certain property, evidence, and records" exists including

> any and all subscriber and account information and history, and retained account data, for [the target] email accounts, any associated or linked accounts, including: payment history, detailed billing information, method of payment, including full debit, credit, or bank account numbers used, Contacts or "Buddy List" content, sent and received email messages that are or were in the account, saved or draft email messages, any files attached to any email messages, Internet Protocol ("IP") log history, connection log data, account creation data, passwords, sign-on codes, account numbers, and any other information maintained by or within the databases of the service provider and related entities regarding the named email account and subscriber and any linked email accounts and subscribers, *which shows or tends to show the following*:
>
> ...
>
> • *involvement in Money Laundering, Offering a False Instrument for Filing, Falsifying Business Records*, and an attempt and conspiracy to commit said crimes, and/or involvement in the planning of, recruiting for, or commission of those crimes; communication with witnesses to and victims of the above-named crimes; communication with third parties relating to witnesses to and victims of the above-named crimes; and communication with third parties while using aliases or other identities.

See, e.g., Dkt. No. 96-1 at 37 (emphasis added). They further authorize executing agents

> to search, enter, retrieve, examine, copy, and analyze the ... servers and ... accounts associated with target email address ... from the time period of the inception of the target email account to the date of the warrant, for any and all payment history, detailed billing information, method of payment and credit card numbers used, contacts, sent and received email messages that are or were in the account, saved or draft email messages, any files attached to such email messages, basic subscriber and account information, and Internet Protocol ("IP") log history ...

Id. at 38.

In response to these search warrants and others, internet service providers provided the D.A. with data consisting of over one million documents from various email accounts —including both Sadr's and others' accounts—which were processed by it on a rolling basis. Dkt. No. 155 at 4. In order to process this data, D.A. employees began in May 2014 to search it for material to be seized pursuant to the search warrants. *Id.* at 5. During this responsiveness review, they seized certain documents identified as responsive to the search warrants. *Id.* at 6. By April 2017, the responsiveness review was complete. *Id.* at 3–7.

At the conclusion of the responsiveness review, the D.A. referred the case to the United States Attorney's Office for the Southern District of New York for federal prosecution and provided the U.S. Attorney's Office with a binder of 420 seized documents at that time. *Id.* at 8. Between the time the case was referred to the U.S. Attorney's Office and the

Indictment was filed, D.A. employees continued to access the entire set of data—beyond just previously seized documents—in order to "pull complete versions of [previously] seized documents" and to query the data "for purposes of preparing materials related to the Indictment." *Id.* These employees were given instructions to "(1) locate specific documents that were responsive to the search warrants—which [members of the review team] ha[d] seen when conducting earlier searches, or (2) query the [entire set of data] regarding topics for which more experienced members of the investigative team had previously seen responsive documents." *Id.*

On March 19, 2019, the Indictment in this case was returned, and on March 28, 2018, Sadr arrived in the Southern District of New York following his arrest in Virginia. *Id.* at 9. From April to May 2018, the U.S. Attorney's Office produced to Sadr, among other things, all of the data from his own email accounts as well as the 420 seized documents the D.A. provided the U.S. Attorney's Office with when it made the referral. *Id.* During the process of producing these documents, D.A. employees again accessed the entire set of data in some instances to, in its words, pull "complete versions" of the 420 documents. *Id.*

In May 2018, the U.S. Attorney's Office requested that the D.A. provide it with information related to Sadr's travel to or from Iran for the purposes of opposing his bail application. *Id.* In response, the D.A. again accessed the entire set of data and ***717** seized some documents that had not previously been seized. *Id.* at 9–10.

In May 2019, the U.S. Attorney's Office learned that the D.A. had seized documents beyond the 420 that were produced to Sadr in May 2018, and that some of these seized materials had not previously been produced to Sadr. *Id.* at 10–11. Ultimately, 622 documents—all from non-Sadr email accounts—were identified that had not previously been provided to Sadr. *Id.* at 11. On September 17, 2019, the Government produced these 622 non-Sadr documents, as well as 1,775 documents seized from Sadr's accounts that had previously been produced to him in April 2018 but were not then identified to him as having been seized. *Id.* at 2, 11.

On February 25, 2019, Sadr filed nine pretrial motions, including the motion for a *Franks* hearing and for suppression of search warrant evidence and the motion for return of property now before the Court. *See* Dkt. Nos. 95, 97. At a conference before the Court on September 9, 2019, the Government revealed to Sadr for the first time the information it had learned back in May: that "there were custodians searched and documents seized that were not Mr. Sadr's accounts, that were not produced in [the] initial Rule 16 discovery"—namely, the 622 documents identified above. Dkt. No. 137 at 35:5–7. Following that revelation, Sadr informed the Court of his intention to supplement his existing motions to suppress and for return of property and to file an additional motion to exclude the 622 late-disclosed documents from the non-Sadr accounts. Dkt. No. 143 at 2.

In its supplemental opposition to the motions now before the Court, the Government represents that it will use neither the 622 non-Sadr documents nor the 1,775 Sadr documents identified above in its case-in-chief. Dkt. No. 155 at 11. The Government further clarified, at oral argument on these motions on November 25, 2019, that it will not rely on these documents at *any* point in trial—whether in its case-in-chief, on cross-examination, or in its rebuttal case—and will thus limit itself to only the 420 documents produced to Sadr in May 2018. *See* Dkt. No. 173 at 38:24–39:4.

At that argument, the Court inquired whether the 420 documents the Government now represents it will exclusively rely on at trial were in fact all identified as responsive by the conclusion of the responsiveness review in April 2017. The Government represented that the "vast majority" were and agreed to conduct a "page-by-page" analysis to determine whether each page of the 420 documents was identified as responsive by that time. *See id.* at 42:11–44:22.

The Government ultimately conducted a page-by-page analysis of 417 documents, having "removed from the universe" of 420 documents three documents the parties agree are subject to spousal privilege. *See* Dkt. No. 168 at 1 n.1. These 417 documents comprise 3,104 pages. *Id.* at 1. The Government's analysis indicates that of these 3,104 pages, 2,064 were identified for seizure by April 2017, and 449 pages are from non-Sadr accounts or are part of grand jury subpoena returns. *Id.* at 5. An additional 36 pages were referenced in work product created by April 2017, and 429 pages are part of or related to email threads and attachments that the D.A. identified by April 2017 but for which the Government has not found any indication that the specific pages were identified as responsive by that time. *Id.* at 3–

5. The Government was unable to determine whether the remaining 126 pages, or related versions, were identified for seizure by April 2017 and has represented to the Court that it will not rely on those pages as a result. *Id.* at 5. Thus, the Government now represents to the Court that it will ***718** only rely at trial on 2,978 pages of the 3,104 pages constituting the 417 documents. *Id.* at 1.

II. A *FRANKS* HEARING IS NOT WARRANTED

Sadr argues that the Government "obtained multiple search warrants for [his] email accounts under false and misleading pretenses," and that, in doing so, it "deliberately misled the reviewing court ... or, at the very least, acted with reckless disregard for the truth." Dkt. No. 96 at 1. As a result, he argues that these warrants are invalid and a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154, 98 S.Ct. 2674, 57 L.Ed.2d 667 (1978), is necessary to establish their invalidity. *See generally* Dkt. No. 96 at 5–17. For the reasons stated below, the Court concludes that a *Franks* hearing is not warranted.

[1] Because the probable cause standard underpins much of the discussion that follows in this and subsequent sections, the Court begins with a description of it. The Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. Thus, "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Kentucky v. King*, 563 U.S. 452, 459, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011)).

[2] **[3]** **[4]** "The Supreme Court has explained that 'probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.' " *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 232, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983)). "In evaluating probable cause in any given case, a judge must make a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (internal quotation marks and ellipsis omitted) (quoting *Falso*, 544 F.3d at 117). "Due to this subjective standard, a reviewing court generally accords 'substantial deference to the finding of an issuing judicial officer that probable cause exists,' limiting [the] inquiry to whether the officer 'had a substantial basis' for bis determination." *Id.* at 113 (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)). "Nevertheless, under this standard, [courts] 'may properly conclude that ... a warrant was invalid because the [judge's] probable-cause determination reflected an improper analysis of the totality of circumstances.' " *Falso*, 544 F.3d at 117 (internal brackets omitted) (quoting *United States v. Leon*, 468 U.S. 897, 915, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

[5] **[6]** **[7]** Although "a search or seizure pursuant to a warrant is presumed valid," a defendant may, "[i]n certain circumstances, ... challenge the truthfulness of factual statements made in the affidavit, and thereby undermine the validity of the warrant and the resulting search or seizure." *United States v. Awadallah*, 349 F.3d 42, 64 (2d Cir. 2003) (citing *Franks*, 438 U.S. at 164–72, 98 S.Ct. 2674). To obtain a *Franks* hearing on a motion to suppress on the basis of alleged misstatements or omissions in a warrant affidavit, a defendant must make a *substantial* preliminary showing that (1) there were intentional misrepresentations or omissions in the warrant affidavit, or, in other words "the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood ***719** or reckless disregard for the truth"; and (2) those misrepresentations or omissions were material, or "necessary to the issuing judge's probable cause finding." *United States v. Rajaratnam,* 719 F.3d 139, 146 (2d Cir. 2013) (alterations omitted) (quoting *United States v. Canfield,* 212 F.3d 713, 717–18 (2d Cir. 2000)); *see also* *Franks*, 438 U.S. at 155–56, 98 S.Ct. 2674. To satisfy this test, "a defendant must 'point out *specifically* the portion of the warrant affidavit that is claimed to be false.' " *United States v. Levy*, 2012 WL 5830631, at *5 (S.D.N.Y. Nov. 16,

2012), *aff'd*, 626 F. App'x 319 (2d Cir. 2015) (emphasis added) (quoting *Franks*, 438 U.S. at 171, 98 S.Ct. 2674).

[8] **[9]** **[10]** With respect to the intentionality prong, "the reviewing court must be presented with credible and probative evidence" that a misstatement or omission "in a [warrant] application was 'designed to mislead' or was 'made in reckless disregard of whether [it] would mislead.' " *Rajaratnam*, 719 F.3d at 154 (second alteration in original) (quoting *Awadallah*, 349 F.3d at 68). Reckless disregard for the truth may be established by demonstrating that an affiant made "statements which failed to take account of the facts as he knew them, or which he seriously doubted were true." *Rivera v. United States*, 728 F. Supp. 250, 258 (S.D.N.Y. 1990), *aff'd in relevant part*, 928 F.2d 592 (2d Cir. 1991). Where omissions are concerned, recklessness may be inferred "where the omitted information was 'clearly critical' to the probable cause determination." *Rivera*, 928 F.2d at 604. However, such an inference is "not to be automatically drawn simply because a reasonable person would have included the omitted information, and the inference is particularly inappropriate where the government comes forward with evidence indicating that the omission resulted from nothing more than negligence, or that the omission was the result of a considered and reasonable judgment that the information was not necessary to the [warrant] application." *Rajaratnam*, 719 F.3d at 154–55 (citation omitted).

[11] **[12]** With respect to the materiality prong, courts "gauge materiality by a process of subtraction" or addition depending on whether misstatements or omissions are at issue. *Awadallah*, 349 F.3d at 65. In other words, to determine materiality, courts should "disregard the allegedly false statements," *Awadallah*, 349 F.3d at 65 (citation omitted), "insert the omitted truths," *Rajaratnam*, 719 F.3d at 146 (citation omitted), and determine whether "there remains a residue of independent and lawful information sufficient to support probable cause," *Awadallah*, 349 F.3d at 65 (citation omitted). "If, after setting aside the allegedly misleading statements or omissions, the affidavit, nonetheless, presents sufficient information to support a finding of probable cause, the district court need not conduct a Franks hearing." *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998).

[13] **[14]** The *Franks* standard is "a high one." *Rivera*, 928 F.2d at 604. As discussed above, to be entitled to a hearing under this standard, "a defendant 'must make a substantial preliminary showing' of each of the prongs." *Levy*, 2012 WL 5830631, at *5 (quoting *Salameh*, 152 F.3d at 113). This substantial preliminary showing must consist of "specific allegations accompanied by an offer of proof"; "[u]nsupported conclusory allegations of falsehood or material omission cannot support a *Franks* challenge." *Velardi v. Walsh*, 40 F.3d 569, 573 (2d Cir. 1994).

A. Sadr Has Not Made a Substantial Showing of Deliberate Falsehood or Reckless Disregard for Truth

As an initial matter, Sadr's offer of proof consists only of his memorandum of law submitted in support of this motion, unaccompanied ***720** by any "[a]ffidavits or sworn or otherwise reliable statements of witnesses," or even any satisfactory explanation for their absence. *Franks*, 438 U.S. at 171, 98 S.Ct. 2674. Even were such an offer of proof sufficient to make the required substantial preliminary showing—which the Court does not and need not decide here—the memorandum of law fails to make a substantial showing of "credible and probative evidence" of deliberate falsehood or reckless disregard for the truth. *See* *Rajaratnam*, 719 F.3d at 154.

In his memorandum of law, Sadr points out what he alleges are numerous misstatements, omissions, and what he calls "misleading claims" that, he argues, derive from "stringing together unrelated facts" to create false implications. *See* Dkt. No. 96 at 7–13. However, he fails to make the requisite *substantial* showing of credible and probative evidence demonstrating that any of these alleged misstatements, omissions, or "misleading claims" were deliberately false or made with reckless disregard for the truth.

1. Misstatements

With respect to alleged misstatements, Sadr claims that the warrant applications contain five "demonstrably false and unsupported statements." These include (1) statements in the April 2014 and June 2014 warrant affidavits that the Sadr family has "substantial ties to the Government of Iran," Dkt. No. 96-1 ¶ 5; Dkt. No. 96-2 ¶ 6; (2) a statement in the April 2014 affidavit that Sadr, his company, and his father's company have "links" to "entities that have been sanctioned by OF AC ... for supporting Iran's nuclear weapons program, proliferation activities, and support of terrorism," Dkt. No. 96-1 ¶ 29; (3) statements in the April 2014, June 2014, and October 2015 affidavits that "there is reason to believe that some of the funds transferred are for covert projects between the [Government of Iran] and Venezuela outside the scope of the Project," Dkt. No. 96-1 ¶ 5; Dkt. No. 96-2 ¶ 6; Dkt. No. 96-3 ¶ 10; (4) statements in the April and June 2014 affidavits that "entities involved in the Project engage in large, U.S.-dollar transactions between Venezuela and Iran ... involv[ing] a variety of non-transparent entities, banks in high-risk jurisdictions, and ... Swiss bank accounts ...," Dkt. No. 96-1 ¶ 5; Dkt. No. 96-2 ¶ 6; and (5) various alleged inaccuracies and inconsistencies that Sadr admits are "not material on their own," Dkt. No. 96 at 10.

Setting aside the fact that he has offered little evidence that these statements are in fact *mis*statements, Sadr offers even less credible and probative evidence that these alleged misstatements were deliberately false or made with reckless disregard for the truth. The evidence that he does offer falls primarily into two categories. First, he points to the fact that the affidavits do not provide additional "support" or "evidence" for these alleged misstatements. *See* Dkt. No. 96 at 7–8 (citing a lack of support or evidence for statements in categories (1), (2), and (3)). Second, he argues that the fact that certain statements appeared in earlier warrant affidavits but were excised from later warrant affidavits is an acknowledgement, on the Government's part, of their falsity. *See id.* at 7–9 (noting that statements in categories (1) and (4) were removed from or revised in later warrant affidavits).

[15] **[16]** **[17]** With respect to Sadr's first category of evidence, he argues that the lack of further "support" or "evidence" for various allegations in the affidavit evinces a "reckless disregard" for the truth. However, reckless disregard for the truth cannot be inferred unless circumstances evince "*obvious* reasons to doubt the veracity" of the allegedly misstated information. *Rajaratnam,* 719 F.3d at 154 (emphasis added) (quoting ***721** *United States v. Whitley*, 249 F.3d 614, 621 (7th Cir. 2001)). The alleged lack of further support or evidence for an allegation does not constitute an *obvious* reason to doubt the veracity of that allegation, and, in any event, "[a]n affiant cannot be expected to include in an affidavit every piece of information gathered in the course of an investigation." *Awadallah*, 349 F.3d at 67–68 (quoting *United States v. Colkley*, 899 F.2d 297, 300 (4th Cir. 1990)). Any further suggestion that the falsity of the allegation *itself* constitutes obvious reason to doubt its veracity is obviously circular. *See, e.g.*, Dkt. No. 96 at 8 (arguing that the "affidavit cites no evidence to support this significant claim [that Sadr had links with entities sanctioned by OFAC for supporting Iran's nuclear weapons program and support of terrorism], and in fact, neither Sadr nor any of the individuals or entities described in this paragraph have any connections whatsoever to nuclear weapons or terrorism").

With respect to the alleged misstatements that appeared in earlier warrant affidavits but were excised from later warrant affidavits, he argues that these subsequent omissions were due to the Government's realizations through further investigation that such deliberately "false allegation[s]" were "untenable." *Id.* at 7. However, the fact that some allegations were omitted from subsequent affidavits does not necessarily suggest that the "affiant in fact entertained serious doubts as to the truth of his allegations" *when he initially made them*, and, in fact, may suggest just the opposite. *Rajaratnam*, 719 F.3d at 154 (quoting *Whitley*, 249 F.3d at 621). Indeed, Sadr's argument demonstrates the willingness of the affiant to *strike* allegations where unsupported, suggesting that the allegations he initially put forth *were* "believed or appropriately accepted by [him] as true" for the simple reason that he would not have otherwise included them. *Franks*, 438 U.S. at 165, 98 S.Ct. 2674. While Sadr's contrary inference may fall within the realm of possibility, this conjecture, unsupported by any additional offer of proof, certainly does not amount to a substantial showing of "credible and probative evidence"

that the alleged misstatements were "designed to mislead." *Rajaratnam*, 719 F.3d at 154.

2. Omissions

[18] Sadr's arguments with respect to omissions that he alleges intentionally or recklessly misled the issuing court fare no better. He alleges that the affidavits: (1) do not allege that the transactions involved the proceeds of criminal conduct, such that they fail to establish probable cause for money laundering, Dkt. No. 96 at 11; (2) fail to acknowledge that the ITRS authorized the charged transactions, *id.*; and (3) "contain no evidence" that Sadr used any of the email accounts searched to conduct any allegedly unlawful business related to the housing construction project, *id.* at 11–12. However, Sadr fails to make *any* showing—let alone a substantial showing—that these alleged omissions were designed to mislead or were made with reckless disregard for whether they would mislead the issuing court, and, in any event, his arguments with respect to these alleged omissions are rejected elsewhere in this Opinion and Order, *see infra* Section II.B (addressing probable cause for money laundering); Section III.B (addressing probable cause that evidence of crimes would be found within the specific target email accounts), or in the Court's December 6, 2019 Opinion and Order resolving Sadr's first seven pretrial motions, *see* Dkt. No. 164 at II.C (rejecting the argument that the ITSR authorized the charged transactions).

3. "Misleading Claims"

Finally, Sadr argues that the affidavits contain "misleading claims" that derive ***722** from "stringing together unrelated"—but true—"facts" to create false implications. Dkt. No. 96 at 12–13. This argument is meritless because it fails to even identify any false statements or omitted truths, prerequisites to the application of the *Franks* doctrine. *See* *Awadallah*, 349 F.3d at 64 ("In order to invoke the *Franks* doctrine, [a defendant] must show that there were intentional and material misrepresentations or omissions in [the agent's] warrant affidavit.").

In sum, in each instance Sadr fails to support his argument that alleged misstatements, omissions, or "misleading claims" in the warrant applications—to the extent there are any—were designed to mislead or made with reckless disregard for whether they would mislead the issuing court. Indeed, these arguments are, at bottom, premised on nothing more than speculation and conjecture. Such "[u]nsupported conclusory allegations of falsehood or material omission cannot support a *Franks* challenge." *Velardi*, 40 F.3d at 573. Because he has failed to make a substantial showing that alleged misstatements or omissions were designed to mislead or made with reckless disregard for whether they would mislead the issuing court, a *Franks* hearing is not warranted.

B. Sadr Has Not Made a Substantial Showing of Materiality

Though Sadr's failure to make a substantial showing of "credible and probative evidence" of deliberate falsehood or reckless disregard for the truth in the warrant affidavits is on its own fatal to his motion for a *Franks* hearing, *see* *Levy*, 2012 WL 5830631, at *5, this motion also fails for the additional reason that Sadr has not made a substantial showing of materiality.

[19] **[20]** "To determine if misrepresentations or omissions are material, a court corrects the errors and then resolves de novo whether the hypothetical corrected affidavit still establishes probable cause." *United States v. Lahey*, 967 F. Supp. 2d 698, 711 (S.D.N.Y. 2013); *see also* *Ganek v. Leibowitz*, 874 F.3d 73, 82 (2d Cir. 2017) ("To determine whether a false statement was necessary to a finding of probable cause, we consider a hypothetical corrected affidavit, produced by deleting any alleged misstatements from the original warrant affidavit and adding to it any relevant omitted information."). Even assuming these affidavits contain errors that require correcting, excising the alleged errors from them only demonstrates the overwhelming strength of the probable cause showing. Indeed, as the Government points out, the hypothetical corrected April 2014 affidavit contains numerous allegations unchallenged by Sadr, including:

- There was a multi-million dollar infrastructure project in Venezuela involving a Venezuelan state-owned

energy company and the Iranian International Housing Corporation—an entity that is part of Stratus Group, an Iranian conglomerate controlled by Sadr's family. Dkt. No. 96-1 ¶ 5.

- A contract involving this housing construction project was signed by a subsidiary of the Venezuelan state-owned energy company and the Iranian International Housing Corporation and was entered into pursuant to an agreement between Venezuela and the Government of Iran. *Id.* ¶ 9.

- An addendum to the contract provided that payments for project-related transactions would be made in U.S. dollars. *Id.* ¶ 10.

- The housing construction project was suspended over a payment issue during May and June 2011. The chairman of the Venezuelan subsidiary told an informant that sanctions regimes against Iran made it difficult to pay for the project in U.S. dollars, ***723** and he repeatedly asked that the Iranians accept payment in Bolivars. *Id.* ¶ 14.

- After work on the project resumed, the Iranian International Housing Corporation provided the chairman of the Venezuelan subsidiary with a letter instructing that payment be made through a bank located in New York to the Swiss bank account of Clarity Trade and Finance S.A. "[i]n view of the current difficulties for transfer and movement of funds." *Id.* ¶ 15.

- Subsequent letters signed by the chairman of the Venezuelan subsidiary instructed that payments in favor of the Iranian International Housing Corporation be made through a New York bank to Clarity's Swiss bank account. *Id.* ¶ 17.

- On several occasions, the Venezuelan state-owned energy company sent payments in U.S. dollars through a New York bank to Clarity's Swiss bank account. *Id.* ¶ 27.

- According to the Stratus Holdings website, Stratus Global Investments held a controlling interest in Clarity. *Id.* ¶ 30.

- Sadr was the Director of Clarity, *id.* ¶ 32, and had signatory authority or a controlling interest in its Swiss bank accounts, *id.* ¶ 37.

See also Dkt. No. 108 at 75–77. [2]

These allegations and others unchallenged by Sadr establish probable cause to believe that he was engaged in a complex scheme designed to evade U.S. sanctions. Under the totality of the circumstances, there remains, even based only on the allegations of the corrected affidavit, a "fair probability" that business records were falsified or false instruments were offered for filing as part of this complex scheme. *See* *Raymonda*, 780 F.3d at 113 (2d Cir. 2015). Moreover, in light of the fact that these allegations establish probable cause that Sadr committed these other state offenses, it follows that there is a high probability that this scheme also violated state money laundering statutes.

[21] Sadr's argument that he does not accept as true the unchallenged allegations in the affidavit but rather culled the affidavit's misrepresentations to "only the most egregious and clear-cut," which on their own "are sufficient to obtain a *Franks* hearing" fundamentally misapprehends the materiality showing required to obtain such a hearing. *See* Dkt. No. 116 at 5 n.2; *id.* at 10. Indeed, a defendant must "point out specifically" *all* portions of the warrant affidavit he claims to be false. *See Levy*, 2012 WL 5830631, at *5. This is necessary to allow the Court to gauge materiality, which involves "deleting any alleged misstatements from the original warrant affidavit," "adding to it any relevant omitted information," and determining whether probable cause still exists "after such a correction." *Ganek*, 874 F.3d at 82. After correcting the errors *specifically* identified by Sadr, the Court finds that the hypothetical corrected affidavit still establishes probable cause. Accordingly, Sadr has not made a substantial showing of materiality to warrant a *Franks* hearing on the basis of the misstatements, omissions, and "misleading claims" specifically identified in his memorandum of law. Nor is he entitled to one to determine whether the "truth or falsity of these and *other* misrepresentations" *not specifically identified and not now before the Court* were necessary to the probable cause showing. Dkt. No. 116 at 5 n.2.

***724 III. SUPPRESSION IS NOT WARRANTED ON PARTICULARITY OR OVERBREADTH GROUNDS**

Sadr also argues that the search warrants are invalid because they lack the requisite particularity and are overbroad. *See* Dkt. No. 96 at 17–22. Ultimately, for the reasons stated below, the Court finds that neither of these arguments provide grounds for suppressing the search warrant evidence.

[22] As discussed above, the Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. "A warrant, therefore, can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries." *United States v. Cohan*, 628 F. Supp. 2d 355, 359 (E.D.N.Y. 2009).

[23] **[24]** **[25]** The Fourth Amendment's particularity requirement targets "the specific evil [of] the 'general warrant' abhorred by the colonists," and is thus meant to prevent the "general, exploratory rummaging in a person's belongings" that such general warrants allowed. *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971). A sufficiently particular warrant is one that "enable[s] the executing officer to ascertain and identify with reasonable certainty those items that the magistrate has authorized him to seize." *United States v. George*, 975 F.2d 72, 75 (2d Cir. 1992). Under Second Circuit law,

> [t]o be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements. First, "a warrant must identify the specific offense for which the police have established probable cause." *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). Second, "a warrant must describe the place to be searched." *Id.* at 445–46. Finally, the "warrant must specify the items to be seized by their relation to designated crimes." *Id.* at 446 (internal quotation marks omitted).

United States v. Ulbricht, 858 F.3d 71, 99 (2d Cir. 2017). The Fourth Amendment "requires particularity in the warrant, not in the supporting documents," and, accordingly, "[t]he fact that the [warrant] *application* adequately described the 'things to be seized' does not save the *warrant*" from failure to satisfy the particularity requirement. *Groh v. Ramirez*, 540 U.S. 551, 557, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004). [3]

In addition to these requirements, courts in this Circuit have identified certain "circumstance-specific considerations" that may bear on whether a given warrant lacks particularity, even if they do not constitute formal, universal requirements. *United States v. Zemlyansky*, 945 F. Supp. 2d 438, 454 (S.D.N.Y. 2013). Many courts, for example, "have found warrants for the seizure of [business] records constitutionally deficient where they imposed too wide a time frame or failed to include one altogether." *Id.* (quoting *Cohan*, 628 F. Supp. 2d at 365–66 (citing "general agreement that a time frame is *relevant*" even if not necessarily "required")); *see also* *United States v. Levy*, 2013 WL 664712, at *11 n.7 (S.D.N.Y. Feb. 25, 2013) ("Several courts in this Circuit have recognized the constitutional questions that are raised by the lack of a specific date range in a warrant for documentary records and warned the Government to include one when possible."); *cf.* ***725** *United States v. Hernandez*, 2010 WL 26544, at *9 (S.D.N.Y. Jan. 6, 2010) ("A failure to indicate a time frame could render a warrant constitutionally overbroad because it could allow the seizure of records dating back arbitrarily far and untethered to the scope of the affidavit which ostensibly provided probable cause." (internal quotation marks, citation, and alterations omitted)).

[26] **[27]** **[28]** "[A] warrant is overbroad if its 'description of the objects to be seized ... is broader than can be justified by the probable cause upon which the warrant is based.' " *United States v. Lustyik*, 57 F. Supp. 3d 213, 228 (S.D.N.Y. 2014) (alteration in original) (quoting *Galpin*, 720 F.3d at 446). Breadth and particularity are thus "related but distinct concepts." *Ulbricht*, 858 F.3d at 102. The two are related in that a warrant's unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause. However, they are distinct in that a broad warrant does not necessarily lack particularity: a "warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material," without necessarily "violating the particularity requirement." *Id.*

"In determining whether a warrant is overbroad, courts must focus on 'whether there exists probable cause to support the breadth of the search that was authorized.' " *Zemlyansky*, 945 F. Supp. 2d at 464 (quoting *Hernandez*, 2010 WL 26544, at *8).

A. Particularity

[29] The warrants are sufficiently particular because they identify the specific offenses for which the police established probable cause, describe the place to be searched, and specify the items to be seized by their relation to designated crimes as required under Second Circuit law. *See* *Ulbricht*, 858 F.3d at 99. Indeed, they identify specific New York State Penal Law offenses—money laundering, offering a false instrument for filing, and falsifying business records—for which law enforcement established probable cause. *See, e.g.*, Dkt. No. 96-1 at 37; Dkt. No. 96-2 at 20. In addition, they describe the places to be searched—specific target email accounts. *See, e.g.*, *id.* Finally, they specify that the items seized—including payment history, billing information, contacts, sent and received messages, saved or draft messages, attachments, IP log history, connection log data, account creation data, passwords, sign-on codes, and account numbers—should be those that tend to demonstrate commission of the aforementioned offenses, including evidence of involvement in money laundering, offering a false instrument for filing, and falsifying business records; an attempt or conspiracy to commit those crimes; involvement in the planning of, recruiting for, or commission of those crimes; communication with witnesses to and victims of those crimes; communication with third parties relating to witnesses to and victims of those crimes; and communication with third parties while using aliases or other identities. *See, e.g.*, *id.*

Sadr, however, argues that the warrants at issue are lacking in particularity for three reasons.[4] First, he argues that the ***726** warrants functioned as general warrants because "identifying broad state law offenses in the warrants did not render them sufficiently particularized, [especially] where the scope of the authorized seizure was not linked to the probable cause showing for those offenses." Dkt. No. 156 at 4. Second, he argues that the warrants "were not limited to certain ... email recipients/users, domains, subjects, or any other particularized places to look for evidence of the alleged offenses." Dkt. No. 96 at 19. Finally, he argues that the "lack of any temporal restrictions on the seizure and search also supports a finding of insufficient particularity." *Id.* at 20. For the reasons stated below, the Court finds that the warrants did not function as general warrants and need not have set out specific email recipients, domains, or subjects to comply with the Fourth Amendment. The Court need not decide whether the lack of any temporal limitations rendered the otherwise particular warrants insufficiently particular, because the agents acted in good-faith reliance on them.

1. Limitations by Crimes

Sadr concedes that the warrants here "state that evidence of three broad criminal violations may be found in the target email accounts," Dkt. No. 116 at 14, but argues that they nonetheless were insufficiently particular—and, in effect, functioned as general warrants—because the paragraphs authorizing seizure do not refer to these crimes. He cites only one case, *United States v. Zemlyansky*, 945 F. Supp. 2d 438 (S.D.N.Y. 2013), for this argument. However, the warrant at issue in *Zemlyansky* is readily distinguishable from those at issue here. Indeed, in *Zemlyansky*, the warrant only referenced the crimes for which the search was being undertaken in a *single* subsection of the *ninth* item enumerated in the warrant. *See* *id.* at 454. The court noted that at "no point prior to or during the enumeration of [the first] eight items does the warrant offer any indication of the relevant criminal allegations," and, as a result, "officers are thus directed to these categories without a single word of guidance regarding the type of criminal offense under investigation." *Id.* In light of the fact that reference to the suspected crimes was buried deep within the warrant in a sole subsection of the ninth item, the court concluded that the warrant, "on any reasonable interpretation, [was] silent as to the federal criminal offenses for which evidence [was] sought." *Id.* at 457. *Zemlyansky* is thus more akin to the line of cases finding warrants insufficiently particular where they completely "fail[ ] to reference the suspected crimes." *United States v. Wey*, 256 F. Supp. 3d 355, 384 (S.D.N.Y. 2017); *see also* *George*, 975 F.2d at 75–76 (finding a warrant permitting search for evidence "relating

to the commission of a crime" lacked particularity because "[n]othing on the face of the warrant tells the searching officer for what crime the search is being undertaken").

The warrants at issue here, however, neither completely fail to reference the suspected crimes nor bury them deep within the warrant. Rather, each warrant is only three pages long and references the suspected crimes within the first page, if not the first paragraph. *See* Dkt. No. 96-1 at 37; *id.* at 40; *id.* at 43; *id.* at 46; Dkt. No. 96-2 at 17; *id.* at 20; *id.* at 23. Indeed, each warrant notes, *prior* to the search and seizure authorization, that there is probable cause to believe that the target email accounts contain evidence of involvement in money laundering, offering a false ***727** instrument for filing, and falsifying business records. *See id.* Unlike in *Zemlyansky*, they "offer an[ ] indication of the relevant criminal allegations" up front and provide "guidance regarding the type of criminal offense[s] under investigation" prior to authorizing the search and seizure of any evidence. 945 F. Supp. 2d at 454.

[30] **[31]** The Court concludes that the fact that these brief warrants do not reference the suspected crimes within the paragraphs authorizing seizure does not render them insufficiently particular. "[T]here is no settled formula" in the Second Circuit "for determining whether a warrant lacks particularity," *id.* at 453; rather a warrant must be sufficiently specific "to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize," *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (alteration in original) (citation omitted). In other words, a warrant is lacking in particularity if it "leave[s] to the unguided discretion of the officers executing the warrant the decision as to what items may be seized." *United States v. Riley*, 906 F.2d 841, 844 (2d Cir. 1990). In contrast to the warrants at issue in *Zemlyansky*, these warrants did not leave the decision as to what items may be seized to the unguided discretion of the executing officers, but rather informed them within the first page that the target email accounts were believed to contain evidence of certain specified crimes. Viewed as a whole, the failure of these search warrants to repeat the suspected crimes in the paragraphs authorizing seizure does not render them lacking in particularity. *See* *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("A warrant need not ... survive a hyper-technical sentence diagraming and comply with the best practices of *Strunk & White* to satisfy the particularity requirement.").

Sadr further argues that even if the warrants could be interpreted as limiting seizure to all evidence of the specified crimes—which, the Court concludes, they can—"identifying broad state law offenses ... did not render them sufficiently particularized." Dkt. No. 156 at 4. However, nearly all the cases he cites to support this argument are over three decades old and do not involve electronic searches, the nature of which, as discussed below, affects the context-dependent particularity inquiry. *See* *United States v. Buck*, 813 F.2d 588, 590 (2d Cir. 1987); *United States v. Maxwell*, 920 F.2d 1028, 1033 (D.C. Cir. 1990); *United States v. Leary*, 846 F.2d 592, 594 (10th Cir. 1988); *Rickert v. Sweeney*, 813 F.2d 907, 908 (8th Cir. 1987); *United States v. Roche*, 614 F.2d 6, 7 (1st Cir. 1980); *United States v. Abrams*, 615 F.2d 541, 542 (1st Cir. 1980). These dated and largely out-of-circuit cases are accordingly of little value to the Court in deciding the issue now before it. [5]

Moreover, Sadr mischaracterizes the warrants, which are more particularized than he admits. Indeed, as discussed above, they include illustrative lists of the kinds of data sought, including payment history, sent and received emails, and IP log history, and specify that such data should show involvement in the suspected crimes, an attempt or conspiracy to commit such crimes, involvement in the planning of, recruiting for, or commission of those crimes, communication with witnesses to and victims of those crimes, and communication with related third parties. *See, e.g.*, Dkt. No. 96-1 at 37. In cases of more recent vintage, courts in this District ***728** have upheld similar warrants for email account data. *See, e.g.*, *United States v. Dupree*, 781 F. Supp. 2d 115, 152 (E.D.N.Y. 2011) (upholding warrant for electronically stored information that "authorize[d] seizure of evidence of violations of 18 U.S.C. §§ 1341, 1343, 1344 and 1349, specifically '[a]ll documents relating to the conspirators', or any of their principals', employees', or agents' calendar, contact, or personal planner data or files including, but not limited to, data contained in Outlook, Lotus Notes, or

Eureka, created or maintained by the user(s) of any computer located at the SUBJECT PREMISES' "); *see also, e.g.*, *United States v. Mathieu*, 2018 WL 5869642, at *2 (S.D.N.Y. Nov. 9, 2018); *United States v. Patel*, 2017 WL 3394607, at *4 (S.D.N.Y. Aug. 8, 2017); *see also* *Lustyik*, 57 F. Supp. 3d at 227 (finding that "[t]he inclusion of an illustrative list of seizable items" brought the email warrants "within the Fourth Amendment's particularity parameters"). Indeed, where, as here, warrants call for the seizure of records relating to the suspected crime or crimes and include a list "providing examples of the items to be seized," they have been found to "offer[ ] sufficient guidance to law enforcement officers to pass constitutional muster." *Lustyik*, 57 F. Supp. 3d at 228; *see also* *Riley*, 906 F.2d at 843 (upholding a warrant calling for the seizure of "records of the distribution of cocaine ... including but not limited to, bank records, brokerage house records, business records, [and] safety deposit box keys or records"). The Court agrees with this precedent and its applicability here.

2. Additional Particularization Relating to the Scope of Search and Seizure

Sadr further argues that the warrants lack particularly because they authorize the executing agents to search the entireties of the target email accounts and seize "all email messages in the account" without placing any further limitations with respect to email recipients, domains, or subjects. Dkt. No. 96 at 19; *see also* Dkt. No. 156 at 6 (arguing that the warrants do not "particularize the evidence sought to specific categories of evidence ... [and thus] the agents had unfettered discretion to seize the entirety of Sadr's email accounts").

As an initial matter, Sadr's objection to the seizure of the entireties of his email accounts misapprehends the case law related to electronic searches and seizures. Indeed, due to the unique challenges that electronic searches pose, "it is frequently the case with computers that the normal sequence of 'search' and then selective 'seizure' is turned on its head, as computer hardware is seized from a suspect's premises before its content is known and then searched at a later time." *United States v. Vilar*, 2007 WL 1075041, at *35 (S.D.N.Y. Apr. 4, 2007) (internal quotation marks and citation omitted); *see also* Fed. R. Crim. P. 41(e)(2)(B) ("A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant."). This rationale applies with equal force to email accounts, and, based on this rationale, courts in this District have "upheld the Government's ability to obtain the entire contents of [an] email account to [later] determine which particular emails come within the search warrant." *In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx gmail.com Maintained at Premises Controlled By Google, Inc.*, 33 F. Supp. 3d 386, 394 (S.D.N.Y. 2014); *see Patel*, 2017 WL 3394607, at *4; *see also United States v. Chalavoutis*, 2019 WL 6467722, at *4 (E.D.N.Y. Dec. 2, 2019) (finding that a "warrant command[ing] the email provider to turn over 'the contents of all emails associated with the account' ... ***729** 'is consistent with the well-established law of this Circuit' " (citation omitted)). Thus, the Court concludes that the search warrants' authorization of the initial seizure of all email messages in the target accounts does not render them insufficiently particular.

[32] Sadr's argument that the search warrants lack particularity because they fail to further limit the scope of the search and ultimate seizure to certain types or categories of evidence also fails for many of the same reasons already articulated above. As discussed above, district courts in this Circuit have found warrants that reference the suspected crimes and "provid[e] an illustrative, but not exhaustive, list of items to be seized," sufficiently particular. *See* *Lustyik*, 57 F. Supp. 3d at 228. Indeed, "[g]eneric terms," such as those employed here to describe the items to be seized, "may be used ... so long as the warrant identifies a specific illegal activity to which the item [sought] related." *Patel*, 2017 WL 3394607, at *5. Thus, the Government's use of "generic, catch-all phrases in its [w]arrant[s] instead of the case-specific information it had at its disposal" to describe the information to be seized here is not fatal to these warrants, which are nonetheless "sufficiently specific to permit the rational exercise of judgment [by the executing officers]." *Dupree*, 781 F. Supp. 2d at 150 (alternation in original) (citation omitted).

[33] Moreover, the type of evidence sought is relevant to the level of specificity the Fourth Amendment requires, *see id.* at 149, and courts typically tolerate less specificity where electronic documentary evidence is involved. *See United States v. DiScala*, 2018 WL 1187394, at *15 (E.D.N.Y. Mar. 6, 2018) ("A broad warrant does not necessarily lack particularity, especially where electronic records are concerned."); *Dupree*, 781 F. Supp. 2d at 149. This is due to the fact that "documentary evidence may be difficult to describe *ex ante* with the same particularity as a murder weapon or stolen property," *Dupree*, 781 F. Supp. 2d at 149 (quoting *United States v. Cioffi*, 668 F. Supp. 2d 385, 391 (E.D.N.Y. 2009)), and, when electronic information is involved, "there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities," *United States v. Graziano*, 558 F. Supp. 2d 304, 315 (E.D.N.Y. 2008). Accordingly, the Court concludes that the email warrants at issue were not lacking in particularity on the ground that they failed to "particularize the evidence sought to specific categories of evidence."

3. Temporal Limitations

[34] Sadr finally argues that the warrants' "lack of any temporal restrictions on the seizure and search ... supports a finding of insufficient particularity." Dkt. No. 96 at 20. While a temporal limitation is "*one indicia* of particularity," *United States v. Triumph Capital Grp., Inc.*, 211 F.R.D. 31, 58 (D. Conn. 2002) (emphasis added), courts in this Circuit have recognized that "[t]he complexity and duration of the alleged criminal activities" may "render a time frame less significant than in a case that required a search for a small set of discrete items related to one or only a few dates," *see, e.g.*, *Hernandez*, 2010 WL 26544, at *11. On the other hand, at least one court in this Circuit has observed that "a warrant's failure to include a temporal limitation on the things to be seized" alone "may, in certain circumstances, render a warrant insufficiently particular." *United States v. Jacobson*, 4 F. Supp. 3d 515, 526 (E.D.N.Y. 2014). The Court need not decide whether the lack of temporal limitations renders the otherwise sufficiently particular warrants at issue here insufficiently particular, because, as discussed ***730** below, *see infra* Section III.C, the executing agents acted in good-faith reliance on them. *See United States v. Ganias*, 824 F.3d 199, 209 (2d Cir. 2016) (en banc) ("Because we conclude that the agents acted in good faith, we need not decide whether a Fourth Amendment violation occurred.").

B. Overbreadth

[35] A warrant "is overbroad if its 'description of the objects to be seized ... is broader than can be justified by the probable cause upon which the warrant is based.' " *Lustyik*, 57 F. Supp. 3d at 228 (alteration in original) (quoting *Galpin*, 720 F.3d at 446). In this case, the warrant affidavits established probable cause for New York state crimes, *see supra* Section II.B, and the warrants limit the descriptions of the information to be seized to evidence of those crimes, *see supra* Section III.A.

Nonetheless, the warrants' failure to include temporal limitations implicates overbreadth as well as particularity concerns. As courts in this District have recognized, a "failure to indicate a time frame could render a warrant constitutionally overbroad because it could 'allow[ ] the seizure of records dating back arbitrarily far' and untethered to the scope of the affidavit which ostensibly provided probable cause." *Hernandez*, 2010 WL 26544, at *9 (alteration in original) (quoting *Cohan*, 628 F. Supp. 2d at 365). However, as above, the Court need not definitively decide whether the lack of temporal limitations renders the warrants unconstitutionally overbroad, because the Court concludes below, *see infra* Section III.C, that the executing agents acted in good-faith reliance on them. *See Ganias*, 824 F.3d at 209.

Sadr's other overbreadth arguments are completely without merit. He first argues that the warrant affidavits offered no reason to believe that evidence of the suspected crimes would be found within the specific target email accounts. Dkt. No. 96 at 18–19. However, contrary to his arguments, "the affidavits for search of a device or account do not have to provide specific evidence that every category of evidence sought will be present in that device or account, but can rely on the affiant['s] training, experience, and the totality of

the circumstances to support a 'common-sense' probability that the evidence may be found there sufficient for probable cause." *See United States v. Pinto-Thomaz*, 352 F. Supp. 3d 287, 306 (S.D.N.Y. 2018).

In this case, the affiant's training, experience, and the totality of the circumstances clearly supported a "common-sense" probability that evidence may be found in the specific target email accounts sufficient to establish probable cause to search them. For example, the April 2014 affidavit supporting the warrant applications specifically notes that "email is a preferred means of communication" within the Venezuelan state-owned energy company from which entities owned by Sadr and his family allegedly received payments for the construction of low-income housing. Dkt. No. 96-1 ¶ 7. It further notes that "personal emails are frequently used to transmit messages and documents amongst individuals involved in ... projects" with the state-owned energy company. *Id.* The affidavit also alleges that Sadr was the director of Clarity Trade and Finance S.A. and that money owed to the Iranian International Housing Corporation was remitted from the Venezuelan state-owned energy company, processed by New York banks, and received by Clarity's Swiss bank account. *Id.* ¶¶ 15–17, 27, 32. As discussed above, these and other allegations were sufficient to establish probable cause that crimes were committed under New York State law in an attempt to evade Iranian sanctions and further suggest ***731** a common-sense probability that evidence of these crimes may be found in Sadr's email accounts. *See United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004) (noting that the nexus between the evidence sought and the location to be searched "may be based on 'reasonable inference' from the facts presented based on common sense and experience" (citation omitted)).

Sadr's second overbreadth argument—that the warrants are overbroad because they fail to identify the sanctions laws allegedly violated—is likewise unavailing. Dkt. No. 96 at 20. In support of this argument, he cites *United States v. Cioffi* for the proposition that "[r]eferences to broad statutes realistically constitute no limitation at all on the scope of an otherwise overbroad warrant." 668 F. Supp. 2d at 392 (citation omitted). However, that quote is merely a reformulation of the particularity principle, discussed above, that warrants must confine searches to evidence of particular crimes. Because the warrants here confine any search to evidence of the particular crimes—money laundering, offering a false instrument for filing, and falsifying business records—for which the warrant affidavits established probable cause, it is irrelevant to the overbreadth inquiry that they did not also specifically identify the sanctions laws alleged to have been violated but that did not form the basis of an independent showing of probable cause.

C. Good-Faith Exception

[36] **[37]** **[38]** As discussed above, Sadr argues that the lack of temporal limitations renders the warrants invalid. Even if the Court were to agree, such a conclusion would not compel suppression of search warrant evidence. "A violation of the Fourth Amendment does not necessarily result in the application of the exclusionary rule." *Rosa*, 626 F.3d at 64. Indeed, the exclusionary rule is not a "personal constitutional right of the party aggrieved," *United States v. Calandra*, 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974), but rather is "a judicially created rule ... 'designed to safeguard Fourth Amendment rights generally through its deterrent effect,' " *Herring v. United States*, 555 U.S. 135, 139–40, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009) (quoting *Calandra*, 414 U.S. at 348, 94 S.Ct. 613). Thus, in order for the exclusionary rule to apply, "the benefits of deterrence" must "outweigh" the often "substantial social costs" of "letting guilty and possibly dangerous defendants go free." *Id.* at 141, 129 S.Ct. 695 (citations omitted).

[39] **[40]** **[41]** These principles are reflected in the good-faith exception to the exclusionary rule, which allows the Government to "introduce evidence obtained in violation of the Fourth Amendment unless the 'police conduct [was] sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.' " *Zemlyansky*, 945 F. Supp. 2d at 465 (alteration in original) (quoting *Herring*, 555 U.S. at 144, 129 S.Ct. 695). The deterrence benefits of exclusion will naturally "vary with the culpability of the law enforcement conduct at issue," *In re 650 Fifth Ave. & Related Properties*, 934 F.3d 147, 162 (2d Cir. 2019) (quoting

Davis v. United States, 564 U.S. 229, 238, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011)):

> "When the police exhibit deliberate, reckless, or grossly negligent disregard for Fourth Amendment rights, the deterrent value of exclusion is strong and tends to outweigh the resulting costs." Conversely, "when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force."

***732** *Id.* (citations omitted). "The pertinent analysis of deterrence and culpability is objective and [the Court's] good-faith inquiry is confined to the objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances." *Rosa*, 626 F.3d at 64 (internal quotation marks and citation omitted).

[42] **[43]** Thus, as a general matter, the good-faith exception applies "when the government acts in 'objectively reasonable reliance on a subsequently invalidated search warrant.' " *In re 650 Fifth Ave.*, 934 F.3d at 162 (quoting *Leon*, 468 U.S. at 922, 104 S.Ct. 3405). However, this is not so "(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable." *Id.* (quoting *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011)).

[44] The good-faith exception applies here because, even assuming the search warrants are invalid, the Government acted in objectively reasonable reliance on them, and none of the four above-noted exceptions to this exception apply here. Indeed, the Court has already considered and rejected arguments that the issuing judge was knowingly misled, *see* Section II.A, and that the warrant applications were lacking in probable cause, *see* Section II.B. Moreover, Sadr does not even suggest that Justice Obus, a justice of the New York County Supreme Court who had no prior involvement in the investigation of this case, wholly abandoned his judicial role in granting the search warrant applications.

[45] **[46]** The only remaining exception to the application of the good-faith exception likewise does not apply because—even assuming the lack of temporal limitations renders them invalid—the warrants are not so facially deficient that reliance on them was unreasonable. The standard of reasonableness in the context of suppression mirrors that in the context of qualified immunity. *See* *Messerschmidt v. Millender*, 565 U.S. 535, 546 n.1, 132 S.Ct. 1235, 182 L.Ed.2d 47 (2012) ("[T]he same standard of objective reasonableness that [applies] in the context of a suppression hearing in *Leon* defines the qualified immunity accorded an officer who obtained or relied on an allegedly invalid warrant." (internal quotation marks and citations omitted)). Thus, "where denial of qualified immunity would be appropriate in the civil context because clearly established law establishes a warrant's invalidity, so too must a court conclude that an officer's conduct was objectively unreasonable for purposes of the good faith inquiry." *Zemlyansky*, 945 F. Supp. 2d at 472. Conversely, where there is no clearly established law establishing a warrant's invalidity, reliance on it cannot be said to be objectively unreasonable for purposes of the good-faith inquiry.

Because there is no consensus in this Circuit as to when temporal limitations are required, *Jacobson*, 4 F. Supp. 3d at 526—or when the lack thereof alone may invalidate an otherwise valid search warrant—the Court cannot here say that "a reasonably well-trained officer would have known that the search was illegal despite the magistrate's authorization." *Leon*, 468 U.S. at 922 n.23, 104 S.Ct. 3405; *see also* *Levy*, 2013 WL 664712, at *11 ("For overbreadth and particularity purposes, no controlling authority requires a specific time frame. In these circumstances, it cannot be said that executing officers should have realized a lack of date limitation constituted a facial deficiency in the Search Warrant such that reliance on it would be unreasonable."); *Cohan*, 628 F. Supp. 2d at 367 (finding the good-faith exception applied under similar ***733** circumstances because "the Second Circuit has never addressed when, if at all, time-frames are a constitutional requirement in business-record search warrants, and district courts in this circuit have not

converged upon a clear rule"). Thus, the Court concludes that, under these circumstances, the warrants were not so facially deficient that reliance upon them was unreasonable, and the good-faith exception applies. Accordingly, even were the Court to find the warrants constitutionally deficient—on particularity or overbreadth grounds—due to their lack of temporal limitations, suppression of search warrant evidence would be unwarranted.

IV. CHALLENGES TO THE EXECUTION OF THE SEARCH WARRANTS

Sadr also argues that the search warrant evidence should be suppressed because the *execution* of the search warrants violated the Fourth Amendment. Specifically, he argues that the responsiveness review the D.A. undertook was unreasonable, and thus unconstitutional, and that the D.A. continued to search the entire set of data long after the responsiveness review was completed in April 2017. Dkt. No. 147 at 11–16; Dkt. No. 156 at 6–12. The Government concedes that "some aspects" of the D.A.'s handling of the entire set of data after April 2017 "were problematic." Dkt. No. 155 at 17. For the reasons stated below, the Court finds that the responsiveness review was reasonable but agrees with Sadr that the D.A.'s handling of the entire set of data after April 2017 was not only problematic but unconstitutional. It concludes that the remedy for this Fourth Amendment violation is, at a minimum, suppression of the 429 pages of the 417 documents that were seized *after* the conclusion of the responsiveness review.

[47] "The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." *United States v. Ramirez*, 523 U.S. 65, 71, 118 S.Ct. 992, 140 L.Ed.2d 191 (1998) (citation omitted); *see also* *Graziano*, 558 F. Supp. 2d at 316 ("[U]nder the Fourth Amendment, the manner of the execution of the warrant in searching the computer also will be subject to judicial review under a 'reasonableness' standard.").

[48] **[49]** **[50]** "A search must be confined to the terms and limitations of the warrant authorizing it." *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988). "[W]hen items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items." *Id.* The "retention of items outside the scope of the warrant can be justified only if the Government meets its burden of demonstrating that those items fall within an exception to the warrant requirement." *Lustyik*, 57 F. Supp. 3d at 230 (citation omitted); *see also* *Vaher v. Town of Orangetown, N.Y.*, 133 F. Supp. 3d 574, 590 (S.D.N.Y. 2015) ("Seizure of items outside the scope of a search warrant is unconstitutional, absent an exception to the Fourth Amendment's warrant requirement").

[51] **[52]** "[T]he drastic remedy of the suppression of *all* evidence seized is not justified unless those executing the warrant acted in 'flagrant disregard' of the warrant's terms." *Matias*, 836 F.2d at 747. "Executing agents are considered to have 'flagrantly disregarded' the warrant's terms where '(1) they effect a widespread seizure of items that were not within the scope of the warrant and (2) do not act in good faith.' " *Pinto-Thomaz*, 352 F. Supp. 3d at 309 (quoting *Shi Yan Liu*, 239 F.3d at 140). The "extreme remedy of blanket suppression should only be imposed in the most extraordinary of cases." *Id.*

*734 A. Responsiveness Review

[53] Under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant may—as the warrants at issue here did—"authorize the seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). The Rule further provides that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." *Id.* The objective of such a responsiveness review is "to determine whether the evidence that the government seized ... fell within the scope of the categories of information sought in the search warrants." *United States v. Metter*, 860 F. Supp. 2d 205, 214–15 (E.D.N.Y. 2012); *see also* Fed. R. Civ. P. 41 Advisory Committee's Note (2009) ("[Rule 41] acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant.").

Sadr argues that the responsiveness review the D.A. conducted to determine what documents fell within the scope

of the search warrants—and thus were properly seized—was unreasonable for three reasons. Specifically, he argues that the D.A. did not use a comprehensive set of search terms in its search and never sorted returns into responsive and non-responsive sets, walling itself off from the latter documents, but rather maintained *all* documents in one continuously-updating database and continued to search all returns over the course of at least three years. Dkt. No. 156 at 10–11. He also argues that the review—and thus the execution of the search warrants—was not performed in a reasonable amount of time. *Id.* Finally, he argues that the seizure of irrelevant documents "confirms that the search warrants imposed no limits." *Id.* at 12–14.

1. Search Terms and Sorting

With respect to the methodology the D.A. employed in conducting its responsiveness review, the Court finds that though the practices Sadr suggests may have been preferable, the D.A.'s failure to follow them did not render the review unreasonable under the circumstances. The Government asserts that the review was conducted by D.A. employees who in many instances were quite familiar with the investigation; these reviewers met and discussed the review of the search warrant returns, including the use of certain search terms, on several occasions; and documents tagged as responsive were typically segregated into responsiveness folders organized by subject matter. *See* Dkt. No. 155 at 19–21. Though it may have been more desirable for the reviewers to have agreed upon a comprehensive set of search terms and consistently removed documents tagged as responsive from the review population over the course of the review, the review methodology was nonetheless reasonable under the circumstances. Indeed, at least one other court in this District has concluded under similar circumstances that the Government's failure to use a search protocol or segregate evidence within the scope of a warrant from evidence outside the scope of a warrant does not violate the Fourth Amendment, because "no authorities hold[ ] that the Fourth Amendment requires anything along those lines for electronic evidence." *United States v. Lumiere*, 2016 WL 7188149, at *4 (S.D.N.Y. Nov. 29, 2016) (finding an electronic search reasonable where no formal document review protocol was followed, documents were not marked "responsive" and "not responsive," responsive documents were not segregated from non-responsive documents, and the "findings" of the search were not "memorialized"). The Court agrees with this authority and concludes ***735** that the Fourth Amendment does not require the practices Sadr argues the D.A. should have employed in its responsiveness review.

2. Duration of Review

[54] As both parties recognize, the review must also have been completed in a reasonable amount of time to comply with the Fourth Amendment and Rule 41's requirements governing the execution of search warrants. *See* *Metter*, 860 F. Supp. 2d at 215 (collecting cases) ("[T]here is no established upper limit as to when the government must review seized electronic data to determine whether the evidence falls within the scope of a warrant," but courts have recognized that "the Fourth Amendment requires the government to complete its review, *i.e.*, execute the warrant, within a 'reasonable' period of time."); *see also United States v. Alston*, 2016 WL 2609521, at *3 (S.D.N.Y. Apr. 29, 2016) ("[T]he time needed to complete off-site copying or review is subject to the rule of reasonableness.").

The Court concludes that the duration of the responsiveness review was reasonable under the circumstances. The responsiveness review in this case concluded around April 2017, roughly three years after issuance of the first search warrant in April 2014 and only one year after issuance of the last warrant in 2016. *See* Dkt. No. 155 at 4. In total, the search warrant returns comprised over one million documents in at least three different languages, *id.* at 18, and the D.A. toggled between review platforms throughout the duration of the review in an attempt to more efficiently process this large volume of documents, *id.* at 4. As the Advisory Committee's Note to Rule 41 explains, "the practical reality is that there is no basis for a 'one size fits all' presumptive period [for the time in which a review must take place]. A substantial amount of time can be involved in the forensic imaging and review of information. This is due to the sheer size of the storage capacity of media, difficulties created by encryption and booby traps, and the workload of the computer labs." Fed. R. Crim. P. 41 Advisory Committee's Note (2009). Given the volume of documents, the various obstacles to review, and the resource constraints under which the D.A. was operating,

the Court concludes that the three years it took the D.A. to complete the search was reasonable under the circumstances.

3. Seizure of Irrelevant Documents

Sadr further argues that the fact that allegedly irrelevant documents were marked responsive "confirms that the search warrants imposed no limits." Dkt. No. 156 at 12–14. As discussed above, though he frames this argument as supporting the invalidity of the warrants themselves due to a lack of particularity, the argument actually bears on whether the search warrants were executed in a reasonable manner. Indeed, Sadr admitted as much at the November 25, 2019 oral argument on this motion. *See* Dkt. No. 173 at 46:25–47:6.

The Court considers the entirety of the universe of documents deemed responsive in determining whether the responsiveness review was conducted reasonably. In doing so, it does not find the allegedly irrelevant documents Sadr cites as compelling the conclusion that the review was unreasonable. The fact that the Government ultimately tagged as responsive fewer than 3,000 documents from a review population of over one million documents indicates that the review was reasonable, and the reviewers were careful to cull from the review population only those documents that fell within the scope of the warrants. *See* Dkt. No. 155 at 21. Indeed, the relatively small number of documents the Government ultimately seized stands in marked contrast to the seizure at issue in ***736** *Wey*—which Sadr cites in support of his "overseizure" argument, Dkt. No. 156 at 12–14—in which the Government seized more than 100,000 electronic documents. *Wey*, 256 F. Supp. 3d at 404. That some much smaller number of the 3,000 documents the Government seized may be irrelevant is not, on its own, sufficient to establish that the responsiveness review was unreasonable.

B. Subsequent Searches

[55] **[56]** Though the Court finds that the responsiveness review was conducted reasonably and thus within the confines of the Fourth Amendment until its completion in April 2017, searches conducted subsequent to the completion of the responsiveness review violated the Fourth Amendment. As an initial matter, Sadr's motion to suppress evidence from subsequent searches is moot with respect to all but the 2,978 pages of the 417 documents that the Government represents it will rely on at trial. *See Mathieu*, 2018 WL 5869642, at *1 (finding that "[d]efendant's motion to suppress is moot as to drmathieu@hotmail.com because the Government does not intend to use information produced from this account at trial"). For the reasons stated below, the Court concludes that 429 of these 2,978 pages must be suppressed because their seizure was in violation of the Fourth Amendment. The Court reserves judgment with respect to the additional 449 pages that constitute the so-called non-Sadr documents and grand jury subpoena returns.

At the conclusion of its responsiveness review in April 2017, the D.A. had identified all of the documents from the entire data set properly seized under the warrants, and the execution of those warrants was thus complete. *See* Dkt. No. 168 at 2 ("[The D.A.'s] review pursuant to the warrants was completed by April 2017."). Documents not identified as responsive at the conclusion of this review "f[e]ll with[out] the scope of the warrant[s]" and thus were not seized pursuant to them. *See* Fed. R. Civ. P. 41 Advisory Committee's Note (2009). Nonetheless, the Government represents that on at least two separate occasions after the conclusion of the responsiveness review, the D.A. conducted searches of the entire set of data. *See* Dkt. No. 155 at 8–10 (describing searches of the entire set of data from April 2017 to March 2018 and in May 2018); *see also* Dkt. No. 168 at 2 ("At times between April 2017 and when the Government produced discovery in May 2018, [D.A.] paralegals were instructed to query the data obtained by [the D.A.] from providers pursuant to the search warrants to retrieve complete versions of documents that previously had been identified for seizure pursuant to the warrants, or to query the database to retrieve documents that members of the [D.A.] team had previously identified for seizure but had not yet segregated. The [D.A.] team also conducted some limited, new searches in the database, including to retrieve documents responsive to Sadr's bail motion."). Because these searches were conducted following the conclusion of the responsiveness review—and thus the execution of the warrants—they exceeded the scope of the warrants' authority. Accordingly, documents first identified as responsive during these searches were seized outside the scope of the search warrants.

Because documents seized following the conclusion of the responsiveness review were seized outside the scope of the

search warrants, they are subject to suppression unless "the Government meets its burden of demonstrating that those items fall within an exception to the warrant requirement." *Lustyik*, 57 F. Supp. 3d at 230 (citation omitted). The Government has not identified any exception that would justify the retention of documents seized after the conclusion of the responsiveness review, ***737** and the Court is aware of none. Accordingly, the proper remedy is suppression.

The Court concludes that 429 pages of the 2,978 the Government intends to rely on at trial were first identified as responsive after the conclusion of the responsiveness review and thus must be suppressed. *See* Dkt. No. 155 at 8–10; *see also* Dkt. No. 168 at 2. Though other portions of these documents or related documents *were* identified as responsive at the conclusion of the responsiveness review, the Government concedes that these 429 pages "were [not] identified for seizure by April 2017 in connection with reasonable searches conducted pursuant to the warrants." Dkt. No. 168 at 5. These pages include attachments for which the parent email or a related parent email was identified by April 2017 (Government categories 5 and 6); pages for which a related version or related version and attachment were identified by April 2017 (Government categories 7 and 8); a parent email for which the attachment was identified by April 2017 (Government category 9); and other portions of documents identified by April 2017 (Government category 10). [6]

The Government's argument that it is nonetheless entitled to rely on these documents is unavailing. It cites to *Lumiere* for the proposition that responsive, identified evidence need not be segregated from documents outside the scope of the warrant during the responsiveness review. *See* *Lumiere*, 2016 WL 7188149, at *4–5. However, the issue here is not one of segregation of documents within the scope of the warrants from those without but rather one of whether these pages were identified as falling within the scope of the warrants during the responsiveness review to begin with. Because the Government cannot demonstrate that these 429 individual pages were identified as responsive at the conclusion of the responsiveness review, their subsequent identification exceeded the scope of the warrants and they must be suppressed.

The Government may rely on 2, 100 of the 2,978 pages it represents it intends to rely on at trial. *See* Dkt. No. 168 at 1. These pages include those located in binders provided by the D.A. to the U.S. Attorney's Office in April 2017 (Government category 1); those with a PDF modified date of April 2017 or earlier (Government category 2); those with a print date of April 2017 or earlier (Government category 3); those identical to content identified by April 2017 (Government category 4); and those referenced in documents created by April 2017 but not specifically segregated by that time (Government category 11). Pages in categories 1, 2, and 3 were clearly seized during the responsiveness review. Furthermore, there is no basis to suppress pages in category 4, as they are identical to content seized during the responsiveness review. Though the pages comprising category 11 may not have been *segregated* from the non-responsive documents by the conclusion of the responsiveness review, the Government's analysis demonstrates that they were identified as responsive—and thus seized—by that time. Indeed, they were included in work product that was created prior to April 2017 "based on their evidentiary value in the ongoing investigation." Dkt. No. 168 at 4; *see also* *Lumiere*, 2016 WL 7188149, at *4 (rejecting defendant's argument "that the Government violated the Fourth Amendment by failing to 'segregate' evidence within the scope of the warrant from evidence outside the scope of the warrant"). In this way, these pages are distinct from the 429 pages subject to suppression, which were ***738** neither seized *nor* segregated by the conclusion of the responsiveness review.

The Court reserves judgment with respect to the final two categories of pages—Government category 12, pages from the so-called non-Sadr documents, and Government category 13, pages from grand jury subpoena returns. The Government argues that Sadr does not have standing to seek the suppression of non-Sadr documents, but Sadr disagrees, at least with respect to email accounts that belonged to his companies. *Compare* Dkt. No. 168 at 5 ("[An] additional 449 pages are not subject to challenge by Sadr because they are confirmed Non-Sadr documents (440 pages)....") *with* Dkt. No. 176 at 2–3 (arguing that Sadr has Fourth Amendment standing with respect to email accounts that belonged to single-member LLCs of which he was the sole owner). The Government also argues that Sadr does not have standing to seek the suppression of grand jury subpoena returns because they "were obtained pursuant to a grand jury subpoena rather

than a search warrant." Dkt. No. 168 at 4. However, a grand jury subpoena may constitute a search, *see United States v. Meregildo*, 876 F. Supp. 2d 445, 450 (S.D.N.Y. 2012), and Sadr implies that the grand jury subpoena returns here are the product of a potentially unconstitutional Fourth Amendment search. *See* Dkt. No. 175 at 2 (requesting a suppression hearing to determine which pages of the grand jury subpoena returns were actually seized by April 2017). In the absence of the parties resolving their disputes with respect to these categories of pages, the Court requires further briefing on them. Accordingly, the parties shall meet and confer and propose an expedited briefing schedule, if necessary, within seven days of the date of this Opinion and Order.

In sum, the Court suppresses 429 pages of the 2,978 the Government intends to rely on at trial. The Government may rely at trial on the 2,100 pages identified above,[7] and the Court reserves judgment with respect to the remaining 449 pages. With respect to the categories of pages the Court is able to rule on at this juncture, the Court concludes that it need not hold an evidentiary hearing and decides Sadr's suppression motion on the papers. *See United States v. Watson*, 404 F.3d 163, 167 (2d Cir. 2005) ("[A]n evidentiary hearing on a motion to suppress ordinarily is [not] required [unless] 'the moving papers are sufficiently definite, specific, detailed, and nonconjectural to enable the court to conclude that contested issues of fact going to the validity of the search are in question.' " (citation omitted)).

V. MOTION FOR RETURN OF PROPERTY

At the November 25, 2019 oral argument on this motion, the Government consented to the return of the non-responsive documents, *see* Dkt. No. 173 at 61:17–23, and on December 9, 2019, Sadr submitted ***739** a proposed order for their return with which the Government agreed as to form. *See* Dkt. No. 165; Dkt. No. 165-1. Subsequent to his submission of this proposed order, however, the Government submitted a letter objecting to the proposed order's inclusion of two email accounts "that do not belong to" Sadr. *See* Dkt. No. 171 at 1. This dispute also centers on Sadr's standing to seek the suppression of some subset of so-called non-Sadr documents. Accordingly, to the extent the parties are unable to resolve this dispute on their own, they shall brief it in conjunction with the supplemental suppression briefing discussed above, and the Court will resolve this issue in due course upon receiving the parties' supplemental briefing. If the parties are able to resolve this dispute on their own, they shall submit a revised proposed order for the return of property within seven days of the date of this Opinion and Order.

VI. MOTION TO EXCLUDE

In light of the Government's representation that it will not rely on the 622 untimely produced non-Sadr documents at trial, Sadr's motion to exclude those documents is moot.

VII. CONCLUSION

For the foregoing reasons, the Court GRANTS in part, DENIES in part, and RESERVES JUDGMENT in part on Sadr's motion to suppress search warrant evidence, DENIES his corollary requests for a *Franks* hearing, RESERVES JUDGMENT on his return of property motion, and DENIES as moot his motion to exclude.

Within seven days of the date of this Opinion and Order, the parties shall either submit an expedited briefing schedule for supplemental briefing or inform the Court that no such briefing is necessary and submit a proposed order for the return of property. Should a briefing schedule be necessary, within fourteen days of the date of this Opinion and Order, the Government shall provide the Court with a page-by-page analysis of when each page of the subset of so-called non-Sadr documents that Sadr claims he has Fourth Amendment standing to seek the suppression of was first identified as responsive. It shall do the same with respect to each page of the grand jury subpoena return documents if Sadr also continues to seek their suppression.

This resolves Docket Nos. 95, 97 and 148.

SO ORDERED.

All Citations

436 F.Supp.3d 707

Footnotes

1 References to the Government throughout this Opinion and Order refer to the United States Attorney's Office for the Southern District of New York.

2 Sadr notes that the affidavits in support of the June 2014 and October 2015 warrants contain "largely the same recycled allegations from the April 2014 warrant affidavit." Dkt. No. 96 at 4. Accordingly, the Court focuses on the April 2014 affidavit here.

3 Notably, the Government does not argue that the Court should consider the warrant affidavits in its particularity analysis, and the Court does not do so.

4 Sadr also argues in his supplemental briefing that the executing agents' identification of allegedly irrelevant documents as responsive "confirms" the warrants' lack of particularity. *See* Dkt. No. 156 at 12–14. However, for reasons the Court explains below, to the extent there are any particularity problems with the warrants, they pertain only to their lack of temporal limitations. That some number of the fewer than 3,000 documents the Government ultimately seized from the over one million documents it reviewed may be irrelevant does not affect the Court's conclusion with respect to the *validity* of the warrants. Nonetheless, this argument is relevant to whether the *execution* of the warrants conformed with the Fourth Amendment, and thus the Court addresses it in more detail below.

5 Moreover, the warrants in the two cases he cites that do involve electronic information were ultimately found to be lacking particularity because they failed to identify *any* specific suspected crimes and are thus inapposite. *See* *United States v. Rosa*, 626 F.3d 56, 58 (2d Cir. 2010); *Wey*, 256 F. Supp. 3d at 384.

6 The category numbers the Court references correspond to those used by the Government in its December 9, 2019 letter. *See generally* Dkt. No. 168.

7 Contrary to Sadr's contentions, there is no basis for blanket suppression of any documents seized *prior* to the conclusion of the responsiveness review. The 2,100 pages identified above were properly seized during the course of a reasonable responsiveness review, and blanket seizure is not justified in this case. Indeed, "the drastic remedy of the suppression of *all* evidence seized is not justified unless those executing the warrant acted 'in flagrant disregard' of the warrant's terms." *Matias*, 836 F.2d at 747. As discussed above, there is scant evidence that the D.A. "effect[ed] a *widespread* seizure of items that were not within the scope of the warrant" and no evidence that it "d[id] not act in good faith." *Pinto-Thomaz*, 352 F. Supp. 3d at 309 (emphasis added) (quoting *Shi Yan Liu*, 239 F.3d at 140). The record is thus devoid of any suggestion that this is one of "the most extraordinary of cases" in which the "extreme remedy of blanket suppression should ... be imposed." *Id.*

2020 WL 5549931
Only the Westlaw citation is currently available.
United States District Court, S.D. New York.

UNITED STATES of America,
v.
Ali Sadr Hashemi NEJAD, Defendant.

18-cr-224 (AJN)
|
Signed 09/16/2020

Synopsis

Background: After defendant's convictions were vacated in prosecution for conspiracy to defraud the United States, conspiracy to violate the International Emergency Economic Powers Act, bank fraud, bank-fraud conspiracy, and money laundering, and after indictment had been dismissed with prejudice, government was ordered to provide information regarding *Brady* violations, and government's response indicated government's previous lack of candor to the court.

[Holding:] The District Court, Alison J. Nathan, J., held that Acting United States Attorney would be ordered to ensure that all current Assistant United States Attorneys (AUSA) and Special Assistant United States Attorneys (SAUSA) would read district court's opinion.

Reading of opinion ordered; preparation of declarations ordered.

Procedural Posture(s): Post-Trial Hearing Motion.

West Headnotes (5)

[1] District and Prosecuting Attorneys

Federal prosecutors, like all parties that appear before the court, have ethical duties of candor.

[2] Searches and Seizures

Review of search-warrant returns must be done in conformity with the warrants themselves. U.S. Const. Amend. 4.

[3] Criminal Law

District court retained its authority to sanction the prosecutors, or to make a referral to the Grievance Committee of the Southern District of New York if district court determined that the prosecutors acted in bad faith in violating their *Brady* disclosure violations and in making a misleading statement to the court, though defendant's motion for new trial had been granted, the jury verdict against him had been vacated, and the indictment had been dismissed with prejudice, in prosecution for in prosecution for conspiracy to defraud the United States, conspiracy to violate the International Emergency Economic Powers Act, bank fraud, bank-fraud conspiracy, and money laundering.

[4] District and Prosecuting Attorneys

In the singular role that federal prosecutors play in the justice system, the United States Attorney is the representative not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all, and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done, and a U.S. Attorney may prosecute with earnestness and vigor, and indeed he should do so, but while he may strike hard blows, he is not at liberty to strike foul ones; it is as much his duty to refrain from improper methods calculated to produce a wrongful conviction as it is to use every legitimate means to bring about a just one.

[5] District and Prosecuting Attorneys

In light of singular role that federal prosecutors played in justice system, Acting United States Attorney would be ordered to ensure that

all current Assistant United States Attorneys (AUSA) and Special Assistant United States Attorneys (SAUSA) would read district court's opinion, issued after defendant's motion for new trial had been granted, after jury verdict against him had been vacated, and after indictment had been dismissed with prejudice, if prosecutors' individual declarations, which would be completed under penalty of perjury, showed that prosecutors acted in bad faith in violating their *Brady* disclosure violations and in making a misleading statement to the court, in prosecution for conspiracy to defraud the United States, conspiracy to violate the International Emergency Economic Powers Act, bank fraud, bank-fraud conspiracy, and money laundering.

Attorneys and Law Firms

Andrew James DeFilippis, Jane Kim, Michael Kim Krouse, Matthew Joseph LaRoche, Pro Hac Vice, Assistant U.S. Attorney, Rebekah Allen Donaleski, David William Denton, Jr., Emil Joseph Bove, III, Shawn Geovjian Crowley, Stephanie Lindsay Lake, United States Attorney's Office, New York, NY, for USA.

OPINION & ORDER

ALISON J. NATHAN, District Judge:

***1** **[1]** Federal prosecutors have constitutional and statutory duties to disclose many types of evidence to defendants. This principle of disclosure is central to our criminal-justice system. "A prosecutor that withholds evidence on demand of an accused which, if made available, would tend to exculpate him or reduce the penalty helps shape a trial that bears heavily on the defendant ... That casts the prosecutor in the role of an architect of a proceeding that does not comport with standards of justice." *Brady v. Maryland*, 373 U.S. 83, 87–88, 83 S.Ct. 1194, 10 L.Ed.2d 215 (1963). And federal prosecutors, like all parties that appear before the Court, have ethical duties of candor. *United States v. Universita*, 298 F.2d 365, 367 (2d Cir. 1962) ("The prosecution has a special duty not to mislead; the government should, of course, never make affirmative statements contrary to what it knows to be the truth."). In the near decade the Undersigned has sat on the bench in the Southern District of New York, the vast majority of Assistant United States Attorneys before the Court have embraced their disclosure obligations, worked diligently to meet them, and forthrightly admitted when they did not.

But not all. In this case, federal prosecutors have by their own admission repeatedly violated their disclosure obligations and, at best, toed the line with respect to their duty of candor. Over the course of years in this prosecution—before, during, and after trial—the Government has made countless belated disclosures of arguably (and, in one instance, admittedly) exculpatory evidence. For some pieces of evidence, the Government provides plausible explanations for its late disclosure. For others, it provides no explanation at all. And when the Court pressed for more information about one of these failures, the Government made a misrepresentation to the Court. This serious dereliction requires a serious response.

The story begins in 2018, with the Government's indictment of Mr. Sadr. After a two-week trial in March 2020, a jury found him guilty on five counts. But in part because of its disclosure failures, the Government later agreed that the Court should grant Mr. Sadr's motion for a new trial, vacate his guilty verdict, and dismiss the indictment against him with prejudice. The Court did just that, thus ending this criminal proceeding with respect to Mr. Sadr—but it is not the end of the matter. As this Court stated to the Government lawyers at trial and in several later orders, the serious and pervasive issues related to disclosure failures and misleading statements to the Court by at least one or more of the Government lawyers must be addressed separate and apart from the resolution of this case against Mr. Sadr. *See* Trial Tr. at 998:8–9; Dkt. Nos. 350, 357.

Consistent with that view, after dismissing the indictment, the Court pressed the Government for more information about its disclosure failures and misstatements. Unfortunately, the response from the United States Attorney's Office (USAO) for the Southern District of New York has been inadequate. To be clear, the Court does commend the USAO for admitting error and ultimately seeking to do justice in this case. But the dismissal of charges is not a basis for sweeping the Government's repeated failures under the rug. Nor does the

dismissal of the indictment obviate the need for inquiry into whether the Government intentionally and in bad faith withheld exculpatory evidence or intentionally misled the Court.

***2** The Court hoped that the Government's response would create a record sufficient to resolve these issues. Instead, the Government revealed an array of additional errors, including disclosure failures and new admissions of misconduct related to the Government's handling of search-warrant returns.

The Government also revealed new, highly problematic internal communications between the AUSAs who prosecuted this case. In particular, in the middle of trial, Government lawyers allegedly realized for the first time that they had not turned over a particular document to the defense. Instead of immediately disclosing that file, Government lawyers spent almost twenty hours strategizing how best to turn it over. One prosecutor suggested to another that they "bury" the evidence along with other, already-disclosed documents, and the second prosecutor agreed. And after looping in more prosecutors, the Government did just that, obfuscating its disclosure. The Government now admits that this document had exculpatory value for Mr. Sadr. Disappointingly, the leadership of the USAO has failed to unequivocally condemn these prosecutors' improper actions and communications, and the Court has not been ensured that an investigation by the Department of Justice's Office of Professional Responsibility will take place. A further response is therefore required from the Court.

Such a response includes making a clear record of the Government's failures in this case in an effort to prevent these issues from reoccurring. The Court thus begins by recounting the factual and procedural background of this prosecution. The Court then details the Government's many search-warrant and disclosure-related failures and urges structural solutions. This factual recitation is based on information provided by the Government. The Court then narrows its focus to a single piece of evidence disclosed mid-trial, and concludes that the Government both violated its disclosure obligations and subsequently made a misrepresentation to the Court about its conduct. The Court finally orders additional fact-finding and briefing to determine whether any of the Government lawyers in this case either intentionally withheld exculpatory evidence or intentionally misled the Court about one of the late disclosures.

Government lawyers wield enormous prosecutorial power. They must exercise it in a way that is fully consistent with their constitutional and ethical obligations. And it is the obligation of the courts to ensure that they do and hold them accountable if they do not.

I. DISCLOSURE AND SUPPRESSION FAILURES RESULT IN DISMISSAL OF THE INDICTMENT

In March 2018, the Government charged Mr. Sadr with conspiracy to defraud the United States, conspiracy to violate the International Emergency Economic Powers Act, bank fraud, bank-fraud conspiracy, money laundering, and money-laundering conspiracy. Dkt. No. 2. Over one year later, this case was transferred to the Undersigned. This Court presided over extensive pretrial litigation—including suppression litigation—after which Mr. Sadr's case proceeded to trial. *See* Dkt. Nos. 164, 197. The Court held a two-week trial in early March 2020, during which the jury continued to serve diligently despite the onset of the COVID-19 pandemic in New York City. On March 16, 2020, the jury convicted Mr. Sadr on five counts, finding him guilty on all but the money-laundering-conspiracy charge. *See* Dkt. No. 310. The Government asked that Mr. Sadr immediately be taken into federal custody, but the Court denied this request. *See* Trial Tr. at 2129:1–10.

***3** After the trial, Mr. Sadr moved for acquittal as a matter of law or, in the alternative, for a new trial. Dkt. No. 335. Although the Court was assured in March that the disclosure issues in this case were being raised at the "level of the U.S. Attorney," Trial Tr. at 996:6–10, it was apparently not until the end of May 2020 that the USAO's Criminal Discovery Coordinator and Professional Responsibility Officer "began" looking into disclosure issues in this case. Dkt. No. 352 at 1. As a result of this inquiry—and while Mr. Sadr's motion remained pending—the Government determined that it would not be in the "interests of justice" to further prosecute this case. Dkt. Nos. 348, 348-1. It thus took the extraordinary step of asking the Court to enter an order of *nolle prosequi* as to the indictments filed against both Mr. Sadr and his co-defendant Bahram Karimi. *Id.*

While Mr. Sadr agreed that the indictment against him should be dismissed with prejudice, he disagreed with the Government's proposed procedural mechanism for dismissal.

See Dkt. Nos. 349. The Government eventually acceded to Mr. Sadr's request that the verdict be vacated and a new trial be granted under Federal Rule of Criminal Procedure 33(a), and that the indictment subsequently be dismissed with prejudice under Rule 48(a). *See* Dkt. Nos. 360, 361. On July 17, 2020, the Court therefore granted Mr. Sadr's motion for a new trial, vacated the verdict against him, and dismissed the indictment with prejudice. *See* Dkt. No. 362. The Court's July 17 Order referenced the Government's explicit acknowledgement of the "disclosure-related issues that arose during the March 2020 trial as well as in pre- and post-trial motion practice, including with respect to pretrial suppression litigation." *See id.* (quoting Dkt. No. 348).

As noted, the Court commends the USAO's admission of error and effort to do justice in this case by agreeing to dismiss the indictment. Better late than never. Still, that dismissal cannot be a basis for failing to grapple fully with the Government's many errors in this prosecution.

II. THE EXISTING RECORD EXPOSES SIGNIFICANT ERRORS

Before granting Mr. Sadr's motion for a new trial and vacating his conviction, the Court ordered the Government to respond to a series of questions addressing disclosure-related issues and any associated misrepresentations or misstatements made to the Court. *See* Dkt. No. 350. The Government's responses not only detailed issues already familiar to the Court, but they also raised—for the first time, over two years after this case was charged and over two months after a jury found Mr. Sadr guilty on five counts—a slew of search-warrant-related issues implicating the Fourth Amendment. Several of these issues, both new and old, suggest patterns that may extend beyond this case and require systemic solutions.

A. Suppression Issues

The Court begins briefly with suppression issues raised by the Government for the first time in its July 2, 2020 letter. *See* Dkt. No. 354. To understand these issues, some background is helpful: The Manhattan District Attorney's Office (DANY) investigated this matter for state-law crimes before referring the case to the USAO. During its state-law investigation, DANY executed search warrants of various email accounts, including Mr. Sadr's personal email accounts. *See, e.g.*, Dkt. No. 96-1. The affidavit in support of one warrant cited "reasonable cause to believe that evidence of the crimes of Money Laundering [under New York State Law,] as well as attempt and conspiracy to commit said crimes, may be found" in these email accounts. *Id.* at 3–4. And the warrant authorized "members of the New York County District Attorney's Office" to seize and search these documents. *Id.* at 38–39. Some of those emails were later turned over to the USAO, and the Government viewed their content as "particularly incriminating and pertinent." Dkt. No. 147-3. Mr. Sadr however argued in his pretrial motions that much of this evidence should be suppressed. The Court only partially granted his request, rejected most of Mr. Sadr's arguments, and allowed the Government to rely upon thousands of pages of seized documents. *See United States v. Sadr*, 436 F. Supp. 3d 707, 736–38 (S.D.N.Y. 2020).

***4** **[2]** During this extensive pretrial suppression litigation, Government lawyers consistently argued that DANY searched those state email search-warrant returns for material pertinent to violations of state law alleged in those warrants. Dkt. No. 354 at 16. In September 2019, the Government specifically represented to Mr. Sadr "that the email search warrant returns had been reviewed by DANY personnel and that after the DANY review had ended ..., 'hot docs' were provided to the U.S. Attorney's Office." *See id.*; *see also* Dkt. No. 147-3. But over six years after the first of these state email search warrants was issued, the Government now informs the Court—and Mr. Sadr—that in fact federal investigators were mining the state search-warrant returns for federal crimes without authorization of a warrant. Dkt. No. 354 at 6, 16. The Government confesses that "early on in the DANY investigation, the FBI had had DANY personnel search email data in general support of at least one witness interview, and that the FBI *was investigating federal crimes rather than the state-law offenses at issue in the warrants, contrary to arguments [the Government] made during suppression litigation.*" Dkt. No. 354 at 6 (emphasis added). The Government further acknowledges "that the FBI was seeking to use material gathered in response to the state email search warrants in aid of FBI interviews, and to further investigation of federal charges." *Id.* at 7. This conduct was likely unconstitutional because review of search-warrant returns must be done in conformity with the warrants themselves. *See generally* *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) ("A search must be confined to the terms and limitations of the warrant authorizing it.").

Moreover, the Government now admits that a central premise of its pretrial arguments opposing Mr. Sadr's suppression motion was directly contrary to what actually occurred during the investigation of this case.

The Court cannot state with certainty the outcome of the pretrial suppression litigation had these additional search-warrant-related issues come to light earlier. But it is certainly possible, as Mr. Sadr argues, that had the Government "disclosed the true facts [regarding the execution of the state email search warrants] to [him], the email evidence would have been suppressed, and the trial would have been avoided altogether." Dkt. No. 355 at 5. Indeed, one of the Government's arguments in seeking dismissal of the indictment against Mr. Sadr's co-defendant Bahram Karimi, who was not tried (and thus not prejudiced by the late disclosure issues discussed extensively below), is that the discovery of the FBI's involvement in DANY's investigation creates a "substantial risk that essential email evidence would be suppressed." Dkt. No. 354 at 7. What is clear, however, from the Government's belated revelations is that the USAO for SDNY specifically, and the Department of Justice more broadly, must implement policy and training procedures that instill in FBI agents the permissible limits of searching electronic warrant returns in a way that conforms to constitutional requirements. Moreover, AUSAs must be trained to conduct proper due diligence about the conduct of investigating agents *before* making misleading representations to the Court about that conduct. *See, e.g.*, Dkt. No. 155 at 3–4 (describing searches of state email search-warrant returns from April 2014 to April 2017, but nowhere mentioning FBI investigation of federal crimes during this period). And if any of the Government lawyers made (or allowed others to make) knowing misrepresentations to the Court in opposing the motion to suppress, as Mr. Sadr argues likely occurred, Dkt. No. 355, their conduct would constitute an egregious ethical violation.

In light of the dismissal of the indictments here, there will be no further litigation of these issues before the Court. Accordingly, it is the view of the Court that the suppression issues belatedly revealed by the Government in its July 2 letter, Dkt. No. 354, ought to be the subject of a referral to the Department of Justice's Office of Professional Responsibility for a full investigation.

B. Disclosure Issues

The Court next turns to the numerous disclosure-related issues that arose prior to, during, and after Mr. Sadr's trial. Disclosure-related issues first arose shortly after this case was transferred to the Undersigned and have—disturbingly—continued unabated since. The Court and Mr. Sadr were made aware of the first of these issues in a conference held on September 9, 2019. At that conference, the Government revealed to Mr. Sadr for the first time information it had learned back in May 2019—namely, that "there were custodians searched and documents seized ... that were not produced in [the] initial Rule 16 discovery." Dkt. No. 137 at 35:5–7. At that point in time, Mr. Sadr believed—based on representations made by the Government—that Rule 16 discovery had been closed for over a year. *See id.* at 40:11–19. The Government did not uncover these discovery-related issues until new prosecutors came into the case in the spring and summer of 2019 and, "in the process of attempting to understand the case," asked questions of former prosecutors regarding the production of documents to the defense. *See id.* at 35:14–22. As a result of the Government's failure to timely comply with its discovery obligations, it agreed not to rely on any of the untimely produced documents at trial. *See* Dkt. No. 155 at 11; Dkt. No. 173 at 38:24–39:4.

***5** The next disclosure-related issue arose during trial, shortly before the Government rested. Though the Court discusses issues surrounding Government Exhibit (GX) 411 in greater detail below, *see* Section III, it mentions the Government's failure to timely disclose this exhibit here to situate it within the larger pattern of the Government's failure to satisfy its disclosure obligations under the Constitution and the Federal Rules of Criminal Procedure. GX 411 is a letter sent by Commerzbank to the Office of Foreign Assets Control (OFAC) flagging the first payment charged in this case. *See* Dkt. No. 274-1. The failure to timely disclose this exhibit precipitated a cascade of failures to timely disclose related materials—including materials from DANY's and the USAO's earlier investigations of Commerzbank and communications with OFAC—some of which were not disclosed until after the trial in this case had concluded. *See* Dkt. No. 354 at 3, 8–9.

The belated disclosures did not stop there. The Government disclosed several additional possibly exculpatory documents *after* the trial in this case ended. Perhaps the most egregious of

these relate to two interviews of Mr. Sadr's co-defendant, Mr. Karimi. First, a recording was made by Canadian authorities of a January 22, 2020 interview with Mr. Karimi. *See* Dkt. No. 307-1 at 2. On February 3, 2020, after Mr. Karimi's public indictment, counsel for Mr. Sadr requested Mr. Karimi's witness statements. *See id.* at 3. On February 11, 2020, the FBI New York office received a recording of the January 22, 2020 interview of Mr. Karimi. *See id.* at 4. By the next week, the FBI special agents were aware that the FBI was in possession of the recording—but they did not inform the prosecutors of this fact. *See id.* Due to communication breakdowns between the prosecutors and the FBI, the prosecutors informed Mr. Sadr on two separate occasions—first on February 23, 2020, and again on March 10, 2020—that the FBI had requested but not yet received the recording from Canadian authorities. *See id.* at 5. After trial ended, an AUSA followed up with the FBI and learned that the recording *had been in the FBI's possession since before the trial had started. See id.* at 5–6. The Government finally produced the recording to Mr. Sadr on March 31, 2020, over two weeks after Mr. Sadr's trial had ended. *See id.* at 6.

Second, a classified FD-1057 report was created from an interview with Mr. Karimi on September 14, 2016. *See* Dkt. No. 354 at 5. Yet despite multiple communications with the FBI, beginning in 2017, regarding discoverable information, the prosecutors on this case did not learn of the FD-1057 Karimi report until an AUSA conducted an "on-site personal review of the FBI case file" in *mid-May 2020*, two months after trial. *Id.* As a result, this report was not declassified and disclosed to Mr. Sadr until May 19, 2020. *Id.* The Government attributes the failure to timely disclose this report, as well as the recording discussed above, to breakdowns in communication between prosecutors and the FBI. Troublingly, the Government makes little effort to explain in detail *why* or *how* these communication breakdowns came to pass, or *why* the prosecutors—well aware of their constitutional and statutory obligations—were not more diligent in communicating with the FBI.

The final category of disclosures made after trial consists of three FBI interview reports (FD-302s) of interviews with Victor Aular, the former CFO and Director of a Venezuelan state-owned oil company, that took place in early 2016. *See* Dkt. No. 354 at 3–4. The parties dispute whether these interviews constitute *Brady* material that the Government was required to disclose. *Compare* Dkt. No. 354 at 3–4 *with* Dkt. No. 355 at 4. But the Government concedes that "even if not required to be disclosed, the Aular 302s *should have been* disclosed ahead of trial as a matter of good practice so that potential defense theories about Sadr's state of mind ... and the admissibility of Aular's statements, could have been developed and addressed in an orderly fashion in limine." Dkt. No. 354 at 4 (emphasis added). Setting aside whether these interview reports constitute *Brady* material, the Government's handling of them reveals failures in its treatment of potentially exculpatory material. Specifically, at the end of January 2020, the prosecutors discussed whether they were required to disclose the Aular 302s under *Brady*. One prosecutor suggested that it "could be worth running [the question] by a chief," but the AUSAs inexplicably "*did not further pursue the question*" and did not ultimately disclose the interview reports to Mr. Sadr pre-trial. *See id.* (emphasis added). Especially in light of the trial blinders that prevented it from timely disclosing conceded *Brady* material to Mr. Sadr, *see* Section III, the Government's failure to further pursue the question of whether the Aular 302s were required to be disclosed under *Brady* is shocking. And even if the Government had considered the *Brady* question and concluded that the Aular 302s did not constitute *Brady* material, the Court agrees that the 302s should nonetheless have been disclosed in advance of trial as a matter of good practice. *See* *Cone v. Bell*, 556 U.S. 449, 470 n.15, 129 S.Ct. 1769, 173 L.Ed.2d 701 (2009) (noting that a prosecutor's ethical "obligation to disclose evidence favorable to the defense" may be broader than constitutional or statutory duties) (citing ABA Model Rule of Professional Conduct 3.8(d)). Better training and an expansive approach to the Government's discovery obligations would help ensure that, in the future, "trial blinders" do not cause AUSAs to wrongfully withhold potentially exculpatory evidence.

***6** The Court turns finally to the Government's complete failure to produce certain classified material at any point—either before, during, or after trial. During its post-trial review, the Government discovered additional classified material subject to Rule 16 disclosure that was never declassified and disclosed to Mr. Sadr. *See* Dkt. No. 354 at 5. It does not explain why this material was discovered only after trial, and it maintains that, following its application for an order of *nolle*

prosequi, the components of the United States Government involved in the handling of classified information would have been unlikely to authorize use of the information. *See id.* As a result, this classified material has never been disclosed to Mr. Sadr.

C. These Issues Call for Systemic Solutions

Having set forth several of the suppression and disclosure-related issues that plagued the prosecution in this case, the Court notes some common themes that have emerged. The issues discussed above appear to have been precipitated by one or a number of the following factors:

1. The sheer number of prosecutors who worked on this case (fourteen total—seven line prosecutors, one Special Assistant United States Attorney (SAUSA), and six supervisors, *see* Dkt. No. 354 at 1–2);

2. The frequency with which different prosecutors subbed into and out of the case, *see id.*;

3. The number of AUSAs on the trial team (this case was tried by four Government lawyers);

4. A failure to coordinate and effectively communicate with the Manhattan District Attorney's Office;

5. Failures to communicate between the AUSAs and the Special Assistant United States Attorney appointed from DANY;

6. Breakdowns in communication between the FBI and line prosecutors, including regarding the FBI's investigation of this case;

7. Insufficient training of FBI agents and AUSAs on appropriate limits to searches of electronic search-warrant returns;

8. Insufficient training for all participating AUSAs and the SAUSA on disclosure obligations;

9. Insufficient policies in place that ensure timely and complete compliance with disclosure obligations; *and*

10. Insufficient supervision of disclosure obligations by the USAO's Unit Chiefs.

It is possible that the issues articulated above, as well as the precipitating factors the Court identifies, are not unique to this case. Indeed, in the last criminal case tried before the Undersigned, the Government also seriously breached its *Brady* obligations. *See United States v. Robert Pizarro*, No. 17-cr-151 (AJN). Following that revelation, the Court was repeatedly assured by the leadership of the USAO that the matter was being taken seriously, would be systemically addressed through training, and would not reoccur. No. 17-cr-151 (AJN), Dkt. No. 135 at 8:11–10:10, 58:2–15. The record before the Court in this case belies those assurances.

It is impossible for the Undersigned alone to address and resolve these issues. Here too, it is thus the Court's view that these errors should be investigated by DOJ's Office of Professional Responsibility. Moreover, the manifold problems that have arisen throughout this prosecution—and that may well have gone undetected in countless others—cry out for a *coordinated, systemic* response from the highest levels of leadership within the United States Attorney's Office for the Southern District of New York. The Court implores the Acting United States Attorney to take seriously the numerous deficiencies set out in detail above and to take action to ensure future prosecutions brought under the aegis of her office do not suffer from the same. In that regard, the Court will prescribe her first order of business: the Acting United States Attorney shall ensure that all current AUSAs and Special AUSAs read this Opinion.

III. THE GOVERNMENT'S FAILURE TO DISCLOSE EXHIBIT 411

***7** The Court next turns to a narrower set of concerns related to Government Exhibit 411. The Court concludes that the Government failed to satisfy its disclosure obligations with respect to this exhibit and then made a misrepresentation to the Court about its conduct. Unfortunately, following the Government's July 2 letter, there remain several significant open questions regarding the Government's conduct that this Court is obligated to resolve. As explained below, further fact-finding by the Court is necessary.

A. The Government Admits GX 411 is Exculpatory

Before diving into the Government's failure to timely disclose GX 411, it is helpful to catalogue the contents of this

document and explain why the Government now concedes that it has exculpatory value for Mr. Sadr.

The document that came to be known as Government Exhibit 411 is a 2011 letter from the New York branch of Commerzbank, a German financial institution, to the Treasury Department's Office of Foreign Assets Control. *See* Dkt. No. 274-1 (GX 411). In this letter, Commerzbank's New York branch informs OFAC of an approximately $30 million payment from a Venezuelan entity to Stratus International Contracting Company. As noted, this payment is the first payment charged in this case. The letter further provides information about Stratus and notes that the "purpose of the payment is for the construction of a 7000 apartment unit project" in Venezuela. *Id.* The letter goes on to say that "Although Stratus is not listed as an SDN [Specially Designated National], and the payment does not indicate any direct involvement of Iran or with Iran, due to conflicting information between [Stratus's] website and the response forwarded by the [Venezuelan bank], [Commerzbank] believes it appropriate to share this information with OFAC since Stratus may be an Iranian Company." *Id.* The letter concludes by noting that Commerzbank had added Stratus "into [its] sanctions filter to monitor any future payments," that Commerzbank had not processed any other transactions involving Stratus, and that this information was being provided to OFAC in hopes of complying with Commerzbank's sanctions-related reporting requirements. *Id.*

The Government maintains that for years it viewed the letter as wholly inculpatory. Specifically, the Government argues that GX 411 was "helpful [to its case-in-chief] because it showed that the information the defendant was trying to hide from the bank was material to the bank, which wouldn't have processed the transaction if it knew it was connected to Iran, and that the bank put the name of the company on its sanctions filter." Dkt. No. 354 at 11; *see also* Trial Tr. at 986:7–16 (The Court: "In the course of this discussion was there any notion as to [GX 411's] potential use to the defense case, having yourselves sat through a week of trial, heard rulings on objections, heard the defendant's opening, in any of that discussion, right at the moment you're talking about, is there the thought: Whether we want to use this or not, it needs to be turned over?" The Government: "Candidly, your Honor, no, there was not that discussion. The discussion was solely about how inculpatory the government viewed the document.").

Mr. Sadr, however, contends that the letter is exculpatory for a slew of reasons. *See* Dkt. No. 274 at 1–2; Dkt. No. 336 at 70–77. To take just a few of Mr. Sadr's explanations of the letter's clear exculpatory value, he argues that GX 411 shows that the affiliation between the recipient of the payment—Stratus International Contracting, a Turkish company—and Stratus Group, an Iranian conglomerate, was immaterial to OFAC. *See* Dkt. No. 274 at 1–2. Indeed, he points out that this affiliation was ultimately not enough for OFAC to stop U.S. dollar payments to Stratus International Contracting. *Id.* at 2. This point undermines several counts of the indictment, including at least the *Klein* conspiracy alleged in Count One and the bank fraud "right to control" charges alleged in Counts Three and Four. Each of these counts is predicated on the prospect of OFAC enforcement—and associated penalties levied on the intermediary banks—had OFAC known of Stratus International Contracting's Iranian connections. *See* *United States v. Ballistrea*, 101 F.3d 827, 831 (2d Cir. 1996) (holding that a *Klein* conspiracy requires a "purpose of *impairing, obstructing, or defeating the lawful function*" of OFAC (citation omitted)); *United States v. Finazzo*, 850 F.3d 94, 111 (2d Cir. 2017) (holding that "misrepresentations or non-disclosure of information cannot support a conviction under the 'right to control' theory [of bank fraud] unless those misrepresentations or non-disclosures can or do result in tangible economic harm" to the banks at issue). But as GX 411 and related disclosures demonstrate, when OFAC was apprised by Commerzbank of this very fact, it took *no* enforcement action.

***8** Mr. Sadr also contends that this letter undermines an argument that was central to the Government's trial theory: that Mr. Sadr structured the charged transactions to conceal connections to Iran. To the contrary, he claims that GX 411 demonstrates that the affiliation between Stratus International Contracting and Stratus Group was readily identifiable—so readily identifiable that it was discovered when the *first* charged payment was processed. *See* Dkt. No. 336 at 74. For these reasons, Mr. Sadr's attorneys stress that if GX 411 had been timely disclosed, their pre-trial investigation, theory of the case, opening and closing statements to the jury, evidentiary submissions, and cross examination of a Government witness all would have materially differed. Dkt. No. 336 at 74–75; Trial Tr. 999:8–18.

The Government has now come around to Mr. Sadr's position and concedes that GX 411 has exculpatory value. *See* Dkt. No. 275 at 2; Dkt. No. 354 at 8; Trial Tr. at 1005:5–6. In the Government's own words, GX 411 is exculpatory because it "advances the defendant's claim that any decision by OFAC not to take enforcement action following this disclosure is probative of the risk of harm from OFAC enforcement that banks face when they process transactions in violation of the sanctions law." Dkt. No. 275 at 2. The Government has thus "concede[d] that it erroneously failed to timely disclose the document at issue, and apologize[d] to the Court and counsel for its error." *Id.* at 1.

B. The Government Has Possessed GX 411 Since 2015

Even accepting the Government's contention that it did not appreciate the letter's exculpatory value does not change the fact that government actors knowingly possessed GX 411 for almost a decade. In January 2011, a slew of federal and state actors—Main Justice, the United States Attorney's Office for the Southern District of New York, OFAC, the Federal Reserve's Board of Governors, and the New York County District Attorney's Office—began investigating Commerzbank for violating U.S. sanctions. Dkt. No. 283 at 2; *see also* Dkt. No. 354 at 8. During these parallel investigations, Commerzbank's New York City branch provided the District Attorney's office various voluntary disclosures, one of which was GX 411. Dkt. No. 283 at 2–3. And about a year into these investigations, an Assistant District Attorney (ADA) was assigned to the District Attorney's investigation. (That ADA would later be appointed a Special Assistant United States Attorney in this case.) In March 2015, Commerzbank resolved these investigations by entering into a universal deferred prosecution agreement. *Id.* at 3; *see also* Dkt. No. 354 at 8.

Two months later, the ADA was assigned to work on the District Attorney's investigation of the "Venezuela housing matter, which ultimately led to this case." Dkt. No. 354 at 9. At around the same time, the ADA was "boxing up material from the Commerzbank investigation that had [recently] ended." *Id.* In doing so, he "came across some documents (including or consisting of [GX 411]) that he realized related to the [investigation of Mr. Sadr.]" *Id.*; *see also* Dkt. No. 283 at 3. At that time, the ADA "set those documents aside in a hard-copy manila folder." Dkt. No. 354 at 9. These documents then lay dormant for years, somewhere in the ADA's office.

In August 2015, "[the ADA] issued a state grand jury subpoena" to Commerzbank's New York branch in connection with the District Attorney's investigation of Mr. Sadr, and the branch duly responded to that request with many documents. Dkt. No. 354 at 9; Dkt. No. 283 at 3. The parties refer to this as the "Commerzbank Subpoena Production." Dkt. No. 283 at 3. The Government produced this entire Subpoena Production to Mr. Sadr during Rule 16 discovery in this case. *Id.*; *see also* Trial Tr. 988:14–25. But there's a catch: GX 411 was *not* part of the Commerzbank Subpoena Production in this matter, so it was not produced to the defense along with these documents. GX 411 had only been turned over to the Government in the earlier and unrelated investigation of Commerzbank, and the letter remained in that manila folder on the ADA's desk for years. By the time of the Commerzbank Subpoena Production in connection with this case, GX 411's contents were, according to the Government, "lost to [the ADA's] memory." Dkt. No. 354 at 9.

***9** Fast forward four years, to late 2019. By this point, the United States Attorney's Office had indicted Mr. Sadr, and attorneys on both sides were gearing up for trial. Around this time, the ADA, who was now an SAUSA, "rediscovered" the hard copy of GX 411 in his office. The Government has made two different representations about how this rediscovery came to pass. First, in its March 9 letter, the Government stated that on January 10, 2020, "AUSA[-1] sent an email to [the SAUSA] ... mention[ing] the April 4, 2011 wire transfer from Fondo Cino to Stratus International Contracting J.S. for $29 million, which is described in GX 411." Dkt. No. 283 at 4. AUSA-1 "stated a document previously provided by a witness—which was produced to the defense during Rule 16 discovery—'should be helpful in tying the wire information we have showing the Fondo Chino transfer to PDVSA.' " *Id.* Her email "triggered for [the SAUSA] a recollection of GX 411." *Id.* "That same day, [the SAUSA] located GX 411 in a hard copy file at his DANY office; [the SAUSA] had segregated [GX 411] from Commerzbank's other voluntary disclosures and stored it in the folder, but does not recall when he did so." *Id.* at 4–5. The SAUSA then emailed the prosecution team, attached GX 411, and said, "In the spirit of closing the loop on the $29M payment through Commerz, attached is the voluntary disclosure Commerze (sic) made to OFAC re: the payment." *Id.* at 5.

But in its July 2 letter, the Government puts forward a different story regarding this rediscovery. This one begins a month earlier: In December 2019, the SAUSA was "making a pre-trial sweep through his office for everything[, and] he rediscovered the separate folder of Commerzbank-Sadr documents." Dkt. No. 354 at 9. The target of the SAUSA's purported pre-trial sweep—"everything"—is vague and unclear. The SAUSA then referenced GX 411 in a December 19 email, three weeks before the January 10 email discussed above. In that December 19 email to the prosecution team, the SAUSA made the following comment, purportedly relating to GX 411: "Now I'm really going off on a tangent, but Commerzbank was an intermediary bank in the first USD payment (to Stratus Turkey) and they actually picked up on 'Stratus' in the payment message, drew the connection to the Iranian entity, and filed a report with OFAC." *Id.* Yet the SAUSA did not attach GX 411 to the December 19 email. He only shared the document with the team three weeks later, in his January 10 email discussed above. In short, the Government has presented two different versions of events. In one, an email from a colleague "triggered" the SAUSA's memory of GX 411 in January 2020. In the other, the SAUSA was conducting a "pre-trial sweep" of his office, stumbled upon GX 411 in December 2019, and referenced GX 411 in an email that same month.

Whichever is true, here's the nub: On January 10, 2020, every prosecutor active in the case received an email with GX 411. But even on that late date—months after *Brady* and Rule 16 disclosures had been made and two months before trial—no attorney disclosed GX 411 to the defense. The Government proffers that the prosecution team made a "reasonable assumption ... that all Commerzbank documents had previously been disclosed" through the Commerzbank Subpoena Production. *Id.* at 10. Of course, recall that GX 411 was not part of that Subpoena Production, but instead came from the earlier, non-Sadr-related investigation of Commerzbank. The Court agrees that this is a plausible explanation for why at least some of the prosecutors thought that GX 411 had already been disclosed and thus took no further action in January. From their perspective, nothing in GX 411 distinguished it from the many other documents from Commerzbank that the Government had duly disclosed. Still, it is harder to accept how the SAUSA, who was fully aware of (and indeed had worked on) the separate, non-Sadr related investigation of Commerzbank and who had himself possessed GX 411 as a result of that investigation since 2015, could have assumed throughout that GX 411 had been produced to the defense. And to be clear, he was appointed as an SAUSA in this matter effective June 2017. *Id.* at 2 n.2. As the Government recognizes, "when an attorney from another agency is appointed a SAUSA to assist this Office in a criminal case, it is this Office, and our AUSAs, who are ultimately responsible for disclosures in the case, and knowledge of any matter in the investigation that may be overlooked by a SAUSA is imputed to the Government, whether or not the AUSAs on a case have actual knowledge of the matter." *Id.* The Government had therefore possessed GX 411 since the day Mr. Sadr was indicted—yet did not disclose the document for *more than two years*, in the midst of trial. Once again, the Government's explanation that it thought the document had been produced to the defense as part of the Commerzbank subpoena production is plausible, but the Court has lingering doubts based on matters discussed below.

C. Government Prosecutors Discuss "Burying" GX 411

***10** Now jump forward another two months, to March 6, 2020. By this point, trial has begun. Around 8 P.M. on that Friday evening, after trial had concluded for the day, AUSA-1 was, according to the Government, "organizing her emails" and stumbled upon the SAUSA's January 10 email attaching what would later be marked as GX 411. Dkt. No. 283 at 5; Dkt. No. 354 at 10. In an email to her colleagues, she wrote, "Given what defense did today, I think [the exhibit that would later be marked as GX 411] could be really valuable to put in. Among other difficulties with doing that is the fact that I don't know that it was ever produced to defense (it's not in the Commerzbank subpoena production). [SAUSA] – do you know where it came from?" Dkt. No. 354 at 10.

But AUSA-1 was unable to get in touch with the SAUSA, so she instead spoke with AUSA-2, another prosecutor on the case. In a chat message, AUSA-1 wrote, "[I] feel like it might be too late to do anything about it, but [I] can't believe we all missed that [C]ommerzbank document," adding "[I] have no idea where that letter came from[;] [I] don't think it has ever been produced to the defense." *Id.* AUSA-2 replied, "[O]h, that letter[;] we can produce it tonight[;] produce it right now and the defense can have 3 days to review[;] that's more than enough time for one document[;] mark and produce it stat—[I] think we should at least try." *Id.* Astonishingly,

AUSA-1 responded, "[I]'m wondering if we should wait until tomorrow and bury it in some other documents." *Id.* (emphasis added). In response to AUSA-1's proposal to "bury" GX 411, AUSA-2 agreed and took the plan further by proposing documents along which GX-411 could be buried when disclosing it to the defense. *Id.* at 11. Specifically, she replied, "that's fine too—some of the [Financial Action Task Force] stuff," referring to another exhibit. *Id.* Later in that chat, AUSA-1 noted that the Government "need[ed] to come up with some explanation for why the defense is just seeing this for the first time ...." *Id.* at 11. According to their own internal communications, therefore, on the evening of March 6, the prosecutors in this case again came across GX 411, recognized somehow for the first time that it had never been disclosed to the defense, recognized that its lack of disclosure would likely draw objection, strategized how to "bury" the document, settled on a plan to do so, and discussed waiting an additional day before turning it over to aid in burying the document among others.

Even the next day, disclosure was not immediately forthcoming. Instead, on the morning of Saturday, March 7, the Government admits that several members of the prosecution team discussed GX 411 and debated how and even whether the exhibit should be disclosed. *Id.* at 11. At this time—in the midst of trial—the Government represents that "there was never any notion [among the AUSAs] that GX 411 might be of exculpatory value to the defense." *Id.* On that morning, "AUSAs discussed ... [w]hether the exhibit was worth offering." *Id.* According to the Government's own theory, if prosecutors believed that the document was wholly inculpatory and decided not to offer it at trial, they likely would have never turned it over to the defense. Indeed, AUSA-1 "did not want to get into a fight with defense counsel over the document," and she "recalls a discussion" amongst the prosecutors that its lack of disclosure may not violate Federal Rule of Criminal Procedure 16. *Id.* There were thus some members of the prosecution team who, even after recognizing that the document had not been disclosed, argued that the Government should not turn it over.

D. The Government Discloses GX 411

At around 4 P.M. on Saturday, March 7, the Government disclosed GX 411. It did so in an email sent from AUSA-1 to the defense team. Dkt. No. 354 at 12–13. The specifics of this transmittal email are critical, so the Court attaches it to this Opinion. *See* Exhibit A. The email began by noting that a potential Government witness remained ill and so he would not testify in the Government's case-in-chief. *Id.* AUSA-1 then wrote "we've attached the following documents" and provided a bulleted list of about fifteen documents, at least two of which were marked for the first time as new Government exhibits. *Id.* All but one of these documents, GX 411, had already been disclosed through discovery; in other words, GX 411 was the *only* document on the list that had not already been provided to the defense. Trial Tr. at 993:5–16 (noting that GX 411 "was the only document" on this list that had not previously been disclosed to the defense); *see also* Dkt. No. 354 at 13 (noting that the other documents were "mostly duplicates of 3500 material or revisions of exhibits"). The *third* bullet, which was virtually identical to the next bullet listing a previously disclosed document, stated as follows: "GX 411 – we intend to offer this Monday. Let us know if you will stipulate to authenticity." Ex. A.

***11** Nothing in this email identified GX 411 as a newly disclosed document, a fact that we now know the Government lawyers were aware of and discussed with each other prior to transmittal. To the contrary, the bulleted list deliberately obscured the fact that GX 411 was different in kind than the other exhibits listed, as it was the only exhibit on that list that had not been previously turned over to the defense. Indeed, as noted, the Government's wording with respect to GX 411 was the same as its wording regarding another exhibit, GX 456, that had already been disclosed. *See id.* (stating as to both exhibits, "we intend to offer this on Monday. Let us know if you will stipulate to authenticity."). Nothing in this email indicated how long the Government had possessed the document. And nothing indicated why the document was disclosed one week into trial. Indeed, the Government now concedes that "[t]his email does not, as we believe it should have, identify GX 411 as a new document that was not previously disclosed." Dkt. No. 354 at 13 (emphasis in original); *see also* Dkt. No. 283 at 1 (Government admitting that it "fail[ed] to make accurate disclosures regarding the status of [GX 411] on March 7 and March 8, 2020."). All four prosecutors who represented the Government at trial have admitted that the "[t]he transmittal email failed to disclose that GX 411 had not been produced previously" and that "there is *no dispute* that [this] was a failure in judgment on [their] part." Dkt. No. 283 at 5 (emphasis added).

Surprisingly, the Government represents that this "failure in judgment" was no accident—it was the product of reasoned discussion among the prosecution team. In addition to the contemporaneous communications among the AUSAs discussed above, the Government states that the prosecutors discussed how to disclose GX 411 before sending this email. AUSA-1 and AUSA-3, both "confident that the defense would know it was a new document given their knowledge of the case," suggested "that the Government should simply produce it and wait for the defense's questions, and if the Government did not make a big deal about the document, the defense might decide that it was not important enough to object." Dkt. No. 354 at 12. In other words, according to their own after-the-fact account, the Government lawyers knew that GX 411 had not previously been disclosed, but nonetheless thought it best to call no attention to the document and hoped that the defense would stipulate to its authenticity with little fanfare. That did not come to pass.

Even if the story stopped there, things would be bad enough. No responsible Government lawyer should strategize how to "bury" a document that was not, but should have been, previously disclosed to the defense. A responsible Government lawyer should—at a minimum—forthrightly and truthfully reveal late disclosures to the defense. The leadership of the USAO attempts to justify this conduct by arguing that what the prosecutors did was not, in fact, "burying" a now-admittedly exculpatory document, and instead conveys to its prosecutors and the Court that the conduct of the Government lawyers described above is not condemnable. Dkt. No. 354 at 11 ("[T]he document, which was in fact produced less than 24 hours later, was not buried.... [W]e believe it would go too far to condemn [AUSA-1] for a Friday night lapse in thinking regarding a document that was in fact disclosed Saturday afternoon."). This Court disagrees and hereby strongly condemns this conduct.

E. The Government Makes a Misrepresentation to the Court

Unfortunately, that is not the end of the story. The day after this disclosure, Mr. Sadr wrote to the Court, represented that the Government had produced GX 411 for the first time, argued that GX 411 was *Brady* material, and sought a curative instruction. *See* Dkt. No. 274. In simpler terms, Mr. Sadr argued that the Government had breached its constitutional duties in failing to turn over this document, and asked the Court to explain that failure to the jury. The Court quickly ordered the Government to make a "detailed representation" explaining why this document was not disclosed, what led to its March 7 disclosure, and which attorneys were involved in this process. Dkt. Nos. 286, 287. The Government provided a narrative that is now familiar: the prosecution team incorrectly believed that GX 411 had been disclosed to Mr. Sadr with the Commerzbank Subpoena Returns, and only realized it had not on March 6. Dkt. No. 275.

***12** The vagueness of the Government's explanation immediately raised flags for the Court. That same day, the Court issued an order stating that the Government had failed in its letter to "indicate if, upon learning of the late disclosure [of GX 411], the Government informed defense counsel or not." Dkt. No. 290. The Court thus ordered "the Government [to] explain precisely when and how it realized that the document had been erroneously withheld," and—importantly for present purposes—"when, if at all, ... the failure to disclose ... was communicated to the defense." *Id.* This Order is also attached to this Opinion. *See* Exhibit B.

The Government's next letter is central to the lingering ethical questions in this case, and the Court likewise attaches it to this Opinion. *See* Exhibit C. In that letter, the Government recounted how its lawyers had "found" GX 411 on Friday evening and discussed the document the next day. *Id.* at 1. The Government then stated that it "promptly had a paralegal mark it as an exhibit and produced it to the defense along with other exhibits and 3500 materials." *Id.* The Court does not dwell on the Government's representation of promptness, though it does note that the Government disclosed GX 411 about twenty hours after it realized it had never been turned over, consistent with the discussion between the AUSAs about waiting a day in order to "bury" it with other documents. The Government next represented that it "*made clear [in its email] that GX 411 was a newly marked exhibit* and that we intended to offer it, and asked the defense if they would stipulate to authenticity." *Id.* (emphasis added).

To reiterate, the Court asked the Government a direct question: When and how did it inform the defense of the failure to timely *disclose* GX 411? *See* Ex. B. But the Government did not respond to that direct question with a direct answer. Rather, it answered that it had made clear

in its March 7 email to defense counsel that GX 411 was newly *marked.* Ex. C. The Court finds that the Government's representation was misleading, as it implied that it had explicitly informed the defense that GX 411 was being disclosed for the first time. Indeed, the Court was misled. Upon receipt of that letter, the Court took great comfort in believing that, despite the disclosure failure, at the very least the Government had clearly indicated that GX 411 had not been previously disclosed. But that was not the truth. To the contrary, the Government placed GX 411 in the middle of a bulleted list of several other documents, *all of which* had already been disclosed, and at least one other of which was newly marked. *See* Ex. A. The Government did not say that the exhibit was not previously disclosed. The Government did not indicate that GX 411 was different in any way from the other, already-disclosed attachments. Nor did the Government's request for a stipulation of authenticity make clear that this exhibit was newly disclosed—the Government made the same request as to another document on the list that had already been disclosed. *See id.* (GX 456). The Government admits that "[t]he transmittal email failed to disclose that GX 411 had not been produced previously." Dkt. No. 283 at 5.

What arguably occurred here is that at least some of the Government lawyers implemented and executed the strategy the prosecutors had discussed: to "bury" GX 411 by deceptively hiding it among several other documents that had previously been disclosed. Having gotten caught in this effort, the Government then made a misleading representation to the Court, perhaps in an attempt to make its conduct appear better than it was. To make matters worse, as recounted in more detail below, the Court has now learned that certain Government lawyers edited the sentence in question from an accurate recounting of the facts—the letter's first draft rightly stated that the "Government did not specifically identify that GX 411 had not previously been produced in discovery," *see* Dkt. No. 354 at 14—to its final, misleading form.

F. Further Fact-Finding Is Necessary

***13** Several critical questions remain regarding the untimely disclosure of GX 411 and the Government's subsequent misleading representation to the Court. The Court is obligated to determine what has occurred.

First, there are discrepancies presented to the Court about who knew what when regarding the provenance of GX 411. To start, as the Court has discussed, the SAUSA has presented two different stories about how and when he "rediscovered" GX 411. Moreover, the SAUSA recalls discussing GX 411 "with AUSAs in January 2020," and further represents that "at or about [this] time, he had a telephone conversation with [AUSA-1] about 'how and from where' [GX 411] had been obtained." Dkt. No. 354 at 10 n.6. If this is true, it means that at least two prosecutors knew in January 2020 that GX 411 had not been disclosed as part of the Commerzbank Subpoena Production, yet they took no steps to produce the document to the defense or correct representations to the contrary made to the Court by other Government lawyers. *See, e.g.*, Dkt. No. 277 at 1–2; Trial Tr. at 982:13–17; *id.* at 984:11–19; Dkt. No. 283 at 5. For their part, the AUSAs deny this account and say they did not discuss GX 411 with the SAUSA in January 2020, and learned only in the middle of trial that the exhibit had not been disclosed. Dkt. No. 354 at 10 n.6. At this stage, the Court cannot determine which version is true.

Second, and relatedly, the Court cannot yet firmly conclude based on the existing factual record whether any of the Government lawyers deliberately withheld exculpatory information. The Government maintains that no prosecutor "had any inkling ... that GX 411 would have exculpatory value for the defense" until defense counsel's emails on March 7. Dkt. No. 354 at 13. The Government further represents that "[h]ad any of the attorneys on the case recognized the exculpatory theory the defense has articulated, that would, we believe, have trigged further analysis, but they did not." *Id.* at 10. And during trial, the Government attributed its misunderstanding to "trial blinders." Trial Tr. at 991:10–992:19.

Certainly, the now-disclosed written, internal communications of the AUSAs—which discuss the usefulness of GX 411 to only the Government's case, and do not speak to its exculpatory value—support the Government's contention that none of the prosecutors recognized the document's now-conceded exculpatory value. The contention that trial blinders prevented the prosecutors from perceiving the exculpatory value of GX 411 is plausible. But there are other facts in the current record that cast some doubt on this representation of ignorance. To start, by the time the AUSAs were discussing "burying" the document, even if not earlier, the relevance of GX 411 to the defense arguably should

have been apparent. Indeed, for reasons already discussed above, GX 411 and subsequent responses to it by OFAC and the intermediary bank tend to demonstrate that Stratus International Contracting's affiliation with Stratus Group was not material to either OFAC or the intermediary banks, a point critical to the Government's ability to establish the elements of several charged counts. *See* Section III.A. Moreover, emails from the SAUSA in late January and early February further call the Government's contention into doubt. The SAUSA at that time notified the trial team that Commerzbank "filed a voluntary disclosure with OFAC regarding the payment [GX 411]," described this disclosure as an "asterisk," and suggested that the team "discuss whether it's worth having the Commerz witness go into that." Dkt. No. 341 at 8. And in a subsequent email, the SAUSA stated "we [the prosecution team] can discuss how we would want to handle" the Commerzbank disclosure. *Id.* Although there are alternative explanations available, these emails at least arguably suggest, as Mr. Sadr argues, that the prosecutors recognized that GX 411 was not wholly helpful to the Government and considered not calling a Commerzbank witness because doing so could lead to disclosure of this document—cutting against the Government's narrative that its prosecutors thought GX 411 was inculpatory. *See* Dkt. No. 355 at 3.

***14** *Third*, there are discrepancies about which prosecutor(s) were involved in making the misrepresentation in the Government's March 8 letter. These discrepancies prevent the Court from resolving, at this time, whether the misrepresentation was intentional. The Government drafted the letter in question in about one hour. *See* Dkt. No. 354 at 14–15. To her credit, in the letter's first draft, written by AUSA-1, the sentence in question stated, "The Government did not specifically identify that GX 411 had not previously been produced in discovery." *Id.* at 14. This sentence was directly responsive to the question the Court had asked and was accurate—had it been included in the final letter, this inquiry may have been avoided. But because AUSA-1 "was ill [and] had to leave the Office shortly after" circulating this first draft, *id.* at 14, the drafting of the letter was passed onto other prosecutors, and AUSA-3 took the lead. In the ten minutes before the Court's deadline, AUSA-3 sent AUSA-1's draft to the Co-Chiefs of the Terrorism & International Narcotics Division of the USAO and then spoke with them on the phone. *Id.* at 14–15. At some point in this process, this truthful sentence was edited to make the misrepresentation in question, becoming "The Government made clear that GX 411 was a newly marked exhibit ...." *Id.* at 15. AUSA-3 then filed the letter. *Id.* One minute after the Court's deadline, AUSA-3 emailed AUSA-2 saying, "They [the Chiefs] called me with some changes. I made them and filed." *Id.*

When pressed to disclose the prosecutor(s) responsible for this edit, the Government lawyers point fingers. The Unit Chiefs "advise[ ] that they did not request ... deletion of the [original language], although they may have missed that deletion ... if the final draft was read to them over the phone." Dkt. No. 356 at 2 n.1. Significantly, this runs contrary to one of the Unit Chief's explanation at trial on the day after the letter was drafted, when he informed the Court that "[The other Unit Chief] and I reviewed [this] letter in realtime before it was filed—our understanding in submitting [the misrepresentation] to your Honor was that this clearly marked language ... related to the fact that the document had been marked as a government exhibit with a yellow government sticker. That is what we intended to convey with that." Trial Tr. at 997:14–20. In other words, nearly contemporaneously with the letter's drafting, the Unit Chiefs represented that they were aware of this language and that it was purposely included in the Government's letter—but in post-trial briefing, the Chiefs claim that they did not request this change and may have missed it entirely. For his part, AUSA-3 "recalls opening [AUSA-1's] draft during the call and making changes that he understood to reflect the input from the unit chiefs." Dkt. No. 354 at 15. AUSA-3 thus "filed a letter that he believed reflected the considered judgment of his supervisors." *Id.* And the other prosecutors' involvement is unclear; AUSA-1 had left the office due to illness by the time of these edits, and the Government says nothing about the SAUSA's and AUSA-2's roles. *Id.* Despite the extensive letter briefing about this issue, therefore, the Court still does not know which prosecutor(s) were responsible for making this misrepresentation. Indeed, the Court notes that these drafting changes were first revealed only with the filing of the Government's July 2 letter, months after trial had ended and months after the Court inquired on the record about this precise misrepresentation. *See* Trial Tr. 989:16–995:16, 996:18–998:18. Fully understanding this drafting process is necessary to determine whether any of the prosecutors intentionally misled the Court.

* * * * *

[3] Even though the Court has now granted Mr. Sadr's motion for a new trial, vacated the verdict against him, and dismissed

the indictment with prejudice, the Court retains authority to sanction the prosecutors in this case. *See* *United States v. Seltzer*, 227 F.3d 36, 41–42 (2d Cir. 2000) (discussing district courts' inherent power to impose sanctions). The Government agrees that the Court retains this supervisory power. Dkt. No. 352 at 2.

It is the fervent hope of the Court that no sanctions are necessary. But it is the firm view of the Court that if Government lawyers acted in bad faith by knowingly withholding exculpatory material from the defense or intentionally made a misleading statement to the Court, then some sanction or referral to the Grievance Committee of the Southern District of New York would be appropriate. The record before the Court neither conclusively establishes intentionality nor resolves the issue.

***15** Given the lack of clarity surrounding the disclosure of GX 411 and the subsequent misrepresentation to the Court, the Court requires further information. The Court therefore orders each AUSA on the trial team, the two Unit Chiefs, and the SAUSA to submit individual declarations, under penalty of perjury, regarding these issues. These declarations should, at a minimum, respond to the following questions with specificity:

1. When did you first learn of GX 411?

2. When did you first realize that GX 411 had not been disclosed to the defense? Why did you not immediately disclose the document at that time?

3. What specific communications did you have regarding GX 411 or the disclosure of GX 411 with other prosecutors, whether oral, written, or electronic in any form? When did these communications occur? Attach any record you have of any such communication.

4. When did you first recognize GX 411 as having exculpatory value? If you thought the document was wholly inculpatory, provide a good-faith basis for that understanding.

5. With specificity, what role did you play in drafting the Government's March 8, 2020 letter? *See* Ex. C. What role did you play in deleting the accurate sentence responsive to the Court's question that was originally drafted by AUSA-1? *See* Dkt. No. 354 at 14 ("The Government did not specifically identify that GX 411 had not previously been produced in discovery."). What role did you play in drafting the sentence that the Court has concluded was a misrepresentation? *See* Dkt. No. 277 at 1 ("The Government made clear that GX 411 was a newly marked exhibit ...."). Why was this sentence changed? Attach any communications related to this change.

6. When the Court asked specific questions at trial on March 9, 2020 regarding the Government's misrepresentation, were you aware that the accurate sentence responsive to the Court's question had been edited or deleted? If so, explain why this was not conveyed to the Court.

The declarations shall further provide any and all other information the prosecutor believes relevant to the unresolved issues identified in this Opinion. Following these declarations, the executive leadership for the USAO may submit letter briefing as to why no further proceeding for additional fact-finding or credibility determinations is necessary. Counsel for Mr. Sadr may file a responsive letter brief, and the Government may file a reply.

After the Court reviews these submissions, it will determine whether a hearing to conduct further fact-finding, including credibility determinations, is necessary.

IV. CONCLUSION

[4] Almost a century ago, the Supreme Court defined the singular role federal prosecutors play in our system of justice:

> The United States Attorney is the representative not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done .... He may prosecute with earnestness and vigor—indeed, he should do so. But, while he may strike hard blows, he is not at liberty to strike foul ones.

> It is as much his duty to refrain from improper methods calculated to produce a wrongful conviction as it is to use every legitimate means to bring about a just one.

Berger v. United States, 295 U.S. 78, 88, 55 S.Ct. 629, 79 L.Ed. 1314 (1935).

[5] The Government in this case has failed to live up to these ideals. The Court has recounted these breaches of trust, proposed some systemic solutions, urged referral to the Office of Professional Responsibility for admitted prosecutorial failures apparent in the existing record, and ordered further fact-finding. The cost of such Government misconduct is high. With each misstep, the public faith in the criminal-justice system further erodes. With each document wrongfully withheld, an innocent person faces the chance of wrongful conviction. And with each unforced Government error, the likelihood grows that a reviewing court will be forced to reverse a conviction or even dismiss an indictment, resulting in wasted resources, delayed justice, and individuals guilty of crimes potentially going unpunished.

***16** The Court thus issues this Opinion with hopes that in future prosecutions, the United States Attorney for the Southern District of New York will use only "legitimate means to bring about a just" result. *Id.* Nothing less is expected of the revered Office of the United States Attorney for the Southern District of New York. That Office has a well- and hard-earned reputation for outstanding lawyers, fierce independence, and the highest of ethical standards. The daily work of the prosecutors in that Office is critically important to the safety of our community and the rule of law. Those who stand up in court every day on behalf of that Office get the benefit of that reputation—but they also have the responsibility to maintain it.

The Court hereby ORDERS that the Acting United States Attorney ensure that all current AUSAs and SAUSAs read this Opinion. Within one week of the date of this Opinion, the Acting United States Attorney shall file a declaration affirming that this has occurred.

The Court FURTHER ORDERS that each of the trial team AUSAs, supervising Unit Chiefs, and the SAUSA submit the declarations described in Section III no later than October 16, 2020. By October 30, 2020, the executive leadership for the USAO may submit a brief as to why no further proceeding for additional fact-finding or credibility determinations is necessary. Counsel for Mr. Sadr may, if they wish, submit a responsive filing by November 13, 2020, and the Government a reply by November 20, 2020.

SO ORDERED.

Exhibit A

From: [Redacted]

Sent: Saturday, March 07, 2020 4:04 PM

To: [Redacted]

Cc: [Redacted]

Subject: U.S. v. Sadr

Counsel,

Mr. Dubowitz is still very ill. As a result, we do not intend to call him as a witness in our case-in-chief. It's possible that, depending on the defense case, we will call him as a rebuttal witness.

In addition, we've attached the following documents:

- Updated GX 2284D – there were formatting problems with our version. We think the attached corrects them.

- 3508-08 – 3500 from today

- GX 411 – we intend to offer this on Monday. Let us know if you will stipulate to authenticity.

- GX 456 – we intend to offer this on Monday. Let us know if you will stipulate to authenticity.

- GX 495A & B – we intend to offer these on Monday (likely in redacted form), although think a stipulation that the defendant had bank accounts at HSBC from January 2010 through October 2013 might be simpler. Let us know how you prefer to proceed.

- GX 704 – this is the modified version of the travel chart. Please confirm whether you have any remaining concerns.

- GX 705A & B – these are summary charts reflecting the information in GX 2090A. Please confirm whether you have any objections.

- Updated GX 2304A – we enlarged some of the cells, as the formatting of the PDFd excel file was cutting off some of the data. The content is the same.

- 3504-10 – Peri 3500, which was provided in hard copy yesterday morning.

- 3505-06 – Blair 3500, which was provided in hard copy yesterday morning.

- 3513-02 – Paralegal 3500 for summary chart (you may already have this)

- 3513-03 – Paralegal 3500 for summary chart (you may already have this)

We are still working on one additional summary chart, which we expect to provide later today.

[Redacted]
Assistant United States Attorney

Southern District of New York

One Saint Andrew's Plaza

New York, NY 10007

Tel: [Redacted]

Exhibit B

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF NEW YORK

United States of America,

–v–

Ali Sadr Hashemi Nejad, Defendants.

18-cr-224 (AJN)

ORDER

ALISON J. NATHAN, District Judge:
In the letter filed this evening by the Government, Dkt. No. 275, the Government states that "It was only in the context of this process that the Government realized that GX 411 was not part of Bank-1's subpoena production, which had been provided to the defense in discovery."

The Court requires further explanation. Specifically, it is unclear from this sentence if the Government realized GX 411 had not been previously disclosed before or after the Government turned it over to the defense yesterday. Nor does this sentence indicate if, upon learning of the late disclosure, the Government informed defense counsel or not. The Government shall explain precisely when and how it realized that the document had erroneously been withheld and when, if at all, upon learning of the failure to disclose this was communicated to the defense.

***17** Furthermore, the previously filed letter does not offer an explanation for how it came to be that GX 411 was not (though should have been) provided to the defense as part of Bank-1's subpoena production.

The Government is ordered to address these points by letter to be filed no later than 10 p.m. this evening. The defense may reply to the Government's letters by 11 p.m.

SO ORDERED.

Dated: March 8, 2020

New York, New York

/s/ ALISON J. NATHAN
ALISON J. NATHAN

United States District Judge

Exhibit C

March 8, 2020

FILED BY ECF

The Honorable Alison J. Nathan
United States District Judge
Southern District of New York
United States Courthouse
40 Foley Square, Courtroom 1306
New York, New York 10007
Re: *United States v. Ali Sadr Hashemi Nejad*, 18 Cr. 224 (AJN)

Dear Judge Nathan:
The Court writes in response to the Court's order from 9:00 this evening. The Government apologizes for the lack of clarity in its prior email.

The Government found GX 411 in its emails on Friday night, looked at the Bank-1 subpoena production, and did not find it. The members of the team discussed the document the next morning and confirmed that it likely had not been produced to the defense previously. The Government promptly had a paralegal mark it as an exhibit and produced it to the defense along with other exhibits and 3500 materials. The Government made clear that GX 411 was a newly marked exhibit and that we intended to offer it, and asked the defense if they would stipulate to authenticity. Defense counsel responded shortly after the Government provided GX 411 and asked how long the Government had GX 411, and why they had not previously received it. The Government responded and explained that we had been aware of the letter since mid-January, and that, at the time, the Government had mistakenly believed it was part of the discovery in the case.

When SAUSA [Redacted] sent what is now GX 411 to the AUSAs in the case in January, the AUSAs assumed that this was a document that came from this case (specifically, the subpoena to Bank-1), and that it was therefore a document that had been previously produced to the defense as part of the Rule 16 discovery. This was an incorrect assumption. The document in fact was obtained in an unrelated DANY investigation and was not provided to this Office before January 2020.

Respectfully submitted,

GEOFFREY S. BERMAN

United States Attorney

By: /s/ [Redacted]
Assistant United States Attorneys

[Redacted]
Special Assistant United States Attorney

(212) 637-2038 / 2279 / 1066

cc: Defense Counsel (by ECF)

All Citations

--- F.Supp.3d ----, 2020 WL 5549931

United States v. Ulbricht

United States Court of Appeals for the Second Circuit

October 6, 2016, Argued; May 31, 2017, Decided

Docket No. 15-1815

Reporter
858 F.3d 71 *; 2017 U.S. App. LEXIS 9517 **; 103 Fed. R. Evid. Serv. (Callaghan) 679; 66 Comm. Reg. (P & F) 1304; 2017 WL 2346566

UNITED STATES OF AMERICA, Appellee, — v. — ROSS WILLIAM ULBRICHT, a/k/a DREAD PIRATE ROBERTS, a/k/a SILK ROAD, a/k/a SEALED DEFENDANT 1, a/k/a DPR, Defendant-Appellant.

Subsequent History: US Supreme Court certiorari denied by *Ulbricht v. United States, 2018 U.S. LEXIS 4043 (U.S., June 28, 2018)*

Prior History: Ross William Ulbricht appeals from a judgment of conviction and sentence to life imprisonment entered in the United States District Court for the Southern District of New York (Katherine B. Forrest, J.), for drug trafficking and other crimes associated with his creation and operation of an online marketplace known as Silk Road. He argues that (1) the district court erred in denying his motion to suppress evidence obtained in violation of the *Fourth Amendment* **[**1]** ; (2) the district court committed several errors that deprived him of his right to a fair trial, and incorrectly denied his motion for a new trial; and (3) his life sentence is both procedurally and substantively unreasonable. For the reasons set forth below, the judgment of the district court is AFFIRMED in all respects.

United States v. Ulbricht, 2014 U.S. Dist. LEXIS 145553 (S.D.N.Y., Oct. 10, 2014)

Core Terms

district court, sentence, site, laptop, chat, marks, quotation, drugs, disclosure, Pirate, corruption, murders, users, communications, cross-examination, searched, orders, records, trap, Internet, connected, username, electronic, contends, warrants, life sentence, vendor, particularized, investigations, reasons

Case Summary

Overview

HOLDINGS: [1]-The issuance of the pen/trap orders under *18 U.S.C.S. § 3122(a)(1)* that the government used to monitor IP address traffic to and from defendant's home router did not violate the *Fourth Amendment* because defendant had no reasonable expectation of privacy in the IP address routing information that the orders allowed the government to collect; [2]-The warrants authorizing the government to search defendant's laptop as well as his electronic media accounts did not violate the *Fourth Amendment's* particularity requirement because the warrants listed the charged crimes, described the places to be searched, and designated the information to be seized in connection with the specified offenses; [3]-Defendant had not shown that the district court abused its discretion in maintaining secrecy of grand jury investigation.

Outcome

Judgment affirmed.

LexisNexis® Headnotes

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Conclusions of Law

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Findings of Fact

Criminal Law & Procedure > ... > Standards of Review > Clearly Erroneous Review > Motions to Suppress

Criminal Law & Procedure > ... > Standards of Review > De Novo Review > Motions to Suppress

HN1 **De Novo Review, Conclusions of Law**

On appeal from a denial of a suppression motion, the appellate court reviews a district court's findings of fact for clear error, and its resolution of questions of law and mixed questions of law and fact de novo.

Criminal Law & Procedure > Search & Seizure > Eavesdropping, Electronic Surveillance & Wiretapping > Pen Registers & Trap & Trace Devices

HN2 **Eavesdropping, Electronic Surveillance & Wiretapping, Pen Registers & Trap & Trace Devices**

The Pen/Trap Act provides that a government attorney may make an application for an order authorizing or approving the installation and use of a pen register or a trap and trace device to a court of competent jurisdiction. 18 U.S.C.S. § 3122(a)(1). A pen register is defined as a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, and shall not include the contents of any communication. § 3127(3). A trap and trace device means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication. § 3127(4). Like pen registers, trap and trace devices may not capture the contents of any communication. Id. The statute does not require a search warrant for the use of a pen register or trap and trace device, nor does it demand the kind of showing required to obtain such a warrant. Rather, the statute requires only that the application contain a certification that the information likely to be obtained is relevant to an ongoing criminal investigation. § 3122(b)(2).

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

HN3 **Search & Seizure, Scope of Protection**

The Fourth Amendment to the United States Constitution provides that: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. The cornerstone of the modern law of searches is the principle that, to mount a successful Fourth Amendment challenge, a defendant must demonstrate that he personally has an expectation of privacy in the place searched. Thus, a Fourth Amendment search' does not occur unless the search invades an object or area in which one has a subjective expectation of privacy that society is prepared to accept as objectively reasonable.

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

Criminal Law & Procedure > Search & Seizure > Eavesdropping, Electronic Surveillance & Wiretapping > Pen Registers & Trap & Trace Devices

HN4 **Search & Seizure, Expectation of Privacy**

A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties, including phone numbers dialed in making a telephone call and captured by a pen register. This is so because phone users typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact

record this information for a variety of legitimate business purposes. Similarly, e-mail and Internet users rely on third-party equipment in order to engage in communication. Internet users thus should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information. Moreover, IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.

Governments > Courts > Judicial Precedent

HN5 **Courts, Judicial Precedent**

Appellate courts remain bound by a rule until and unless it is overruled by the United States Supreme Court.

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

Criminal Law & Procedure > Search & Seizure > Eavesdropping, Electronic Surveillance & Wiretapping > Pen Registers & Trap & Trace Devices

HN6 **Search & Seizure, Expectation of Privacy**

Collecting IP address information devoid of content is constitutionally indistinguishable from the use of a pen register.

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

HN7 **Search & Seizure, Expectation of Privacy**

A defendant cannot claim a reasonable expectation of privacy in the government's acquisition of his subscriber information, including his IP address and name, because it had been revealed to a third party.

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

HN8 **Search & Seizure, Expectation of Privacy**

There is no expectation of privacy in subscriber information provided to an internet provider, such as an IP address.

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

HN9 **Search & Seizure, Expectation of Privacy**

Computer users do not have a legitimate expectation of privacy in their bulletin board subscriber information because they have conveyed it to another person.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

HN10 **Search & Seizure, Scope of Protection**

Third-party information relating to the sending and routing of electronic communications does not receive *Fourth Amendment* protection.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Scope of Protection

Criminal Law & Procedure > Search & Seizure > Expectation of Privacy

HN11 **Search & Seizure, Scope of Protection**

Courts have not extended *Fourth Amendment* protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like IP addresses.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

Criminal Law & Procedure > Search & Seizure > Search Warrants > Probable Cause

HN12[] **Search & Seizure, Warrants**

The *Fourth Amendment* explicitly commands that warrants must be based on probable cause and must particularly describe the place to be searched, and the persons or things to be seized. *U.S. Const. amend. IV*. It is familiar history that indiscriminate searches and seizures conducted under the authority of general warrants' were the immediate evils that motivated the framing and adoption of the *Fourth Amendment*. Those general warrants specified only an offense, leaving to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched. The principal defect in such a warrant was that it permitted a general, exploratory rummaging in a person's belongings, a problem that the *Fourth Amendment* attempted to resolve by requiring the warrant to set out with particularity the scope of the authorized search.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN13[] **Search & Seizure, Warrants**

In addition to preventing general searches, the particularity requirement serves two other purposes not relevant to this appeal: preventing the seizure of objects upon the mistaken assumption that they fall within the magistrate's authorization, and preventing the issuance of warrants without a substantial factual basis.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN14[] **Search & Seizure, Warrants**

To be sufficiently particular under the *Fourth Amendment*, a warrant must satisfy three requirements. First, a warrant must identify the specific offense for which the police have established probable cause. Second, a warrant must describe the place to be searched. Finally, the warrant must specify the items to be seized by their relation to designated crimes.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN15[] **Search & Seizure, Warrants**

Where the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. A general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be akin to a residence in terms of the scope and quantity of private information they may contain. The seizure of a computer hard drive, and its subsequent retention by the government, can therefore give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure. Such sensitive records might include tax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, and banking and shopping information. Because of the nature of digital storage, it is not always feasible to extract and segregate responsive data from non-responsive data, creating a serious risk that every warrant for electronic information will become, in effect, a general warrant, Thus, warrants that fail to link the evidence sought to the criminal activity supported by probable cause do not satisfy the particularity requirement because they lack meaningful parameters on an otherwise limitless search of a defendant's electronic media.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN16[] **Search & Seizure, Warrants**

The *Fourth Amendment* does not require a perfect description of the data to be searched and seized,

however. Search warrants covering digital data may contain some ambiguity so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN17[] **Search & Seizure, Warrants**

A search warrant does not necessarily lack particularity simply because it is broad. Since a search of a computer is akin to a search of a residence, searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants. Similarly, traditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those records that are. And in many cases, the volume of records properly subject to seizure because of their evidentiary value may be vast. None of these consequences necessarily turns a search warrant into a prohibited general warrant.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN18[] **Search & Seizure, Warrants**

Breadth and particularity are related but distinct concepts. A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement. For example, a warrant may allow the government to search a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence. Similarly, when the criminal activity pervades an entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Warrants

Criminal Law & Procedure > Search & Seizure > Search Warrants > Particularity Requirement

HN19[] **Search & Seizure, Warrants**

An invasion of a criminal defendant's privacy is inevitable in almost any warranted search because in searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. The *Fourth Amendment* limits such unwarranted intrusions upon privacy, by requiring a warrant to describe its scope with particularity.

Constitutional Law > ... > Fundamental Rights > Search & Seizure > Exclusionary Rule

Criminal Law & Procedure > ... > Exclusionary Rule > Exceptions to Exclusionary Rule > Reasonable Reliance Upon Warrant

HN20[] **Search & Seizure, Exclusionary Rule**

The exclusion of evidence is inappropriate when the government acts in objectively reasonable reliance on a search warrant, even when the warrant is subsequently invalidated.

Criminal Law & Procedure > ... > Secrecy > Disclosure > Judicial Proceedings

HN21[] **Disclosure, Judicial Proceedings**

Grand jury proceedings are secret and a government attorney must not disclose a matter occurring before the grand jury, *Fed. R. Crim. P. 6(e)(2)(B)(vi)*, without a court order, *Rule 6(e)(3)(E)*, subject to limited exceptions.

Criminal Law & Procedure > Commencement of Criminal Proceedings > Grand Juries > Secrecy

HN22[] **Grand Juries, Secrecy**

The proper functioning of the grand jury system depends upon the secrecy of grand jury proceedings. There are five rationales for such secrecy: (1) to prevent the escape of those whose indictment may be contemplated; (2) to insure the utmost freedom to the grand jury in its deliberations, and to prevent persons subject to indictment or their friends from importuning the grand jurors; (3) to prevent subornation of perjury or tampering with the witnesses who may testify before the grand jury and later appear at the trial of those indicted by it; (4) to encourage free and untrammeled disclosures by persons who have information with respect to the commission of crimes; (5) to protect the innocent accused who is exonerated from disclosure of the fact that he has been under investigation, and from the expense of standing trial where there was no probability of guilt.

Criminal Law & Procedure > ... > Secrecy > Disclosure > Judicial Proceedings

HN23[] **Disclosure, Judicial Proceedings**

Fed. R. Crim. P. 6(e)(6) implements this policy of secrecy by requiring that all records, orders, and subpoenas relating to grand jury proceedings must be sealed.

Criminal Law & Procedure > ... > Secrecy > Disclosure > Judicial Discretion

Criminal Law & Procedure > ... > Disclosure > Standards > Particularized Need Standard

HN24[] **Disclosure, Judicial Discretion**

Information falling within Fed. R. Crim. P. 6(e)'s protections is entitled to a presumption of secrecy and closure. To rebut the presumption of secrecy, the party seeking disclosure must show a particularized need that outweighs the need for secrecy. To prove a particularized need, parties seeking disclosure must show that the material they seek is needed to avoid a possible injustice in another judicial proceeding, that the need for disclosure is greater than the need for continued secrecy, and that their request is structured to cover only material so needed. A district court's decision as to whether the burden of showing a particularized interest has been met will be overturned only if the court has abused its discretion.

Criminal Law & Procedure > Preliminary Proceedings > Discovery & Inspection > Discovery by Defendant

HN25[] **Discovery & Inspection, Discovery by Defendant**

Fed. R. Crim. P. 16(a)(1)(E) requires the government to disclose information within its control if the information is material to preparing the defense or will be a part of the government's case-in-chief. Evidence is material if it could be used to counter the government's case or to bolster a defense. An appellate court, in assessing the materiality of withheld information, considers not only the logical relationship between the information and the issues in the case, but also the importance of the information in light of the evidence as a whole. To justify a new trial, there must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor.

Criminal Law & Procedure > ... > Witnesses > Subpoenas > Discovery

Criminal Law & Procedure > ... > Witnesses > Subpoenas > Scope

HN26[] **Subpoenas, Discovery**

Fed. R. Crim. P. 17(c) allows parties to subpoena documents and objects to be introduced at criminal trials. A subpoena must meet three criteria: (1) relevancy; (2) admissibility; and (3) specificity. The party requesting the subpoena must also show that the information sought is not otherwise procurable reasonably in advance of trial by exercise of due diligence, that the party cannot properly prepare for trial

without such production, and that the application is made in good faith and is not intended as a general fishing expedition.

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > Discovery

HN27 **Abuse of Discretion, Discovery**

The appellate court reviews the district court's discovery rulings for abuse of discretion.

Criminal Law & Procedure > Trials > Continuances

HN28 **Trials, Continuances**

A district court has a great deal of latitude in scheduling trials. Thus, trial courts enjoy very broad discretion in granting or denying trial continuances. A decision to grant or deny a request for an adjournment is reviewed for abuse of discretion, and courts will find no such abuse unless the denial was an arbitrary action that substantially impaired the defense. Thus, the party seeking a continuance has the burden of showing both arbitrariness and prejudice in order to obtain reversal based on a denial of an adjournment.

Evidence > ... > Statements as Evidence > Hearsay > Rule Components

HN29 **Hearsay, Rule Components**

Hearsay is not admissible unless an exception applies. Fed. R. Evid. 802. The Federal Rules of Evidence define hearsay as a declarant's out-of-court statement offered in evidence to prove the truth of the matter asserted in the statement. If the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay.

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > Evidence

HN30 **Abuse of Discretion, Evidence**

The trial court's ultimate decisions as to the admission or exclusion of evidence are reviewed for abuse of discretion.

Criminal Law & Procedure > Postconviction Proceedings > Motions for New Trial

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > New Trial

HN31 **Postconviction Proceedings, Motions for New Trial**

Fed. R. Crim. P. 33(a) provides that, on the defendant's motion, the court may vacate any judgment and grant a new trial if the interest of justice so requires. District courts have been advised to exercise Rule 33 authority sparingly and in the most extraordinary circumstances. Where a defendant's Brady claim was raised in a motion for a new trial pursuant to Rule 33, the appellate court reviews the denial of the motion for abuse of discretion. In the context of denying a Rule 33 motion, a district court abuses the discretion accorded to it when (1) its decision rests on an error of law or a clearly erroneous factual finding, or (2) its decision, though not necessarily the product of a legal error or a clearly erroneous factual finding, cannot be located within the range of permissible decisions.

Criminal Law & Procedure > ... > Discovery & Inspection > Brady Materials > Brady Claims

HN32 **Brady Materials, Brady Claims**

There are three components of a Brady violation: (1) The evidence at issue must be favorable to the accused, either because it is exculpatory or because it is impeaching; (2) that evidence must have been suppressed by the government, either willfully or inadvertently; and (3) prejudice must have ensued. Information is exculpatory if it relates to the defendant's guilt or innocence. In order to show that he has been prejudiced, a defendant must demonstrate a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different, such that the failure to disclose undermines confidence in the verdict. Thus, the prosecution must disclose exculpatory and impeachment information no later than the point at which a reasonable probability will exist that the outcome would have been different if an earlier disclosure had been made. In general, a prudent

prosecutor will err on the side of transparency, resolving doubtful questions in favor of disclosure.

Criminal Law & Procedure > ... > Duty of Disclosure > Witness Lists > Defense Witnesses

HN33 **Witness Lists, Defense Witnesses**

In general, the defendant must, at the government's request, give to the government a written summary of any expert testimony that a defendant intends to use. This summary must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications. Fed. R. Crim. P. 16(b)(1)(C). The purpose of the expert disclosure requirement is to minimize surprise that often results from unexpected expert testimony, reduce the need for continuances, and to provide the opponent with a fair opportunity to test the merit of the expert's testimony through focused cross-examination. Fed. R. Crim. P. 16, advisory committee's note. Indeed, with increased use of both scientific and nonscientific expert testimony, one of counsel's most basic discovery needs is to learn that an expert is expected to testify.

Criminal Law & Procedure > ... > Duty of Disclosure > Witness Lists > Appellate Review & Judicial Discretion

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > Discovery

HN34 **Witness Lists, Appellate Review & Judicial Discretion**

If a party fails to comply with Fed. R. Crim. P. 16, the district court has broad discretion in fashioning a remedy, which may include granting a continuance or ordering the exclusion of evidence. Rule 16(d)(2)(A)-(D) provides that a district court may order any other remedy that is just under the circumstances. The appellate court thus reviews the district court's choice of remedy for abuse of discretion. In considering whether the district court abused its discretion, the appellate court looks to the reasons why disclosure was not made, the extent of the prejudice, if any, to the opposing party, the feasibility of rectifying that prejudice by a continuance, and any other relevant circumstances.

Evidence > Admissibility > Expert Witnesses > Daubert Standard

HN35 **Expert Witnesses, Daubert Standard**

Daubert requires the district court to make a preliminary assessment of whether the reasoning or methodology underlying the expert testimony is scientifically valid and can be applied to the facts in issue.

Evidence > Admissibility > Expert Witnesses > Daubert Standard

HN36 **Expert Witnesses, Daubert Standard**

A Daubert reliability assessment requires a district court to consider the extent to which the expert's theory has been subjected to peer review and publication, whether the technique is subject to standards controlling the technique's operation, the known or potential rate of error, and the degree of acceptance within the relevant scientific community. That inquiry is a flexible one, however, and Daubert is not a definitive checklist or test for the reliability of expert testimony. Thus, whether Daubert's specific factors are, or are not, reasonable measures of reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine.

Criminal Law & Procedure > ... > Discovery & Inspection > Brady Materials > Duty of Disclosure

HN37 **Brady Materials, Duty of Disclosure**

Careful consideration of a range of possible sanctions short of preclusion is especially important in the atypical case where a criminal defendant, rather than the government, is precluded from putting on his case because of a Fed. R. Crim. P. 16 violation. Limiting the defense's presentation of his case implicates the fundamental right of an accused to present witnesses in his own defense. However, the defendant must still comply with established rules of procedure and evidence designed to assure both fairness and reliability in the ascertainment of guilt and innocence.

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > Evidence

HN38[] **Abuse of Discretion, Evidence**

The appellate court reviews a trial court's decision to limit the scope of cross-examination for abuse of discretion.

Constitutional Law > ... > Fundamental Rights > Criminal Process > Right to Confrontation

Evidence > ... > Examination > Cross-Examinations > Scope

Criminal Law & Procedure > Trials > Defendant's Rights > Right to Confrontation

HN39[] **Criminal Process, Right to Confrontation**

A district court is accorded broad discretion in controlling the scope and extent of cross-examination. Fed. R. Evid. 611(a). Thus, a district court may impose reasonable limits on cross-examination to protect against, e.g., harassment, prejudice, confusion, and waste. In general, however, a district court should afford wide latitude to a defendant in a criminal case to cross-examine government witnesses. That is so because the Confrontation Clause gives a defendant the right not only to cross-examination, but to effective cross-examination. It does not follow, of course, that the Confrontation Clause prevents a trial judge from imposing any limits on defense counsel's cross-examination of government witnesses.

Criminal Law & Procedure > Trials > Witnesses > Presentation

Criminal Law & Procedure > Defenses > Right to Present

HN40[] **Witnesses, Presentation**

In order to elicit testimony implicating an alternative perpetrator, a defendant must show that his proffered evidence on the alleged alternative perpetrator is sufficient, on its own or in combination with other evidence in the record, to show a nexus between the crime charged and the asserted alternative perpetrator. Thus, to avoid a grave risk of jury confusion, a defendant must offer more than unsupported speculation that another person may have done the crime. An agent's state of mind as the investigation progressed is ordinarily of little or no relevance to the question of the defendant's guilt.

Evidence > ... > Procedural Matters > Objections & Offers of Proof > Objections

Evidence > ... > Procedural Matters > Objections & Offers of Proof > Timeliness

HN41[] **Objections & Offers of Proof, Objections**

An objection should be made after the question has been asked but before an answer has been given. That rule is not inflexible, however, and courts do not necessarily find an objection affirmatively waived because it might have been interposed a few questions earlier.

Evidence > ... > Examination > Cross-Examinations > Scope

HN42[] **Examination, Cross-Examinations**

Once any direct examination is concluded, cross-examination within the scope of the direct follows.

Evidence > ... > Statements as Evidence > Hearsay > Hearsay Within Hearsay

HN43[] **Hearsay, Hearsay Within Hearsay**

When confronted with hearsay within hearsay, or double hearsay, courts must determine that each part of the combined statement is independently admissible.

Criminal Law & Procedure > ... > Standards of Review > Abuse of Discretion > Evidence

HN44[] **Abuse of Discretion, Evidence**

A district court's ultimate decisions as to the admission or exclusion of evidence are reviewed for abuse of discretion, and will not be disturbed unless they are manifestly erroneous.

Evidence > ... > Hearsay > Exceptions > Statements

Against Interest

HN45 **Exceptions, Statements Against Interest**

To invoke the *Fed. R. Evid. 804(b)(3)* exception for a statement against interest, the proponent of the statement must show (1) that the declarant is unavailable as a witness, (2) that the statement is sufficiently reliable to warrant an inference that a reasonable man in the declarant's position would not have made the statement unless he believed it to be true, and (3) that corroborating circumstances clearly indicate the trustworthiness of the statement. The exception applies only if the district court determines that a reasonable person in the declarant's shoes would perceive the statement as detrimental to his or her own penal interest. The key to this inquiry is whether the statement is sufficiently self-inculpatory, which the district court must evaluate on a case-by-case basis.

Constitutional Law > ... > Fundamental Rights > Procedural Due Process > Self-Incrimination Privilege

HN46 **Procedural Due Process, Self-Incrimination Privilege**

In the *Fifth Amendment* context, there can be a legitimate fear of adverse consequences from further testimony where a sentence has not yet been imposed.

Evidence > ... > Hearsay > Exceptions > Residual Exception

HN47 **Exceptions, Residual Exception**

Fed. R. Evid. 807 provides for a limited, residual exception to the rule against hearsay where no other exception applies. A hearsay statement may be admissible under *Rule 807* if: (i) it is particularly trustworthy; (ii) it bears on a material fact; (iii) it is the most probative evidence addressing that fact; (iv) its admission is consistent with the rules of evidence and advances the interests of justice; and (v) its proffer follows adequate notice to the adverse party. The residual hearsay exception will be used very rarely, and only in exceptional circumstances.

Criminal Law & Procedure > ... > Appeals > Standards of Review > Abuse of Discretion

Criminal Law & Procedure > Sentencing > Appeals > Proportionality & Reasonableness Review

HN48 **Standards of Review, Abuse of Discretion**

A district court has broad latitude to impose either a United States Sentencing Guidelines sentence or a non-Guidelines sentence. Accordingly, the role of the court of appeals is limited to examining a sentence for reasonableness, which is akin to review under an abuse-of-discretion' standard. This standard applies both to the substantive reasonableness of the sentence itself and to the procedures employed in arriving at the sentence.

Criminal Law & Procedure > Sentencing > Imposition of Sentence > Factors

Criminal Law & Procedure > Sentencing > Appeals > Proportionality & Reasonableness Review

Criminal Law & Procedure > Sentencing > Ranges

Criminal Law & Procedure > Sentencing > Sentencing Guidelines

HN49 **Imposition of Sentence, Factors**

A sentence is procedurally unreasonable if the district court fails to calculate (or improperly calculates) the Sentencing Guidelines range, treats the Sentencing Guidelines as mandatory, fails to consider the *18 U.S.C.S. § 3553(a)* factors, selects a sentence based on clearly erroneous facts, or fails adequately to explain the chosen sentence. To hold that a factual finding is clearly erroneous, the court must be left with the definite and firm conviction that a mistake has been committed. Where there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous. In general, a sentencing court has discretion to consider a wide range of information in arriving at an appropriate sentence. The district court's factual findings at sentencing need be supported only by a preponderance of the evidence. Where the appellate court identifies procedural error in a sentence, but the record indicates clearly that the district court would have

imposed the same sentence in any event, the error may be deemed harmless, avoiding the need to vacate the sentence and to remand the case for resentencing.

Civil Procedure > Appeals > Amicus Curiae

HN50 **Appeals, Amicus Curiae**

The court is not required to address arguments raised only by an amicus.

Constitutional Law > ... > Fundamental Rights > Criminal Process > Right to Jury Trial

Criminal Law & Procedure > Sentencing > Imposition of Sentence > Factors

HN51 **Criminal Process, Right to Jury Trial**

A district court may consider as part of its sentencing determination uncharged conduct proven by a preponderance of the evidence as long as that conduct does not increase either the statutory minimum or maximum available punishment. Broad sentencing discretion, informed by judicial factfinding, does not violate the *Sixth Amendment*.

Criminal Law & Procedure > ... > Appeals > Standards of Review > Abuse of Discretion

HN52 **Standards of Review, Abuse of Discretion**

The appellate court will set aside a district court's substantive sentencing determination only in exceptional cases where the trial court's decision cannot be located within the range of permissible decisions. The appellate court's review is deferential, and it does not consider what weight it would have given a particular factor. Rather, the appellate court considers whether the factor, as explained by the district court, can bear the weight assigned it under the totality of the circumstances in the case. The appellate court's role in patrolling the boundaries of reasonableness is modest. Accordingly, the appellate court will set aside only those outlier sentences that reflect actual abuse of a district court's considerable sentencing discretion.

Criminal Law & Procedure > Sentencing > Imposition of Sentence > Factors

Criminal Law & Procedure > Sentencing > Appeals > Proportionality & Reasonableness Review

Criminal Law & Procedure > Sentencing > Sentencing Guidelines

HN53 **Imposition of Sentence, Factors**

That the sentence imposed accorded with the United States Sentencing Guidelines recommendation does not automatically render it reasonable. The Guidelines are, however, themselves a factor that Congress has directed district courts to consider. *18 U.S.C.S. § 3553(a)(4)(A)*. Moreover, as the considered judgment of the United States Sentencing Commission, they bear on the other factors that Congress has required courts to evaluate, including the need to reflect the seriousness of the offense, *§ 3553(a)(2)(A)*, to provide adequate deterrence, *§ 3553(a)(2)(B)*, and, because they are considered by all judges throughout the federal system, the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct, *§ 3553(a)(6)*.

Criminal Law & Procedure > Sentencing > Imposition of Sentence > Factors

HN54 **Imposition of Sentence, Factors**

The ability of a sentence to afford adequate deterrence to criminal conduct is a factor that district courts are required by Congress to consider in arriving at the appropriate sentence. *18 U.S.C.S. § 3553(a)(2)(B)*

Counsel: JOSHUA L. DRATEL, Joshua L. Dratel, P.C., New York, NY, for defendant-appellant Ross William Ulbricht.

EUN YOUNG CHOI, Assistant United States Attorney (Michael D. Neff, Timothy T. Howard, Adam S. Hickey,

Assistant United States Attorneys, on the brief), for Preet Bharara, United States Attorney for the Southern District of New York, New York, NY.

Tamar Todd, Jolene Forman, Drug Policy Alliance, Oakland, CA, for amici curiae Drug **[**2]** Policy Alliance, Law Enforcement Against Prohibition, JustLeadershipUSA, and Nancy Gertner.

Joel B. Rudin, Law Offices of Joel B. Rudin, P.C., New York, NY; Steven R. Morrison, University of North Dakota School of Law, Grand Forks, ND, for amicus curiae National Association of Criminal Defense Lawyers.

Judges: Before: NEWMAN, LYNCH, and DRONEY, Circuit Judges.

Opinion by: GERARD E. LYNCH

Opinion

[*82] GERARD E. LYNCH, *Circuit Judge*:

Defendant Ross William Ulbricht appeals from a judgment of conviction and sentence to life imprisonment entered in the United States District Court for the Southern District of New York (Katherine B. Forrest, *J.*). A jury convicted Ulbricht of drug trafficking and other crimes associated with his creation and operation of Silk Road, an online marketplace whose users primarily purchased and sold illegal goods and services. He challenges several aspects of his conviction and sentence, arguing that (1) the district court erred in denying his motion to suppress evidence assertedly obtained in violation of the *Fourth Amendment*; (2) the district court committed numerous errors that deprived him of his right to a fair trial, and incorrectly denied his motion for a new trial; and (3) his life sentence is both procedurally **[**3]** and substantively unreasonable. Because we identify no reversible error, we AFFIRM Ulbricht's conviction and sentence in all respects.

BACKGROUND

In February 2015, a jury convicted Ross William Ulbricht on seven counts arising from his creation and operation of Silk Road under the username Dread Pirate Roberts ("DPR").[1] Silk Road was a massive, anonymous criminal marketplace that operated using the Tor Network, which renders Internet traffic through the Tor browser extremely difficult to trace.[2] Silk Road users principally bought and sold drugs, false identification documents, and computer hacking software. Transactions on Silk Road exclusively used Bitcoins, an **[*83]** anonymous but traceable digital currency.[3] The site also contained a private message system, which allowed users to send messages to each other (similar to communicating via email), a public forum to discuss topics related to Silk Road, and a "wiki," which is like an encyclopedia that users could access to receive advice

[1] The seven crimes of conviction were: (1) distribution and aiding and abetting distribution of narcotics, *21 U.S.C. § 812*, *§ 841(a)(1)*, *§ 841(b)(1)(A)* and *18 U.S.C. § 2*; (2) using the Internet to distribute narcotics, *21 U.S.C. § 812*, *§ 841(h)* and *§ 841(b)(1)(A)*; (3) conspiracy to distribute narcotics, *21 U.S.C. § 846*; (4) engaging in a continuing criminal enterprise, *21 U.S.C. § 848(a)*; (5) conspiring to obtain unauthorized access to a computer for purposes of commercial advantage and private financial gain and in furtherance of other criminal and tortious acts, *18 U.S.C. § 1030(a)(2)* and *§ 1030(b)*; (6) conspiring to traffic in fraudulent identification documents, *18 U.S.C. § 1028(f)*; and (7) conspiring to launder money, *18 U.S.C. § 1956(h)*.

[2] Tor is short for the "The Onion Router." The Tor Network is "a special network on the Internet designed to make it practically impossible to physically locate the computers hosting or accessing websites on the network." App'x 53. The Tor Network can be accessed via the Tor browser using software that anyone may obtain for free on the Internet.

[3] Bitcoins allow vendors and customers to maintain their anonymity in the same way that cash does, by transferring Bitcoins between anonymous Bitcoin accounts, which do not contain any identifying information about the user of each account. The currency is "traceable" in that the transaction history of each individual Bitcoin is logged in what is called the blockchain. The blockchain prevents a person from spending the same Bitcoin twice, allowing Bitcoin to operate similarly to a traditional form of currency. Bitcoin is also a completely decentralized currency, operating free of nation states or central banks; anyone who downloads the Bitcoin software becomes part of the Bitcoin network. The blockchain is stored on that network, and the blockchain automatically "self-updates" when a Bitcoin transaction takes place. Tr. 160.

about using the site. Silk Road customers and vendors could also access a support section of the website to seek help from the marketplace's administrators when an issue arose.

According to the government, between **[**4]** 2011 and 2013, thousands of vendors used Silk Road to sell approximately $183 million worth of illegal drugs, as well as other goods and services. Ulbricht, acting as DPR, earned millions of dollars in profits from the commissions collected by Silk Road on purchases. In October 2013, the government arrested Ulbricht, seized the Silk Road servers, and shut down the site.

I. Silk Road Investigation

After Ulbricht created Silk Road in 2011, the site attracted the interest of at least two separate divisions of the Department of Justice:[4] the United States Attorney's Offices for the District of Maryland and for the Southern District of New York. Throughout the investigations, law enforcement agents knew that the person using Dread Pirate Roberts as his or her Silk Road username had created and managed the site, but they did not know DPR's actual identity. In 2012 and 2013, agents from both offices investigated several individuals who the government suspected were operating Silk Road as DPR. Those individuals included Ulbricht, Anand Athavale, and Mark Karpeles. Ultimately, the New York office identified Ulbricht as DPR, but the Maryland office had investigated and later abandoned the theory **[**5]** that either Athavale or Karpeles might have been Dread Pirate Roberts.

Two aspects of the pre-arrest investigation into Ulbricht are particularly relevant to this appeal: (1) the pen/trap orders that the government obtained to monitor Internet Protocol ("IP") address traffic to and from various devices associated with Ulbricht; and (2) the corrupt behavior of two Baltimore agents who worked on the Silk Road investigation.

A. The Pen/Trap Orders

In September 2013, after Ulbricht became a primary suspect in the DPR investigation, the government obtained five "pen/trap" orders. *See* 18 U.S.C. §§ 3121-27 ("Pen/Trap Act"). The orders authorized law enforcement agents to collect IP address data for Internet traffic to and from Ulbricht's home wireless router and other devices that regularly connected to Ulbricht's home router. According to the government's applications for the pen register and trap and trace device, "[e]very device on the Internet is identified by a **[*84]** unique number" called an IP address. S.A. 73.[5] "This number is used to route information between devices, for example, between two computers." *Id.* at 73-74. In other words, an "IP address is analogous to a telephone number" because "it indicates the online identity of **[**6]** the communicating device without revealing the communication's content." *Id.* at 74. Ulbricht does not dispute that description of how IP addresses function.

The pen/trap orders thus did not permit the government to access the content of Ulbricht's communications, nor did the government "seek to obtain[] the contents of any communications." *Id.* at 75. According to Ulbricht, the government's use of his home Internet routing data violated the *Fourth Amendment* because it helped the government match Ulbricht's online activity with DPR's use of Silk Road. Ulbricht argues that he has a constitutional privacy interest in IP address traffic to and from his home and that the government obtained the pen/trap orders without a warrant, which would have required probable cause.

B. Corrupt Agents Force and Bridges

One of the many other tactics that the government used to expose DPR's identity was to find low-level Silk Road administrators who helped DPR maintain the site, obtain their cooperation, take over their Silk Road usernames, and chat with DPR under those identities. The true owners of the administrator accounts would assist in the investigation by helping the government chat with DPR and access various aspects of the site. **[**7]** Government agents would also create their own new usernames and pose as drug dealers or buyers to purchase or sell narcotics and occasionally contact DPR directly. One of the government's principal trial witnesses, Special Agent Jared Der-Yeghiayan, used the former technique to chat with DPR under the name Cirrus. Cirrus had been a member of the Silk Road support staff before the government took over his

[4] The government first learned of Silk Road and began investigating it in 2011 after international packages containing drugs were intercepted at Chicago's O'Hare airport.

[5] S.A. refers to the joint sealed appendix in this case. Portions of the sealed appendix quoted in this opinion are to that extent unsealed.

account, and Der-Yeghiayan frequently used Silk Road's messaging system to communicate with DPR and other administrators as Cirrus. Cirrus also gave the government access to the staff chat, a separate program allowing DPR to communicate only with his employees.

Two undercover agents involved in the Silk Road investigation are of particular import to this appeal: Secret Service Special Agent Shaun Bridges and Drug Enforcement Administration ("DEA") Special Agent Carl Force, both of whom were assigned to the Baltimore investigation. Both Force and Bridges used their undercover access to exploit the site for their own benefit in various ways, and they eventually pleaded guilty to criminal charges in connection with their work on the Silk Road investigation.[6]

For example, Force and Bridges **[**8]** took over an administrator account belonging to Curtis Green, who worked for Silk Road under the name Flush. According to the criminal complaint against Force and Bridges, in January 2013, Bridges used the Flush username to change other users' passwords, empty their Bitcoin wallets,[7] **[*85]** and keep $350,000 in Bitcoins in offshore bank accounts, all while attempting to hide his activity through a series of transactions.[8] Specifically, the complaint against Force and Bridges alleges that Bridges "act[ed] as an administrator to reset pins and passwords on various Silk Road vendors' accounts," then exchanged the Bitcoins for U.S. dollars using the Mt. Gox exchanger.[9] Supp. App'x 180. Shortly after he committed the January 2013 thefts, Bridges asked Force to chat with DPR as Nob, Force's authorized undercover username, to get advice about how to liquidate Bitcoins. He also sought Force's help in convincing Curtis Green (formerly Flush) to help him transfer Bitcoins to other accounts, and he ultimately tried to blame Green for the theft.

With the government's approval, Force also posed as a drug dealer and communicated with DPR as Nob. As part of his official undercover work as Nob, Force agreed to sell **[**9]** fraudulent identification documents to DPR for $40,000 in Bitcoins. According to the criminal complaint against the agents, Force kept the Bitcoins received by his Nob account in connection with that transaction for his personal use. On another occasion, again as part of his authorized undercover work, Force advised DPR that he had access to information about Silk Road from an invented corrupt government employee. DPR paid Force $50,000 in Bitcoins for purported inside law enforcement information; Force allegedly purloined that payment as well. Moreover, outside his authorized undercover work, Force operated another account under the name French Maid, through which he again offered to sell DPR information about the government's Silk Road investigation. Acting as French Maid, Force received about $100,000 in Bitcoins that he kept for his personal use.

Force created yet another unauthorized Silk Road account, under the name DeathFromAbove, which was unknown to law enforcement until the defense identified it during trial. Force used the DeathFromAbove account to try to extort money from DPR. For example, in one such chat that took place on April 16, 2013, DeathFromAbove told DPR that he **[**10]** knew that DPR's true identity was Anand Athavale. DeathFromAbove demanded a payment of $250,000 in exchange for which DeathFromAbove would remain silent about DPR's identity.[10] There is no evidence that DPR made the requested payment to DeathFromAbove;

---

[6] Both Force and Bridges pleaded guilty to money laundering and obstruction of justice; Force also pleaded guilty to extortion. Force was sentenced to 78 months in prison, and Bridges received a 71-month sentence.

[7] According to the criminal complaint against Ulbricht, a Bitcoin wallet is a storage method for Bitcoins. The wallet is associated with a Bitcoin address, which is "analogous to the account number for a bank account, while the 'wallet' is analogous to a bank safe where the money in the account is physically stored." App'x 59. Users can transact in Bitcoin by transferring Bitcoins from one "Bitcoin address to the Bitcoin address of another user, over the Internet." *Id.* Ulbricht does not dispute that definition.

[8] As described below, the government disclosed shortly before trial that Force was under investigation for Silk Road corruption, but said nothing about Bridges. Specifically, the pretrial disclosure noted that Force was under investigation for using the Flush account to steal $350,000, but the criminal complaint against the agents alleges that Bridges committed that particular theft. According to the government, both Force and Bridges had access to the Flush account, which might explain their initial suspicion that Force stole the funds.

[9] Mt. Gox was a prominent Bitcoin exchanger owned by Mark Karpeles.

[10] DeathFromAbove also referred to the $250,000 payment he demanded as "punitive damages." App'x 875. In the government's view, the "punitive damages" remark referenced the murder of a Silk Road administrator that Ulbricht ordered and paid for (but that was never carried out). That and other killings that DPR commissioned will be described in more detail below.

indeed, DPR shrugged off the **[*86]** attempted blackmail as "bogus." App'x 710.

As will be explained in more detail below, the district court prevented Ulbricht from introducing evidence at trial related to Force's corruption because doing so would have exposed the ongoing grand jury investigation into Force's conduct. The district court also denied Ulbricht discovery related to the investigation and excluded certain hearsay statements that arguably revealed Force's corruption. Ulbricht contends on appeal that the district court's various rulings concerning evidence related to Force deprived him of a fair trial. Additionally, Ulbricht did not learn of Bridges's corrupt conduct until after trial when the criminal complaint against both agents was unsealed. Thus, in his motion for a new trial, he argued that the belated disclosure violated his due process rights under *Brady v. Maryland, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963)*. Ulbricht contends on appeal that the district court incorrectly denied that motion. **[**11]**

II. Ulbricht's Arrest

Ulbricht was arrested in a San Francisco public library on October 1, 2013, after the government had amassed significant evidence identifying him as Dread Pirate Roberts. The arrest was successfully orchestrated to catch Ulbricht in the act of administering Silk Road as DPR. Federal agents observed Ulbricht enter the public library, and a few minutes later Dread Pirate Roberts came online in the Silk Road staff chat. Der-Yeghiayan, under the undercover administrator username Cirrus, initiated a chat with DPR, asking him to go to a specific place on the Silk Road site to address some flagged messages from users. Der-Yeghiayan reasoned that this would "force [Ulbricht] to log in under . . . his Dread Pirate Roberts account" in the Silk Road marketplace, as well as in the staff chat software. Tr. 331-32.

Once Der-Yeghiayan knew that DPR had logged onto the flagged message page in the marketplace, he signaled another agent to effect the arrest. Ulbricht was arrested, and incident to that arrest agents seized his laptop. The same chat that Der-Yeghiayan had initiated with Dread Pirate Roberts a few minutes earlier was open on Ulbricht's screen. Ulbricht also visited the **[**12]** flagged post in the marketplace that Der-Yeghiayan (as Cirrus) had asked DPR to look at during their chat. While he was chatting with Cirrus, moreover, Ulbricht had accessed Silk Road by using the "Mastermind" page. That page was available only to Dread Pirate Roberts.

A great deal of the evidence against Ulbricht came from the government's search of his laptop and his home after the arrest. On the day of Ulbricht's arrest, the government obtained a warrant to seize Ulbricht's laptop and search it for a wide variety of information related to Silk Road and information that would identify Ulbricht as Dread Pirate Roberts. Ulbricht moved to suppress the large quantity of evidence obtained from his laptop, challenging the constitutionality of that search warrant. Ulbricht argues on appeal that the district court erred in denying his motion to suppress. More details concerning the search warrant will be described in context below.

III. The Trial

Ulbricht's trial lasted approximately three weeks, from January 13 through February 4, 2015. Judge Forrest handled the complex and contentious trial with commendable patience and skill. Although Ulbricht does not challenge the sufficiency of the evidence **[**13]** to support the jury's verdict on any of the counts of conviction, we **[*87]** summarize the evidence presented at trial as context for the issues raised on appeal.

A. The Government's Case

The government presented overwhelming evidence that Ulbricht created Silk Road in 2011 and continued to operate the site throughout its lifetime by maintaining its computer infrastructure, interacting with vendors, crafting policies for site users, deciding what products would be available for sale on the site, and managing a small staff of administrators and software engineers. Defense counsel conceded in his opening statement that Ulbricht did in fact create Silk Road.

According to Ulbricht's own words in a 2009 email, Ulbricht originally conceived of Silk Road as "an online storefront that couldn't be traced back to [him] . . . where [his] customers could buy [his] products" and pay for them "anonymously and securely." Tr. 991. From 2009 through 2011, Ulbricht worked to get the site up and running, relying on computer programming assistance from others, including his friend Richard Bates. According to one of the journal entries discovered on his laptop, in 2010 Ulbricht began to grow hallucinogenic mushrooms **[**14]** to sell on the site "for cheap to get people interested." Tr. 899. As the site began to garner significant interest in 2011, Ulbricht wrote in his journal

that he was "creating a year of prosperity and power beyond what I have ever experienced before. Silk Road is going to become a phenomenon and at least one person will tell me about it, unknowing that I was its creator." Tr. 899-900.

1. Evidence Linking Ulbricht to Dread Pirate Roberts

Around January 2012, the Silk Road user who represented himself as the lead administrator of the site adopted the username Dread Pirate Roberts.[11] The name alludes to the pseudonym of a pirate in the popular novel and film *The Princess Bride* that is periodically passed on from one individual to another.[12] In order to assure users that posts purporting to be authored by DPR were indeed his own, DPR authenticated his posts using an electronic signature known as a PGP key.[13] Silk Road users had access to a public PGP key, and DPR had a private PGP key that he alone could use to sign his Silk Road posts. When DPR signed a post using his private key, Silk Road users could run the code in the public key, and if the post was signed with the correct private key the **[**15]** user would receive a message that the authentication was successful. The government recovered DPR's private PGP key on Ulbricht's laptop. Importantly, the public PGP key did not change during the site's life span, meaning that DPR used the same private key to sign his posts throughout the time that he administered Silk Road.

Additional evidence supported the conclusion that Ulbricht was Dread Pirate Roberts. For example, the instructions that DPR provided to Cirrus (the account that Der-Yeghiayan later used for undercover work) for how to access the staff chat and contact DPR directly were found in a file on Ulbricht's laptop. The government also discovered the following evidence, covering the entire period during **[*88]** which DPR managed the Silk Road site, on Ulbricht's computer: thousands of pages of chat logs with Silk Road employees; detailed journal entries describing Ulbricht's ownership of the site; a list that tracked Ulbricht's tasks and ideas related to Silk Road; a copy of Silk Road's database; and spreadsheets cataloguing both the servers that hosted Silk Road and expenses and **[**16]** profits associated with the site. The government seized approximately $18 million worth of Bitcoins from the wallet on Ulbricht's laptop and analyzed their transaction history (through blockchain records) to determine that about 89% of the Bitcoins on Ulbricht's computer came from Silk Road servers located in Iceland.

A search of Ulbricht's home yielded additional evidence linking him with the site. That evidence included two USB hard drives with versions of documents related to Silk Road that were also stored on Ulbricht's laptop. There were also handwritten notes crumpled in Ulbricht's bedroom trash can about ideas for improving Silk Road's vendor rating system—an initiative that Dread Pirate Roberts had just revealed through a post in a discussion forum on the site.

The government also introduced other circumstantial evidence connecting Ulbricht to DPR's activity on Silk Road, such as evidence matching Ulbricht's actual travel history with DPR's online discussion of his travel plans. As one concrete example, the government discovered a Tor Chat log[14] on Ulbricht's laptop memorializing DPR's chat with a user named H7. On October 30, 2011, DPR told H7 that he would be traveling soon. **[**17]** On Ulbricht's Gmail account, which uses an email address that incorporates his full name, the government discovered a travel itinerary from CheapAir that indicated that Ulbricht would be traveling on November 15, 2011.

The government introduced several additional examples of DPR discussing travel plans that matched up with travel disclosed in Ulbricht's email and social media activity. At one point, for example, Ulbricht uploaded photos to his Facebook account in an album entitled "Thailand, February 2012." DPR discussed going to Thailand in a Tor chat on January 27, 2012, indicating that he was in "Thailand now," attracted by the "allure of a warm beach." Tr. 1300. He also mentioned in a January 26 chat with a user named "vj," which stood for Variety Jones, that he was in Thailand to experience the "beaches and jungles." *Id.* at 1298. One of the photos in the Thailand Facebook album depicted Ulbricht "in front of what appears to be jungles and beaches," both of which were referenced in DPR's chats from late January. *Id.* at 1301.

---

[11] The timing of this change corresponds to a January 15, 2012 Tor chat between a user named "vj" and Ulbricht, in which vj advised Ulbricht to change his username from Admin to Dread Pirate Roberts.

[12] *See* William Goldman, *The Princess Bride: S. Morgenstern's Classic Tale of True Love and High Adventure* (1973); *The Princess Bride* (20th Century Fox 1987).

[13] PGP stands for "Pretty Good Privacy."

[14] Tor Chat is a program that allows "communication between people on the Tor network." Tr. 889.

2. Murders Commissioned by Dread Pirate Roberts

The government also presented evidence that DPR commissioned the murders of five people to protect Silk Road's anonymity, although there **[**18]** is no evidence that any of the murders actually occurred.[15] In **[*89]** March 2013, a Silk Road vendor whose username was FriendlyChemist threatened to release "thousands of usernames, ordr [*sic*] amounts, [and] addresses" of Silk Road customers and vendors if DPR did not ensure that FriendlyChemist received money from another person, Lucydrop. Tr. 1806. Releasing the information would have destroyed the affected users' anonymity, undermining the security of the site. In a later chat with another person, RealLucyDrop, DPR wrote that it would be "terrible" if the personal information were to be released, and thus he needed FriendlyChemist's "real world identity so I can threaten him with violence if he were to release any names." *Id.* at 1811.

The episode escalated from there. DPR connected with Redandwhite, who was FriendlyChemist's supplier, and wrote that "FriendlyChemist is a liability and I wouldn't mind if he was executed." *Id.* at 1822. After negotiating the logistical details of the murder, Ulbricht agreed to pay Redandwhite $150,000 in Bitcoins to kill FriendlyChemist. DPR paid Redandwhite, who later confirmed that he had received the payment and carried out the murder, and sent what appeared **[**19]** to be a photo of the dead victim to DPR. DPR replied that he had "received the picture and deleted it," and thanked Redandwhite for his "swift action." *Id.* at 1892. Around the same time, Ulbricht recorded in a file on his laptop that he "[g]ot word that the blackmailer was executed." *Id.* at 1887. The government was not able to develop any evidence linking these conversations to an actual murder. A reasonable jury could easily conclude, however, that the evidence demonstrated that Ulbricht ordered and paid for the killing, and that he believed that it had occurred.

Later, DPR ordered four other murders through Redandwhite. Dread Pirate Roberts identified another Silk Road user, Tony76, who knew FriendlyChemist and might compromise the site's anonymity. After some negotiations, DPR agreed to pay Redandwhite $500,000 in Bitcoins to kill Tony76 and three of his associates. DPR then sent the payment to Redandwhite. On April 6, 2013, Ulbricht wrote in a file on his laptop that he "[g]ave angels go ahead to find tony76." Tr. 1900. Two days later, Ulbricht recorded that he "[s]ent payment to angels for hit on tony76 and his three associates." *Id.* One of the government's expert witnesses was able to link the payments for all five **[**20]** murders to Bitcoin wallets located on Ulbricht's laptop. Again, while the evidence demonstrates that Ulbricht ordered and paid substantial sums for the murders, there is no evidence that the killings actually took place; the government theorized that Redandwhite had tricked Ulbricht into thinking that he actually committed the murders, but that in fact he had not.

B. The Defense Case

As noted above, Ulbricht conceded at trial that he had created Silk Road, and he was caught red-handed operating the site at the end of the investigation. His principal defense strategy at trial—more of an effort at mitigation than outright denial of his guilt of the conspiracy and other charges in the indictment—was to admit his role at the beginning and end of the site's operation, but to contend that he sold Silk Road to someone else in 2011 and **[*90]** abandoned his role as its administrator, only to be lured back by the successor DPR near the end of its operation to take the blame for operating the site. The defense attempted on several occasions to implicate as alternative suspects Karpeles and Athavale, both of whom the government had investigated for a possible connection to Silk Road but later abandoned **[**21]** as candidates for DPR's real-world identity. As part of his alternative-perpetrator defense, Ulbricht theorized that the person or persons who operated as the true Dread Pirate Roberts during the purported interim period planted incriminating evidence on his laptop in order to frame him. For the

[15] Ulbricht was not charged in this case with crimes based on ordering these killings, although evidence relating to the murders was introduced at trial as actions taken in furtherance of the charged conspiracies and criminal enterprise. The killings were referenced again in connection with Ulbricht's sentencing. He faces open attempted murder-for-hire charges in the District of Maryland, however. *United States v. Ulbricht*, No. 13-0222-CCB (D. Md.). That indictment charges Ulbricht with the attempted murder of Curtis Green (Flush). According to the criminal complaint against the corrupt officers, after Bridges, using Flush's account, stole $350,000 in Bitcoin in January 2013, DPR recruited Nob (Force) to kill Flush as punishment for the theft. DPR paid Nob $80,000 to carry out the murder, which Force faked to make Ulbricht believe that the task was complete. Presumably because the government removed from its trial evidence anything that the corrupted agent Force may have touched, it did not present evidence of the Flush murder-for-hire agreement, nor did it rely on that murder at sentencing.

most part, the defense advanced this theory through cross-examination of government witnesses. Ulbricht did not testify at trial.

One point in the testimony of Richard Bates exemplifies the defense's approach and the government's response. Bates, Ulbricht's friend who assisted with computer programming issues when Ulbricht launched Silk Road, testified for the government. According to Bates, Ulbricht told him in November 2011 that he had sold Silk Road to someone else, a claim that Bates believed at the time to be true. Moreover, in a February 2013 Google chat between Bates and Ulbricht, Ulbricht wrote that he was "[g]lad" that Silk Road was "not [his] problem anymore." Tr. 1140-41.[16] Bates understood that to mean that Ulbricht no longer worked on the site.

To mitigate any damage from Bates's testimony, the government introduced a December 9, 2011 Tor chat between Ulbricht and vj. In that chat, vj asked **[**22]** Ulbricht whether anyone else knew about his involvement in Silk Road. Ulbricht responded: "[U]nfortunately yes. There are two, but they think I sold the site and got out and they are quite convinced of it." Tr. 1191. He further wrote that those two people thought he sold the site "about a month ago," *id.*, which roughly corresponds to the November 2011 conversation between Bates and Ulbricht. Significantly, it was shortly after this conversation that vj suggested that Ulbricht change his online identity to DPR. In view of the fictional character it referenced, the government contended that the online moniker DPR was deliberately adopted to support the cover story that the lead administrator of Silk Road changed over time.

Thus, although the government elicited testimony that Ulbricht told Bates that he sold the site in 2011, it also presented evidence that Ulbricht had lied to Bates about that sale and continued to operate the site in secret.

1. Cross-Examination of Government Witnesses

Ulbricht's defense depended heavily on cross-examination of government witnesses, much of which was designed to support the argument that either Karpeles or Athavale was the real DPR, or that multiple people operated **[**23]** as Dread Pirate Roberts during Silk Road's life span. The district court limited his cross-examination in two ways that Ulbricht challenges on appeal. First, the district court prevented Ulbricht from exploring several specific topics with Der-Yeghiayan, the government's first witness, through whom it introduced much of its evidence. Those topics included, *inter alia*, Der-Yeghiayan's prior suspicions that Karpeles was DPR. Second, the district court limited Ulbricht's ability to cross examine FBI computer scientist Thomas Kiernan, who testified **[*91]** about evidence that he discovered on Ulbricht's laptop, concerning several specific technical issues related to software on Ulbricht's computer. More details about those attempted cross-examinations will be discussed in context below.

2. Hearsay Statements

Ulbricht also attempted to introduce two hearsay statements in his defense, both of which the district court excluded as inadmissible. Those hearsay statements comprise: (1) chats between DPR and DeathFromAbove (Force) concerning Force's attempt to extort money from DPR in exchange for information about the government's investigation of Silk Road; and (2) the government's letter describing a **[**24]** statement by Andrew Jones, a site administrator, concerning one particular conversation that he had with DPR. The contents of those hearsay statements and other relevant facts will be discussed in more detail below.

3. Defense Expert Witnesses

Long after the trial began on January 13, 2015, and shortly before the government rested on February 2 and the defense rested on February 3, Ulbricht disclosed to the government his intent to call two expert witnesses: Dr. Steven Bellovin and Andreas Antonopoulos.[17] The Antonopoulos disclosure indicated that he would testify on several subjects relevant to Silk Road, including "the origins of Bitcoin," "the various purposes and uses of Bitcoin," "the mechanics of Bitcoin transactions," "the value of Bitcoin over time since its inception," and "the concepts of Bitcoin speculating and Bitcoin mining," among other things. App'x 349. The Bellovin disclosure followed a similar pattern, indicating that he would testify about "[g]eneral principles of internet security and vulnerabilities," the "import of some lines of PHP code provided to defense counsel in discovery," and "[g]eneral principles of public-key cryptography," among other topics. *Id.* at 360. Neither disclosure summarized **[**25]** the opinions that the experts would

[16] There are two versions of the trial transcript for January 22, 2015 on the district court docket. The page citations here refer to the version of the transcript marked "corrected," which is listed on the district court docket as Document No. 208 (14-cr-68).

[17] Ulbricht noticed his intent to call Antonopoulos on January 26 and Bellovin on January 30, 2015.

offer on those subjects, nor did either identify the bases for the experts' opinions.

On January 29 and 31, the government moved to preclude the testimony of both proffered experts. The government argued that the expert notices were untimely and did not contain the information required by *Rule 16 of the Federal Rules of Criminal Procedure*, including a summary of the opinions that the experts would offer on the stand.[18] On February 1—three days before the end of the trial—the district court granted the government's motions and precluded both experts from testifying, concluding that the defendant's notices were late and that the disclosures were substantively inadequate under *Rule 16*. Ulbricht claims that the district court erred in precluding his experts from testifying.

In sum, the defense case was limited to cross-examining government witnesses, briefly calling four character witnesses, having a defense investigator authenticate a task list on Ulbricht's computer, and reading a few of DPR's posts into the record. Ulbricht contends, however, that his defense was hamstrung by the rulings described above.

C. The Verdict and Post-Trial Motion

After deliberating for about three and a half hours, the jury returned **[**26]** a guilty verdict **[*92]** on all seven counts in the Indictment. As described in more detail below, Ulbricht then moved for a new trial under *Rule 33, Fed. R. Crim. P.* The district court denied the motion, and Ulbricht argues here that it erred in doing so.

IV. Sentencing

The United States Probation Office prepared the Pre-Sentence Investigation Report ("PSR") in March 2015. It described the offense conduct in detail and discussed the five murders that Ulbricht allegedly hired Redandwhite to commit.[19] Over Ulbricht's objection, the PSR also discussed six drug-related deaths that the government contended, and the district court found, were connected with Silk Road. Circumstantial evidence linked each of those fatalities with varying degrees of certainty to the decedent's purchase of drugs on Silk Road. For example, one user died from an overdose of heroin combined with other drugs. The deceased individual was found with a needle and a bag of heroin, as well as a torn-open delivery package. Open on his computer was a Silk Road chat in which a vendor described the package of heroin that was due to arrive that day, including a tracking number that matched the opened package.

Two other individuals whose deaths the PSR **[**27]** described were Silk Road customers who purchased drugs on the site shortly before their deaths. A fourth person died after ingesting a synthetic drug originally purchased on Silk Road that he obtained through an intermediary dealer, and a fifth died after leaping from a balcony while high on a psychedelic drug that he bought from the site. A sixth person died of pneumonia after placing over thirty orders for heroin and other drugs on Silk Road; the autopsy report theorized that his drug use may have "blunted the deceased's perception of the severity of his illness," thus contributing to his premature death. PSR ¶ 83. In arguing that the district court should consider the six deaths, the government explained that they "illustrate the obvious: that drugs can cause serious harm, including death." App'x 902.

In the first of several sentencing submissions, Ulbricht urged the district court not to consider the six drug-related deaths and to strike them from the PSR. In support of that argument, Ulbricht claimed that Silk Road had harm-reducing effects, meaning that it made drug use less dangerous. Specifically, Ulbricht employed Dr. Fernando Caudevilla (username Doctor X), a physician who **[**28]** provided drug-use advice to the site's customers. Caudevilla spent up to two or three hours a day on Silk Road discussion fora and sent over 450 messages providing guidance about illegal drug dosage and administration, as well as information about the harms associated with certain drugs. Caudevilla also provided weekly reports to DPR concerning the advice he gave to the site's users. Ulbricht further claimed that Silk Road allowed for better drug quality control because vendors were subject to a rating system,[20] buyers were able to choose from among many different

[18] The government also argued generally that some of the topics identified in the disclosures were not relevant to Ulbricht's case or did not require expert testimony.

[19] The PSR did not refer to the additional murder of "Flush" that DPR allegedly paid Force, under his undercover identity Nob, to commit. *See supra* note 15.

[20] As the government pointed out in its sentencing submission, fake vendor reviews were commonplace, and vendors sometimes coerced customers into giving them perfect ratings.

sellers, and the site's anonymity encouraged free dialogue about drug use that helped mitigate the stigma accompanying drug addiction.[21] According **[*93]** to Caudevilla, when the site received negative feedback about the quality of the drugs sold by a vendor, that vendor was removed from the site. Finally, Ulbricht claimed that the site reduced violence associated with the drug trade by providing a safe, computer-based method of purchasing drugs.

Ulbricht also submitted an expert report from Dr. Mark Taff, which provided an alternative reason for excluding the six deaths from the PSR. In his report, Dr. Taff explained that, based on the **[**29]** information available, it was impossible to know with medical certainty that Silk Road drugs caused the six deaths described in the PSR. There were "gaping holes" in the investigations into each death, and some were missing autopsy reports, toxicology reports, and death certificates. App'x 911. Moreover, Dr. Taff claimed that it was impossible to know the cause of each death because several of the deceased had ingested multiple drugs prior to their deaths. Ulbricht argued that, absent a clear causal link between the deaths and the offense conduct, the deaths were not relevant to his sentencing at all.

The defense later submitted another sentencing memorandum, which included 97 letters from friends and family describing Ulbricht's good character as well as academic articles about the myriad problems associated with unduly severe sentences for drug crimes. He also urged the district court not to consider the five murders commissioned by DPR, in part because he claimed only to have fantasized about the murders, implying that he did not expect them to be carried out. In its sentencing submission, the government requested that the district court impose a sentence substantially above the **[**30]** twenty-year mandatory minimum.

Ulbricht's sentencing hearing took place on May 29, 2015.[22] The district court concluded that Ulbricht's offense level was 43—the highest possible offense level under the Sentencing Guidelines—and that his criminal history category was I.[23] The high offense level largely resulted from the massive quantity of drugs trafficked using Silk Road, as well as several enhancements, including one for directing the use of violence, *U.S.S.G. § 2D1.1(b)(2)*.[24] Ulbricht does not dispute that calculation. Due to the high offense level, the Guidelines advisory sentence "range" was life in prison, and the U.S. Probation Office recommended that sentence.

At the sentencing hearing, the district court resolved several disputed issues of fact. For example, because Ulbricht contested **[*94]** his responsibility for the five commissioned murders for hire, the district court found by a preponderance of the evidence that Ulbricht did in fact commission the murders, believing that they would be carried out. The district court characterized the evidence of the murders for hire, which included Ulbricht's journal, chats with other Silk Road users, and the evidence showing that Ulbricht actually paid a total of $650,000 **[**31]** in Bitcoins for the killings, as "ample and unambiguous." App'x 1465.

The court then turned to the six drug-related deaths described in the PSR. Over Ulbricht's objection, the district court found that the deaths were "related conduct relevant to his sentencing" because the "question as to whether this information is properly included in the PSR is whether the Court finds, by a preponderance of the evidence[,] that the deaths, in some way, related to Silk Road." *Id.* at 1472. It went on to explain that "the relevant offense committed is the unlawful distribution of drugs and the running of a criminal drug enterprise, . . . [and] based on the evidence before the Court, the sale of the drugs through Silk Road caused harm to the

---

[21] Ulbricht referenced a study by Tim Bingham, who researched Silk Road users between September 2012 and August 2013. Bingham interviewed Silk Road customers and concluded that the site operated as a "novel technological drug subculture, potentially minimiz[ing] drug-related stigma by reinforcing a[] sense of community." App'x 905. Thus, Bingham concluded, and Ulbricht argued, that Silk Road encouraged more "responsible forms of recreational drug use." *Id.* at 906.

[22] At sentencing, the district court vacated Ulbricht's convictions on Counts One and Three because they were lesser included offenses of Counts Two and Four respectively. Ulbricht was therefore sentenced on Counts Two, Four, Five, Six, and Seven. The district court based its Guidelines calculation only on those counts.

[23] The calculated offense level was actually 50, which is higher than the maximum offense level of 43 on the Guidelines sentencing table. The Guidelines provide that "[a]n offense level of more than 43 is to be treated as an offense level of 43." ***U.S.S.G. ch. 5 pt. A, cmt. n.2***.

[24] Because of the grouping rules, ***U.S.S.G. ch. 3 pt. D***, the lower offense levels of the computer hacking and fraudulent identification charges did not contribute to Ulbricht's offense level.

decedents." *Id.* at 1473. The district court described the facts associated with five of the deaths and specifically found that each was connected to Silk Road, rejecting the defendant's argument that but-for causation was required in order for the court to consider the deaths as relevant to the offense conduct.[25] Parents of two of the decedents also made statements at the proceeding, describing the emotional impact that the losses had on them and their families.

In the course of explaining **[**32]** its reasons for choosing Ulbricht's sentence, the district court discussed the facts of Ulbricht's offense, his apparent character, and the purposes of criminal punishment. The court described Doctor X as "enabling," App'x 1530, rather than reducing the harms associated with drug use, emphasized the social costs attendant to expanding the scope of the drug market, discussed the five murders for hire, and stated that the sentence imposed on Ulbricht could have a powerful general deterrent effect because the case had attracted an unusually large amount of publicity. The court then sentenced Ulbricht principally to life imprisonment.

This appeal followed.

DISCUSSION

On appeal, Ulbricht raises a number of claims of error. For purposes of organizational clarity, we group them into three categories, and present them in the order in which the issues arose in the district court. Accordingly, we discuss first Ulbricht's claims that much of the evidence against him should have been suppressed because it was obtained in violation of his *Fourth Amendment* rights; second, his arguments that the district court's evidentiary errors denied him a fair trial; and third, his objections to his sentence.

I. *Fourth Amendment* Issues

Ulbricht **[**33]** claims that the district court erred in denying his motion to suppress evidence obtained in violation of the *Fourth Amendment*. ***HN1***[⬆] On appeal from a denial of a suppression motion, "we review a district court's findings of fact for clear error, and its resolution of questions of law **[*95]** and mixed questions of law and fact *de novo*." *United States v. Bohannon, 824 F.3d 242, 247-48 (2d Cir. 2016)*. Ulbricht raises two principal arguments. First, he contends that the pen/trap orders that the government used to monitor IP address traffic to and from his home router violated the *Fourth Amendment* because the government obtained the orders without a warrant. Second, he claims that the warrants authorizing the government to search his laptop as well as his Google and Facebook accounts violated the *Fourth Amendment's* particularity requirement. We reject those contentions and affirm the denial of Ulbricht's motion to suppress.

A. Pen/Trap Orders

Pursuant to orders issued by United States magistrate judges in the Southern District of New York, the government used five pen registers and trap and trace devices to monitor IP addresses associated with Internet traffic to and from Ulbricht's wireless home router and devices that regularly connected to that router. The government obtained the orders pursuant to ***HN2***[⬆] the Pen/Trap **[**34]** Act, which provides that a government attorney "may make [an] application for an order . . . authorizing or approving the installation and use of a pen register or a trap and trace device . . . to a court of competent jurisdiction." *18 U.S.C. § 3122(a)(1)*. A "pen register" is defined as a "device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," and "shall not include the contents of any communication." *Id. § 3127(3)*. A "trap and trace" device means "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." *Id. § 3127(4)*. Like pen registers, trap and trace devices may not capture the "contents of any communication." *Id.* The statute does not require a search warrant for the use of a pen register or trap and trace device, nor does it demand the kind of showing required to obtain such a warrant. Rather, the statute requires only that the application contain a "certification . . . that **[**35]** the information likely to be obtained is relevant to an ongoing criminal investigation." *Id. § 3122(b)(2)*.

[25] The district court did not specifically address one of the six deaths. That decedent was a frequent Silk Road customer who was found dead in his home with a used syringe and other drug paraphernalia. The record does not indicate why the district court did not discuss that case, and neither party makes any argument based on that omission.

The orders in this case authorized the government to "use a pen register and trap and trace device to identify the source and destination [IP] addresses, along with the dates, times, durations, ports of transmission, and any Transmission Control Protocol ('TCP') connection data,[26] associated with any electronic communications sent to or from" various devices, including Ulbricht's home wireless router and his laptop.[27] S.A. 93. In each order, the government **[*96]** specified that it did not seek to obtain the contents of any communications. Instead, it sought authorization to collect only "dialing, routing, addressing, and signaling information" that was akin to data captured by "traditional telephonic pen registers and trap and trace devices." *Id.* at 130. Ulbricht claims that the pen/trap orders violated the *Fourth Amendment* because he had a reasonable expectation of privacy in the IP address routing information that the orders allowed the government to collect.[28]

HN3[↑] The *Fourth Amendment to the United States Constitution* provides that: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, **[**36]** and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The "cornerstone of the modern law of searches is the principle that, to mount a successful *Fourth Amendment* challenge, a defendant must demonstrate that he personally has an expectation of privacy in the place searched." *United States v. Haqq, 278 F.3d 44, 47 (2d Cir. 2002)* (internal quotation marks omitted). Thus, a "*Fourth Amendment* 'search[]' . . . does not occur unless the search invades an object or area [in which] one has a subjective expectation of privacy that society is prepared to accept as objectively reasonable." *United States v. Hayes, 551 F.3d 138, 143 (2d Cir. 2008)*.

The Supreme Court has long held that ***HN4***[↑] a "person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," including phone numbers dialed in making a telephone call and captured by a pen register. *Smith v. Maryland, 442 U.S. 735, 743-44, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979)*. This is so because phone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes." *Id. at 743*. Similarly, "e-mail and Internet **[**37]** users . . . rely on third-party equipment in order to engage in communication." *United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)*. Internet users thus "should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information." *Id.* Moreover, "IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers." *United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010)* (internal quotation marks omitted).

Ulbricht notes that questions have been raised about whether some aspects of modern technology, which entrust great quantities of significant personal information to **[*97]** third party vendors, arguably making extensive government surveillance possible, call for a re-evaluation of the third-party disclosure doctrine established by *Smith*. *See, e.g., United States v. Jones, 565 U.S. 400, 417-18, 132 S. Ct. 945, 181 L. Ed. 2d 911 (2012)* (Sotomayor, J., concurring); *American Civil Liberties Union v. Clapper, 785 F.3d 787, 824 (2d Cir.*

---

[26] Data are transmitted on the Internet via discrete packets, rather than in a continuous stream. TCP is a "communications protocol used to process such data packets associated with popular Internet applications," such as browser and e-mail applications. S.A. 97. Like IP address data, the TCP data that the orders permitted the government to acquire do not include the contents of communications, and Ulbricht has not expressed any independent concern over the government's collection of TCP connection data.

[27] Some of the pen/trap orders phrased the scope of the order slightly differently. For example, one order authorized installing "a trap and trace device to identify the source [IP] address of any Internet communications directed to, and a pen register to determine the destination IP addresses of any Internet communications originating from," the relevant devices. S.A. 67. In other words, not every order sought TCP connection data as well as IP address information. Neither party has suggested that the differences among the pen/trap orders are material to any issue presented by this appeal.

[28] In the district court, Ulbricht made the same arguments concerning his *Fourth Amendment* privacy interest in the information captured by the pen registers and trap and trace devices. The district court ruled generally that the "type of information sought [in the orders] was entirely appropriate for that type of order." App'x 208. The court declined to address Ulbricht's "novel *Fourth Amendment* arguments" regarding the pen/trap devices because he had "not established the requisite privacy interest . . . to" demonstrate his standing to challenge the orders. *Id.* The government has agreed that Ulbricht has standing to pursue his *Fourth Amendment* arguments on appeal.

2015). HN5[↑] We remain bound, however, by that rule until and unless it is overruled by the Supreme Court. *See* United States v. Gomez, 580 F.3d 94, 104 (2d Cir. 2009); *see also* United States v. Wheelock, 772 F.3d 825, 829 (8th Cir. 2014).

Moreover, whatever novel or more intrusive surveillance techniques might present future questions concerning the appropriate scope of the third-party disclosure doctrine, the orders in this case do not present such issues. The recording of IP **[**38]** address information and similar routing data, which reveal the existence of connections between communications devices without disclosing the content of the communications, are precisely analogous to the capture of telephone numbers at issue in *Smith*. That is why the orders here fit comfortably within the language of a statute drafted with the earlier technology in mind. The substitution of electronic methods of communication for telephone calls does not alone create a reasonable expectation of privacy in the identities of devices with whom one communicates. Nor does it raise novel issues distinct from those long since resolved in the context of telephone communication, with which society has lived for the nearly forty years since *Smith* was decided. Like telephone companies, Internet service providers require that identifying information be disclosed in order to make communication among electronic devices possible. In light of the *Smith* rule, no reasonable person could maintain a privacy interest in that sort of information.

We therefore join the other circuits that have considered this narrow question and hold that HN6[↑] collecting IP address information devoid of content is "constitutionally **[**39]** indistinguishable from the use of a pen register." *Forrester, 512 F.3d at 510*; *see, e.g., Wheelock, 772 F.3d at 828* (holding that HN7[↑] the defendant "cannot claim a reasonable expectation of privacy in [the] government's acquisition of his subscriber information, including his IP address and name," because it had been "revealed to a third party" (internal quotation marks omitted)); Christie, 624 F.3d at 573 (holding that HN8[↑] there is no expectation of privacy in "subscriber information provided to an internet provider," such as an IP address (internal quotation marks omitted)); *see also* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that HN9[↑] "computer users do not have a legitimate expectation of privacy in their [bulletin board] subscriber information because they have conveyed it to another person"); United States v. Graham, 824 F.3d 421, 432 (4th Cir. 2016) (en banc) (noting that HN10[↑] "third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection"); United States v. Carpenter, 819 F.3d 880, 887 (6th Cir. 2016) (HN11[↑] "[C]ourts have not (yet, at least) extended [Fourth Amendment] protections to the internet analogue to envelope markings, namely the metadata used to route internet communications, like . . . IP addresses."). Where, as here, the government did not access the contents of any of Ulbricht's communications, it did not need to obtain a warrant to collect IP address routing information in which **[**40]** Ulbricht did not have a legitimate privacy interest. We therefore reject Ulbricht's contention that the issuance of such orders **[*98]** violated his Fourth Amendment rights.[29]

Ulbricht's additional arguments are not persuasive. Ulbricht contends generally that pen/trap orders may monitor a communication's content by tracking metadata, but he does not identify what metadata the government might have collected or explain how the pen/trap orders in this case gave the government information concerning the content of his communications. He also claims that the orders violated the Fourth Amendment by impermissibly monitoring activity within his home, relying on Kyllo v. United States, 533 U.S. 27, 121 S. Ct. 2038, 150 L. Ed. 2d 94 (2001). In *Kyllo*, the Court held that using thermal-imaging technology from outside the home to discern whether a person was growing marijuana in the home might reveal innocent, non-criminal information in which a resident has a privacy interest. Id. at 38. Ulbricht contends that monitoring IP address traffic through his

---

[29] The issue presented in this case is narrowly confined to orders that are limited to the capture of IP addresses, TCP connection data, and similar routing information. Our holding therefore does not address other, more invasive surveillance techniques that capture more information (such as content), which may require a warrant issued on probable cause or an order pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, codified as amended at 18 U.S.C. §§ 2510-22. *See generally* In the Matter of a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 393-96 (S.D.N.Y. 2014), as amended (Aug. 7, 2014) (describing the available caselaw concerning search warrants of email accounts). Similarly, to the extent that some of the out-of-circuit cases cited in the text also address the Fourth Amendment status of other types of evidence, such as historical cell-site location information, we express no views on such issues, which are not presented in this case.

router is similar to the thermal-imaging technology because it might reveal when and how Ulbricht used his computer when he was at home. The same can **[**41]** be said, however, of an ordinary telephone pen register, which can reveal if, when, and how a person uses his or her home phone to make calls. *See* Smith, 442 U.S. at 743. IP address traffic similarly reveals whether an Internet subscriber (or, more precisely, a person who uses the subscriber's Internet connection) is home and using the Internet. Nothing in Kyllo suggests that government monitoring of data disclosed to an outside telephone or Internet provider for ordinary business purposes becomes constitutionally suspect when investigators use that information to draw inferences about whether someone is making telephone calls or accessing websites from inside his or her home. We therefore see no constitutional difference between monitoring home phone dialing information and IP address routing data. Thus, we conclude that the pen register and trap and trace orders did not violate the Fourth Amendment.[30]

[*99] B. Search Warrants

Ulbricht also contends that the warrants authorizing the search and seizure of his laptop as well as his Facebook and Google accounts violated the Fourth Amendment's particularity requirement. **HN12**[↑] The Fourth Amendment explicitly commands that warrants must be based on probable cause and must "particularly describ[e] the place to be searched, and the persons **[**42]** or things to be seized." U.S. Const. amend. IV. "It is familiar history that indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." Payton v. New York, 445 U.S. 573, 583, 100 S. Ct. 1371, 63 L. Ed. 2d 639 (1980). Those general warrants "specified only an offense," leaving "to the discretion of the executing officials the decision as to which persons should be arrested and which places should be searched." Steagald v. United States, 451 U.S. 204, 220, 101 S. Ct. 1642, 68 L. Ed. 2d 38 (1981). The principal defect in such a warrant was that it permitted a "general, exploratory rummaging in a person's belongings," Andresen v. Maryland, 427 U.S. 463, 480, 96 S. Ct. 2737, 49 L. Ed. 2d 627 (1976) (internal quotation marks omitted), a problem that the Fourth Amendment attempted to resolve by requiring the warrant to "set out with particularity" the "scope of the authorized search," Kentucky v. King, 563 U.S. 452, 459, 131 S. Ct. 1849, 179 L. Ed. 2d 865 (2011).[31]

HN14[↑] To be sufficiently particular under the Fourth Amendment, a warrant must satisfy three requirements. First, "a warrant must identify the specific offense for which the police have established probable cause." United States v. Galpin, 720 F.3d 436, 445 (2d Cir. 2013). Second, "a warrant must describe the place to be searched." Id. at 445-46. Finally, the "warrant must specify the items to be seized by their relation to designated crimes." Id. at 446 (internal quotation marks omitted).

HN15[↑] "Where, as here, the property to be searched is a computer hard drive, the particularity requirement **[**43]** assumes even greater importance." *Id.* A general search of electronic data is an especially potent threat to privacy because hard drives and e-mail accounts may be "akin to a residence in terms of the scope and quantity of private information [they] may contain." *Id.* The "seizure of a computer hard drive, and its subsequent retention by the government, can [therefore] give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely

[30] Ulbricht's alternative argument, that the pen/trap orders violated the Pen/Trap Act and the Stored Communications Act ("SCA") because they sought prospective data, is without merit. Ulbricht claims that the orders were obtained both through the Pen/Trap Act, 18 U.S.C. §§ 3121-27, and the SCA, 18 U.S.C. § 2703(d). To the contrary, each pen/trap order (and the underlying requests for such orders) relied exclusively on the Pen/Trap Act, not the SCA. The fact that one of the government's goals was to monitor IP address traffic to match Ulbricht's Internet activity with DPR's does not undermine the validity of the orders. The orders themselves did not allow the government to track the location of the router and other equipment to which the trap and trace device was attached. Thus, they were not "geo-locating" devices, as Ulbricht suggests, any more than subpoenas for hotel registers, parking tickets, and credit card receipts, or any other methods by which the government obtains information that can be used to identify a suspect's location at particular points in time.

[31] **HN13**[↑] In addition to preventing general searches, the particularity requirement serves two other purposes not relevant to this appeal: "preventing the seizure of objects upon the mistaken assumption that they fall within the magistrate's authorization, and preventing the issuance of warrants without a substantial factual basis." United States v. Young, 745 F.2d 733, 759 (2d Cir. 1984).

irrelevant to the criminal investigation that led to the seizure." *United States v. Ganias, 824 F.3d 199, 217 (2d Cir. 2016)* (en banc). Such sensitive records might include "[t]ax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, [and] banking and shopping information." *Id. at 218*. Because of the nature of digital storage, it is not always feasible to "extract and segregate responsive data from non-responsive data," *id. at 213*, creating a "serious risk that every warrant for electronic information will become, in effect, a general warrant," *Galpin, 720 F.3d at 447* (internal quotation marks omitted). Thus, we have held that warrants that fail to "link [the evidence **[*100]** sought] to the criminal activity supported by probable **[**44]** cause" do not satisfy the particularity requirement because they "lack[] meaningful parameters on an otherwise limitless search" of a defendant's electronic media. *United States v. Rosa, 626 F.3d 56, 62 (2d Cir. 2010)*.

HN16[↑] The *Fourth Amendment* does not require a perfect description of the data to be searched and seized, however. Search warrants covering digital data may contain "some ambiguity . . . so long as law enforcement agents have done the best that could reasonably be expected under the circumstances, have acquired all the descriptive facts which a reasonable investigation could be expected to cover, and have insured that all those facts were included in the warrant." *Galpin, 720 F.3d at 446* (internal quotation marks omitted).

Moreover, it is important to bear in mind that ***HN17***[↑] a search warrant does not necessarily lack particularity simply because it is broad. Since a search of a computer is "akin to [a search of] a residence," *id.*, searches of computers may sometimes need to be as broad as searches of residences pursuant to warrants. Similarly, traditional searches for paper records, like searches for electronic records, have always entailed the exposure of records that are not the objects of the search to at least superficial examination in order to identify and seize those **[**45]** records that are. And in many cases, the volume of records properly subject to seizure because of their evidentiary value may be vast. None of these consequences necessarily turns a search warrant into a prohibited general warrant.

1. Laptop Search Warrant

The warrant authorizing the search and seizure of Ulbricht's laptop (the "Laptop Warrant") explicitly incorporated by reference an affidavit listing the crimes charged, which at the time included narcotics trafficking, computer hacking, money laundering, and murder-for-hire offenses in violation of *21 U.S.C. § 846*, *18 U.S.C. §§ 1030*, *1956*, and *1958*. *See 650 Fifth Ave. v. Alavi Found., 830 F.3d 66, 101 (2d Cir. 2016)* (describing the requirements for a criminal search warrant's incorporation of an affidavit by reference).[32] The affidavit also described the workings of Silk Road and the role of Dread Pirate Roberts in operating the site and included a wealth of information supporting a finding that there was probable cause to believe that Ulbricht and DPR were the same person. Based on that information, the Laptop Warrant alleged that Ulbricht "use[d] [the laptop] in connection with his operation of Silk Road," and that there was "probable cause to believe that evidence, fruits, and instrumentalities of the [charged offenses]" would be found on **[**46]** the laptop. S.A. 246.[33]

Generally speaking, the Laptop Warrant divided the information to be searched for and seized into two categories. The first covered evidence concerning Silk Road that was located on the computer, including, *inter alia*, "data associated with the Silk Road website, such as web content, server code, or database records"; any evidence concerning servers or computer equipment connected with Silk Road; e-mails, private messages, and forum postings or "other communications concerning Silk Road in any way"; evidence concerning "funds used to facilitate or proceeds **[*101]** derived from Silk Road," including Bitcoin wallet files and transactions with Bitcoin exchangers, or "information concerning any financial accounts . . . where Silk Road funds may be stored"; and "any evidence concerning any illegal activity associated with Silk Road." *Id.* at 246-48.

The second category of information in the Laptop Warrant included "evidence relevant to corroborating the identification of Ulbricht as the Silk Road user 'Dread Pirate Roberts.'" *Id.* at 248. In order to connect Ulbricht with DPR, the Laptop Warrant authorized agents to search for: "any communications or writings by Ulbricht, which may reflect linguistic **[**47]** patterns or idiosyncra[s]ies associated with 'Dread Pirate Roberts,' or political/economic views associated with [DPR] . . .";

---

[32] Because the warrant incorporated the affidavit by reference, we refer to the documents together as the Laptop Warrant for the sake of simplicity.

[33] Ulbricht does not challenge the existence of probable cause to believe both that he committed these offenses and that the laptop would contain evidence of them.

"any evidence concerning any computer equipment, software, or usernames used by Ulbricht, to allow comparison with" computer equipment used by DPR; "any evidence concerning Ulbricht's travel or patterns of movement, to allow comparison with patterns of online activity of [DPR]"; "any evidence concerning Ulbricht's technical expertise concerning Tor, Bitcoins," and other computer programming issues; any evidence concerning Ulbricht's attempts to "obtain fake identification documents," use aliases, or otherwise evade law enforcement; and "any other evidence implicating Ulbricht in the subject offenses." *Id.* at 248-49 (footnote omitted).

After careful consideration of the warrant, the supporting affidavit, and Ulbricht's arguments, we conclude that the Laptop Warrant did not violate the *Fourth Amendment's* particularity requirement.[34] We note, at the outset of our review, that the warrant plainly satisfies the basic elements of the particularity requirement as traditionally understood. By incorporating the affidavit by reference, the Laptop Warrant lists the charged crimes, describes the place to be searched, **[**48]** and designates the information to be seized in connection with the specified offenses. Each category of information sought is relevant to Silk Road, DPR's operation thereof, or identifying Ulbricht as DPR. We do not understand Ulbricht's arguments to contest the Laptop Warrant's basic compliance with those requirements.[35]

Rather, Ulbricht's arguments turn on the special problems associated with searches of computers which, as we have acknowledged in prior cases, *Galpin, 720 F.3d at 447*; *Ganias, 824 F.3d at 217-18*, can be particularly intrusive. These arguments merit careful attention. For example, Ulbricht questions the appropriateness of the protocols that the Laptop Warrant instructed officers to use in executing the search. Those procedures included opening or "cursorily reading the first few" pages of files to "determine their precise contents," searching for deliberately hidden files, using "key word searches through all electronic storage areas," and reviewing **[*102]** file "directories" to determine what was relevant. S.A. 253. Ulbricht, supported by *amicus* the National Association of Criminal Defense Lawyers ("NACDL"), argues that the warrant was insufficiently particular because the government and the magistrate judge failed to specify **[**49]** the search terms and protocols *ex ante* in the warrant.

We cannot agree. As illustrated by the facts of this very case, it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes. Files and documents can easily be given misleading or coded names, and words that might be expected to occur in pertinent documents can be encrypted; even very simple codes can defeat a pre-planned word search. For example, at least one of the folders on Ulbricht's computer had a name with the misspelling "aliaces." App'x 309. For a more challenging example, Ulbricht also kept records of certain Tor chats in a file on his laptop that was labeled "mbsobzvkhwx4hmjt." *Id.* at 398.[36]

The agents reasonably anticipated that they would face such problems in this case. Operating Silk Road involved using sophisticated technology to mask its users' identities. Accordingly, although we acknowledge the NACDL's suggestions in its *amicus* submission for limiting the scope of such search terms, the absence of the proposed limitations **[**50]** does not violate the particularity requirement on the facts of this case. We therefore conclude that, in preparing the Laptop

---

[34] The district court ruled that Ulbricht did not have standing to raise his *Fourth Amendment* challenges because he did not establish that he had a personal expectation of privacy in the laptop or his Facebook and Google accounts. We express no view on that issue, since the district court also reached the merits of the motion to suppress and the government has agreed that Ulbricht has standing to challenge the warrants and accompanying searches.

[35] It is worth noting that Ulbricht does not challenge the validity of the search warrant covering his home, although that warrant is quite similar to the Laptop Warrant and appears to be just as broad. Specifically, the home search warrant allows the government to search for and seize evidence concerning Ulbricht's travel or patterns of movement and any of his communications or writings.

[36] We note that Ulbricht and *amicus* NACDL somewhat exaggerate the novelty of computer searches in this regard. A traditional physical search for paper "drug records" or "tax records" may entail a similar examination of all sorts of files and papers to determine whether such records are hidden in files with innocuous or misleading names or written in coded terms to mask their content. For obvious reasons, search warrants authorizing the seizure of such evidence have not traditionally specified that agents may look only at file folders labeled "drug records" or may seize only papers containing the word "cocaine"—the equivalent of the *ex ante* "search terms" demanded by Ulbricht.

Warrant, "law enforcement agents [did] the best that could reasonably be expected under the circumstances, [had] acquired all the descriptive facts which a reasonable investigation could be expected to cover, and [had] insured that all those facts were included in the warrant." *Galpin, 720 F.3d at 446* (internal quotation marks omitted).

The fundamental flaw in Ulbricht's (and the NACDL's) argument is that it confuses a warrant's breadth with a lack of particularity. As noted above, ***HN18***[⬆] breadth and particularity are related but distinct concepts. A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement. For example, a warrant may allow the government to search a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence. Similarly, "[w]hen the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad **[**51]** language used in warrants will not offend the particularity requirements." *U.S. Postal Serv. v. C.E.C. Servs., 869 F.2d 184, 187 (2d Cir. 1989)*. Ulbricht used his laptop to commit the charged offenses by creating and continuing to operate Silk Road. Thus, a broad warrant allowing the government to search his laptop for potentially extensive evidence of those crimes does not offend the *Fourth Amendment*, as long as that **[*103]** warrant meets the three particularity criteria outlined above.

It is also true that allowing law enforcement to search his writings for linguistic similarities with DPR authorizes a broad search of written materials on Ulbricht's hard drive. That fact, however, does not mean that the warrants violated the *Fourth Amendment*. The Laptop Warrant clearly explained that the government planned to compare Ulbricht's writings to DPR's posts to confirm that they were the same person, by identifying both linguistic patterns and distinctive shared political or economic views. Ulbricht and the NACDL similarly claim that searching for all evidence of his travel patterns and movement violates the *Fourth Amendment's* particularity requirement. Again, the warrant explained that it sought information about Ulbricht's travel "to allow comparison with patterns of online activity of 'Dread Pirate Roberts' **[**52]** and any information known about his location at particular times." S.A. 248. Thus, the Laptop Warrant connects the information sought to the crimes charged and, more specifically, its relevance to identifying Ulbricht as the perpetrator of those crimes.[37]

We remain sensitive to the difficulties associated with preserving a criminal defendant's privacy while searching through his electronic data and computer hard drives. In the course of searching for information related to Silk Road and DPR, the government may indeed have come across personal documents that were unrelated to Ulbricht's crimes. Such ***HN19***[⬆] an invasion of a criminal defendant's privacy is inevitable, however, in almost any warranted search because in "searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized." *Ganias, 824 F.3d at 211*, quoting *Andresen, 427 U.S. at 482 n.11*. The *Fourth Amendment* limits such "unwarranted intrusions upon privacy," *id.* (internal quotation marks omitted), by requiring a warrant to describe its scope with particularity. The Laptop Warrant satisfied that requirement. Ulbricht has challenged only the facial validity of the Laptop Warrant **[**53]** and not its execution. Because we have no reason to doubt that the officers faithfully executed the warrant, its execution did not result in an undue invasion of Ulbricht's privacy.

Finally, we note that the crimes charged in this case were somewhat unusual. This case does not involve a more typical situation in which officers searched for evidence of a physician's illegal distribution of pain medications, to use the NACDL's example, which may have electronically-stored data associated with the alleged crimes on a hard drive that largely contains non-

---

[37] Evidence revealing a suspect's past movements is often highly relevant to a criminal investigation. Such evidence might be used to establish—or rule out—the suspect's presence at a crime scene or other pertinent location at a particular time. It may also disclose other, unrelated information about the suspect's non-criminal associations, interests, and behavior, and may be drawn from a wide variety of sources. Government efforts to develop such information, including by search warrants authorizing its seizure, are not inherently questionable under the *Fourth Amendment*. Using piecemeal or laborious investigative techniques, it might take law enforcement officers a great deal of time and effort to compile a comprehensive record of a suspect's travel or other movements. The fact that extensive travel records are stored on a digital device and may be accessed readily via a keystroke or quick search does not immunize those records from seizure. Indeed, the seizure of a paper journal or calendar in a conventional search will often allow officers to map out a defendant's travel history with similar ease.

criminal information. Here the crimes under investigation were committed largely **[*104]** through computers that there was probable cause to believe included the laptop at issue, and the search warrant application gave ample basis for the issuing magistrate judge to conclude that evidence related to Silk Road and Ulbricht's use of the DPR username likely permeated Ulbricht's computer. Thus, given the nature of Ulbricht's crimes and their symbiotic connection to his digital devices, we decline to rethink the well-settled *Fourth Amendment* principles that the Laptop Warrant may implicate. A future case may require this Court to articulate special limitations on digital **[**54]** searches to effectuate the *Fourth Amendment's* particularity or reasonableness requirements. Such a case is not before us.

2. The Google and Facebook Warrants

Ulbricht also challenges the warrants that allowed the government to search his Google and Facebook accounts, although he does not present any specific arguments related to those warrants. Both warrants, through affidavits incorporated by reference, set forth the basis for probable cause to search those accounts for evidence of Ulbricht's involvement in Silk Road. The warrants also authorized the government to search his Google and Facebook accounts for "evidence, fruits, and instrumentalities" of the specified offenses, including, *inter alia*: "any communications or writings by Ulbricht"; "any evidence concerning any computer equipment, software, or usernames used by Ulbricht"; "any evidence concerning Ulbricht's travel or patterns of movement"; and any "other evidence of the" crimes charged. S.A. 334-35, 393-94. The scope of the Google and Facebook warrants thus substantially paralleled that of the Laptop Warrant.

The Google and Facebook warrants were constitutional for the same reasons that the Laptop Warrant was valid. They satisfied all three **[**55]** of the particularity requirements because they listed the subject offenses, described the things to be searched, and identified the information to be seized in relation to the charged crimes. Ulbricht does not advance any additional arguments specific to the Google and Facebook warrants, nor have we identified any independent reason to find them unconstitutionally lacking in specificity.

3. Conclusion

In sum, the issuance of the pen/trap orders and the three search warrants that Ulbricht challenges in this appeal did not violate the *Fourth Amendment*.[38] Thus, we affirm the district court's denial of Ulbricht's suppression motion.

II. The District Court's Trial Rulings and Ulbricht's *Rule 33* Motion

Ulbricht contends that he did not receive a fair trial for several reasons: (1) the district court's rulings surrounding corrupt agents Force and Bridges violated his due process rights; (2) the district court erroneously precluded two defense experts from testifying; (3) the district court abused its discretion when it curtailed Ulbricht's cross-examination of two government witnesses; and (4) the district court erred when it ruled that certain hearsay statements were inadmissible. He also contends that, even if each **[**56]** individual error is harmless, the cumulative effect of those **[*105]** errors prejudiced him to the extent that his trial was fundamentally unfair. We detect no error in the district court's rulings on any of those issues and therefore conclude that Ulbricht was not deprived of his right to a fair trial.

A. Corrupt Agents Force and Bridges

Ulbricht's principal fair trial argument is that the district court erred in numerous ways by preventing him from relying on information related to the corruption of two federal agents, Force and Bridges, involved in the investigation of the Silk Road site. Before trial, the district court (1) precluded Ulbricht from referring at trial to the secret grand jury proceeding against Force; (2) denied Ulbricht discovery related to the Force investigation; and (3) denied Ulbricht an adjournment of the trial until the Force investigation was complete. During trial, the district court excluded as hearsay certain chats that related to Force's illicit use of Silk Road. Finally, Ulbricht learned after trial that the government was investigating a second corrupt agent, Bridges. Ulbricht contends that the failure to disclose

[38] The government also contends that, even if the warrants were invalid, the good faith exception prevents the application of the exclusionary rule. In general, *HN20*[↑] the "exclusion of evidence is inappropriate when the government acts in objectively reasonable reliance on a search warrant, even when the warrant is subsequently invalidated." *Ganias, 824 F.3d at 221* (internal quotation marks omitted). Because we conclude that all three of the warrants were valid, we need not address the government's alternative argument.

Bridges's corruption until after the trial violated **[**57]** *Brady v. Maryland, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963)*, and that the district court erroneously denied his motion for a new trial on that ground.

Without question, the shocking personal corruption of these two government agents disgraced the agencies for which they worked and embarrassed the many honorable men and women working in those agencies to investigate serious criminal wrongdoing. Even more importantly, when law enforcement officers abuse their offices for personal gain, commit other criminal acts, violate the rights of citizens, or lie under oath, they undermine the public's vital trust in the integrity of law enforcement. They may also compromise the investigations and prosecutions on which they work.

At the same time, the venality of individual agents does not necessarily affect the reliability of the government's evidence in a particular case or become relevant to the adjudication of every case in which the agents participated. Courts are obligated to ensure that probative evidence is disclosed to the defense, carefully evaluated by the court for its materiality to the case, and submitted for the jury's consideration where admissible. But courts must also take care that wrongdoing by investigators that has no bearing on the **[**58]** matter before the court not be used as a diversion from fairly assessing the prosecution's case. Like any other potential evidence, information about police corruption must be evaluated by reference to the ordinary rules of criminal procedure and evidence, a task to which we now turn.

1. Background: Pretrial Disclosure of the Force Investigation

The government disclosed its investigation into Force's corruption to the defense about six weeks before trial. Initially, on November 21, 2014, the government wrote a sealed *ex parte* letter to the district court seeking permission to disclose to the defense information about the Force grand jury investigation subject to a protective order.[39] The district court granted the application. On December 1, the government provided a copy of the November 21 letter, which otherwise remained sealed, to defense **[*106]** counsel. According to the letter, Force leaked information to DPR in exchange for payment and "corruptly obtain[ed] proceeds from the Silk Road website and convert[ed] them to his personal use."App'x 649. The government then undertook to purge its trial evidence of anything arguably traceable to Force.

Ulbricht moved to unseal the entire November 21 letter so that he could **[**59]** rely on the information in the letter that related to Force's corruption at trial, arguing that the letter included *Brady* information and that he therefore had a particularized need to disclose the information that outweighed the presumption of grand jury secrecy. He also requested discovery and subpoenas under *Rules 16* and *17, Fed. R. Crim. P.*, to learn more about the scope of Force's corruption. In the alternative, Ulbricht sought an adjournment of the trial until the Force investigation concluded and information about his corruption might become public through the filing of charges against him. On December 15, the district court held a sealed hearing on that issue and invited further written submissions, including a particularized list of Ulbricht's discovery requests. One week later, the district court issued a sealed and partially redacted opinion[40] denying all of Ulbricht's requests. The court did indicate, however, that throughout the trial it would "entertain specific requests to use information from the November 21, 2014 Letter on cross-examination." App'x 700. Moreover, the court explained that it would "entertain a renewed application" for a "particularized disclosure" of facts relevant to Force's corruption **[**60]** if the government's trial tactics or evidence "open[ed] the door" to such facts. *Id.*

2. Preclusion of Force Investigation Evidence: *Rule 6(e)*

On appeal, Ulbricht claims that the district court erred in denying his motion to unseal the November 21 letter because he demonstrated a particularized need that rebutted the presumption of secrecy that attaches to grand jury investigations. We disagree.

HN22[↑] "[T]he proper functioning of our grand jury system depends upon the secrecy of grand jury

[39] The government required such an order because *HN21*[↑] grand jury proceedings are secret and a government attorney "must not disclose a matter occurring before the grand jury," *Rule 6(e)(2)(B)(vi), Fed. R. Crim. P.*, without a court order, *Rule 6(e)(3)(E)*, subject to limited exceptions not relevant here.

[40] Portions of the district court opinion were redacted because they referenced the defendant's *ex parte* submissions explaining how he would use information related to the Force investigation at trial. This Court has reviewed an unredacted version of the district court opinion in connection with this appeal, but not the *ex parte* letters that the opinion references.

proceedings." *Douglas Oil Co. of California v. Petrol Stops Nw., 441 U.S. 211, 218, 99 S. Ct. 1667, 60 L. Ed. 2d 156 (1979)*. We have described five rationales for such secrecy:

> (1) To prevent the escape of those whose indictment may be contemplated; (2) to insure the utmost freedom to the grand jury in its deliberations, and to prevent persons subject to indictment or their friends from importuning the grand jurors; (3) to prevent subornation of perjury or tampering with the witnesses who may testify before the grand jury and later appear at the trial of those indicted by it; (4) to encourage free and untrammeled disclosures by persons who have information with respect to the commission of crimes; (5) to protect the innocent accused who is exonerated from disclosure of the fact that he has been under investigation, and **[**61]** from the expense of standing trial where there was no probability of guilt.

In re Grand Jury Subpoena, 103 F.3d 234, 237 (2d Cir. 1996). ***HN23***[] *Rule 6(e)(6) of the Federal Rules of Criminal Procedure* implements this policy of secrecy by requiring **[*107]** that "all records, orders, and subpoenas *relating to* grand jury proceedings [must] be sealed." *In re Grand Jury Subpoena, 103 F.3d at 237* (emphasis in original).

HN24[] Information falling within *Rule 6(e)*'s protections is entitled to a "presumption of secrecy and closure." *Id. at 239*. To rebut the presumption of secrecy, the party "seeking disclosure [must] show a particularized need that outweighs the need for secrecy." *Id.* (internal quotation marks omitted). To prove a particularized need, parties seeking disclosure must show that the "material they seek is needed to avoid a possible injustice in another judicial proceeding, that the need for disclosure is greater than the need for continued secrecy, and that their request is structured to cover only material so needed." *Id.* (internal quotation marks omitted). "A district court's decision as to whether the burden of showing a particularized interest has been met will be overturned only if the court has abused its discretion." *Id.*

We cannot say that the district court abused its discretion when it denied Ulbricht's request to unseal the November 21 letter discussing the Force **[**62]** grand jury investigation. It is undisputed that the letter contained information related to a grand jury proceeding that, if made public, would disclose matters occurring before the grand jury. Ulbricht did not demonstrate a particularized need for disclosure because he did not show that the need for disclosure was greater than the need for continued secrecy or that a possible injustice would result if the grand jury investigation was not disclosed. Specifically, the district court did not err in concluding that revealing the entire letter could have compromised the Force grand jury investigation in a number of ways. For example, potential co-conspirators might have learned of the investigation and attempted to intimidate witnesses or destroy evidence. The investigation was also likely to garner significant media attention, a fact that might influence witnesses or grand jurors. And, although Force knew of the investigation, revealing its existence to the public might have harmed him if the allegations had ultimately proved untrue. Finally, Ulbricht's request was not structured to cover only the information needed to avoid any possible injustice; instead, he sought to unseal the entire **[**63]** November 21 letter and did not propose a more narrowly tailored disclosure.

In redacted portions of its opinion, the district court also considered *ex parte* arguments concerning how the Force investigation might be relevant to Ulbricht's defense. In general terms, Ulbricht argued that the agents' corruption was critical to his defense because it would reveal the agents' ability to falsify evidence against him and demonstrate their motive to do so. According to the district court's characterization of his *ex parte* letters, Ulbricht speculated that Force may have used Curtis Green's (Flush) administrative capabilities to impersonate DPR; Force's corrupt conduct might have demonstrated technical vulnerabilities in the site that would render it susceptible to hacking; and learning that Force had good information about the Silk Road investigation might have caused the true DPR to recruit Ulbricht as his successor.[41]

---

[41] As noted above, *see* note 5, we have carefully considered to what extent it is appropriate to refer to portions of the record that remain under seal. We have been especially careful in describing the portions of the district court's opinion that remain redacted and therefore are still not available to the government or to the public. We appreciate that charges against Ulbricht remain pending in Maryland and that the redacted information describes what would have been his trial strategy had he been able to reference Force's corruption. We have thus described the defense's redacted arguments at a fairly high level of generality. We are confident that any experienced prosecutor could anticipate those arguments, and that in any event the information is largely stated or implied in Ulbricht's own publicly filed briefs on appeal. Particularly given

[*108] The district court reasoned that much of the information that might have arguably supported any of those theories was made available to the defense in discovery. The only new information in the November 21 letter concerned the investigation of Force's corruption; the fact of **[**64]** that investigation and its scope does not bolster any of the defense theories that Ulbricht described before the district court or on appeal. That Force was personally corrupt and used his undercover identity to steal money from Silk Road and DPR does not suggest either a motive or an ability on his part to frame Ulbricht as DPR. Absent any explanation of how Force could have orchestrated a massive plant of incriminating information on Ulbricht's personal laptop, his larcenous behavior does not advance the claim that such a frame-up was possible beyond mere speculation. Thus, Ulbricht was equally capable of presenting his various defense theories to the jury with or without the November 21 letter.[42]

The government's commitment to eliminating all evidence that came from Force's work on the Silk Road investigation[43] further undermines Ulbricht's claim that he needed the information to avoid a possible injustice. Had Force been called as a government witness, or had any of the government's evidence relied on his credibility, his character for truthfulness would have been at issue during the trial, and information that impeached his credibility would have become highly relevant. Ulbricht's **[**65]** reliance on the general fact of cooperation among different government agencies and different U.S. Attorney's Offices does not undermine the government's explicit representations that none of the evidence presented at trial derived from Force, and nothing in the record suggests that those representations were false. Ulbricht had no need to rely on the grand jury investigation of Force to attack the credibility of the actual government witnesses or the integrity of its other evidence.

In sum, Ulbricht has not shown that the district court abused its discretion in maintaining the secrecy of the Force grand jury investigation. He did not demonstrate to the district court, and has not demonstrated on appeal, that keeping the November 21 letter under seal resulted in any injustice, or that his need for disclosing the investigation was greater than the need for continued secrecy.[44]

[*109] 3. Denial of Discovery Related to Force

Ulbricht claims that the district court erred in denying him discovery, including requested subpoenas, related to the Force investigation. ***HN25***[↑] *Rule 16(a)(1)(E), Fed. R. Crim. P.*, requires the government to disclose information within its control if the information is "material to preparing the defense" or will be **[**66]** a part of the government's case-in-chief. Evidence is material if it "could be used to counter the government's case or to bolster a defense." *United States v. Stevens, 985 F.2d 1175, 1180 (2d Cir. 1993)*. "An appellate court, in assessing the materiality of withheld information, considers not only the logical relationship between the information and the issues in the case, but also the importance of the information in light of the evidence as a whole." *Id.* To justify a new trial, there "must be some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor." *Id.* (internal quotation marks omitted).

HN26[↑] *Rule 17(c), Fed. R. Crim. P.*, allows parties to subpoena documents and objects to be introduced at criminal trials. A subpoena must meet three criteria: "(1) relevancy; (2) admissibility; [and] (3) specificity." *United*

---

that our description relates to how the Force information might have been used at a trial that is now completed, and that we now hold that Ulbricht is not entitled to a new trial, we conclude that the public's need to understand and evaluate Ulbricht's arguments that he was unfairly prejudiced by the district court's rulings, as well as our reasons for rejecting those arguments, outweighs any minimal interest that Ulbricht might have in withholding his contentions from the government.

[42] Even on appeal, moreover, after the disclosure of additional information in the prosecutions of Bridges and Force, Ulbricht does not provide any concrete explanation of how the techniques used by the corrupt agents to steal money from Silk Road could have been used, by them or by others, to plant the massive amounts of incriminating information found on Ulbricht's laptop and in his house.

[43] For example, the government declined to present evidence of DPR's attempt to commission an additional murder because that conduct involved Force acting as Nob.

[44] Moreover, the district court specifically ruled that it would entertain Ulbricht's applications to rely on specific parts of the letter at trial if doing so would be necessary for effective cross-examination. Thus, Ulbricht was given the opportunity to show particularized need in the context of specific trial evidence. Ulbricht has not identified any point in the trial where he attempted to show that Force's behavior had become relevant to challenging the credibility of particular aspects of the prosecution's case.

States v. Nixon, 418 U.S. 683, 700, 94 S. Ct. 3090, 41 L. Ed. 2d 1039 (1974). The party requesting the subpoena must also show that the information sought is "not otherwise procurable reasonably in advance of trial by exercise of due diligence," that "the party cannot properly prepare for trial without such production," and that "the application is made in good faith and is not intended as a general 'fishing expedition.'" Id. at 699-700. HN27[↑] We review the district **[**67]** court's discovery rulings for abuse of discretion. United States v. Rigas, 583 F.3d 108, 125 (2d Cir. 2009).

The district court did not abuse its discretion when it denied Ulbricht's discovery requests related to the Force investigation. Ulbricht submitted 28 individual discovery requests in connection with the Force disclosure. Those ranged from the reasonably specific, such as "records from any and all Bitcoin accounts" used by Force, to the very broad, such as "any spending, net worth, or other financial analysis conducted with respect to former SA Force," "any and all phone records relating to former SA Force," and "bank account records from any and all bank accounts maintained by former SA Force or his spouse." App'x 669-70. The district court concluded that those requests were too broad and unfocused, and that the information requested was not material in the Rule 16 sense because the defense "has not articulated a coherent and particular reason why" the Force investigation could "counter the government's case or bolster a defense." *Id.* at 697. Next, the district court concluded that the Rule 17 subpoenas were part of the same overall fishing expedition and that the issuance of such subpoenas could compromise the Force grand jury investigation.

There was no **[**68]** abuse of discretion in those rulings. Ulbricht has not shown that, had the government produced every piece of requested information, he would have been able to alter the quantum of proof in his favor at trial. That is so because there is no indication, beyond Ulbricht's speculation, that Force manufactured any of the **[*110]** evidence on which the government relied at trial, let alone the most damning evidence discovered on the hard drive on Ulbricht's laptop and at his apartment. Because Force did not testify at trial, information related to his corruption would not have been relevant to attack the credibility of any testimony he would have given. Moreover, Ulbricht has not identified any specific aspect of the trial evidence that he could have undermined using the requested information. Thus, even if the district court erred in not granting at least some of Ulbricht's discovery requests, any such error does not justify a new trial.

4. Ulbricht's Motion to Adjourn the Trial

Ulbricht contends that the district court erred in denying his request to adjourn the trial until the Force investigation was complete. HN28[↑] "[A] district court has a great deal of latitude in scheduling trials." United States v. Griffiths, 750 F.3d 237, 241 (2d Cir. 2014) (internal quotation **[**69]** marks omitted). Thus, "trial courts enjoy very broad discretion in granting or denying trial continuances." United States v. Stringer, 730 F.3d 120, 127 (2d Cir. 2013). A decision to grant or deny a request for an adjournment is reviewed for abuse of discretion, and we "will find no such abuse unless the denial was an arbitrary action that substantially impaired the defense." *Id.* (internal quotation marks omitted). Thus, the party seeking a continuance has the burden of showing "both arbitrariness and prejudice in order to obtain reversal" based on a denial of an adjournment. Id. at 128 (internal quotation marks omitted).

The district court did not abuse its discretion in denying Ulbricht's request for an adjournment of the trial. In a sealed portion of the proceedings on the first day of trial, the district court explained its reasons for denying the adjournment. The court ruled that because none of the evidence revealed by the government concerning Force's corruption was exculpatory, there was no reason to believe that delaying the trial would assist Ulbricht's defense. That analysis was not irrational or arbitrary. Moreover, as explained in more detail both above and below, Ulbricht has not shown how information related to Force's corruption was either **[**70]** exculpatory or material to his defense. Thus, he has not shown that the district court's refusal to adjourn the trial was prejudicial, let alone substantially so.

5. Preclusion of the DeathFromAbove Chats

As already described, Force used DeathFromAbove as an unauthorized Silk Road username through which he attempted to extort money from DPR. The government only learned of Force's activity as DeathFromAbove during trial, when the defense attempted to introduce a redacted chat between DPR and DeathFromAbove. In the chat at issue, DeathFromAbove implied that he knew that DPR's real identity was Anand Athavale. DeathFromAbove then attempted to blackmail DPR by saying that, if DPR gave him $250,000, he would not "give you [*sic*] identity to law enforcement." App'x 712.

The government objected to admitting the chat on three

grounds: (1) it was hearsay; (2) its probative value was substantially outweighed by unfair prejudice under Rule 403, Fed. R. Evid.; and (3) it was a "back-door attempt to re-inject" Force's corruption into the defense's trial evidence. App'x 707. The district court excluded the chat as hearsay. At trial, Ulbricht claimed that the chat was not being offered for its truth, but instead to show its **[**71]** effect on DPR; that is, if DPR was actually Athavale, one would expect DPR to take certain steps to protect his identity. The district **[*111]** court disagreed and ruled that the DeathFromAbove chat was hearsay because it was offered for the truth of the matter asserted therein—that government agents at one time thought that Athavale was DPR—and it did not fall into any hearsay exceptions. In the alternative, the district court found that the Athavale-as-DPR theory lacked sufficient support, was speculative, and risked jury confusion.

In general, HN29[] hearsay is not admissible unless an exception applies. *See* Fed. R. Evid. 802. "The Federal Rules of Evidence define hearsay as a declarant's out-of-court statement offered in evidence to prove the truth of the matter asserted in the statement." United States v. Dupree, 706 F.3d 131, 136 (2d Cir. 2013) (internal quotation marks and alterations omitted). If "the significance of an offered statement lies solely in the fact that it was made, no issue is raised as to the truth of anything asserted, and the statement is not hearsay." *Id.* (internal quotation marks omitted). HN30[] "The trial court's ultimate decisions as to the admission or exclusion of evidence are reviewed for abuse of discretion." Davis v. Velez, 797 F.3d 192, 201 (2d Cir. 2015).

The district court concluded that **[**72]** the DeathFromAbove chat was hearsay because it was an out-of-court statement being offered for the truth of the matter asserted therein. That ruling was not an abuse of discretion. Contrary to Ulbricht's assertions on appeal, the district court did not rest its decision on the need for grand jury secrecy to protect the Force investigation. Instead, the decision was a straightforward application of the rule against hearsay.

Ulbricht does not provide any detailed arguments to the contrary that are specific to the DeathFromAbove chat; instead, he discusses the district court's preclusion of all of the evidence related to the Force investigation collectively. At trial, however, he claimed that the statement was offered only to demonstrate "the fact that it was communicated to DPR . . . in that this particular piece of evidence communicates to DPR the name and profile of the person [D]eath[F]rom[A]bove believes is DPR." Tr. 1866. Ulbricht claimed that the statement was "offered for the fact that DPR was getting information about people who were supposed to be DPR," and "one of these people is [Athavale]." *Id.* at 1867. Once the district court expressed skepticism about his argument, Ulbricht claimed that he sought to admit **[**73]** the chat to demonstrate its effect on DPR: "if you're DPR and you get a name . . . this Anand Athavale and a profile and details . . . and you're put on notice that it's you, you're going to take steps." *Id.* at 1867-68. In other words, Ulbricht claimed that he did not offer it for the truth of the matter asserted in the chat: that agents in the Baltimore investigation, including Force, believed that Athavale was the real Dread Pirate Roberts, or that Athavale was in fact the real DPR.

Ulbricht's proposed non-hearsay use of the chat—to show its effect on DPR—is not sufficiently probative that the evidence's exclusion prejudiced him. The statement does not appear to have had an effect on DPR that would bolster Ulbricht's defense. DPR did not alter his behavior in response to the extortion attempt. Indeed, he referred to it as "bogus" in one of the journal entries discovered on Ulbricht's laptop. App'x 710. If Athavale had been the real Dread Pirate Roberts, he likely would have had a different reaction to the threatened exposure of his identity. DPR's reactions to other attempts to destroy the site's anonymity were dramatic, and included hiring people to kill the users who threatened to compromise **[**74]** Silk Road. Therefore, even if Ulbricht did not **[*112]** offer the chat for its truth, any relevance of the arguably non-hearsay use of the statement was entirely too remote to outweigh the possible jury confusion that would result from the injection of Force into the trial or the likelihood that the jury would confuse the hearsay and non-hearsay significance of the evidence.

6. Ulbricht's *Rule 33* Motion: *Brady v. Maryland*

Ulbricht moved for a new trial under Rule 33, Fed. R. Crim. P., raising several issues concerning the unfairness of the assertedly belated disclosures of the investigations into Force and Bridges.[45] The only argument that he pursues in this appeal is that the belated disclosures violated his due process rights

[45] Ulbricht filed his *Rule 33* motion on March 6, 2015. The criminal complaint against Force and Bridges was unsealed on March 30, which is the first time that Ulbricht learned that Bridges was corrupt and was involved in the case.

under *Brady* because the information was both material and exculpatory.

HN31[] Rule 33(a) provides that, on "the defendant's motion, the court may vacate any judgment and grant a new trial if the interest of justice so requires." We have advised district courts to "exercise Rule 33 authority sparingly and in the most extraordinary circumstances." United States v. Coté, 544 F.3d 88, 101 (2d Cir. 2008) (internal quotation marks omitted). "Where a defendant's *Brady* claim was raised in a motion for a new trial pursuant to Rule 33[,] . . . we review the denial of the motion for abuse of discretion." **[**75]** United States v. Douglas, 525 F.3d 225, 245 (2d Cir. 2008) (internal quotation marks omitted). In the context of denying a Rule 33 motion, a "district court abuses . . . the discretion accorded to it when (1) its decision rests on an error of law . . . or a clearly erroneous factual finding, or (2) its decision—though not necessarily the product of a legal error or a clearly erroneous factual finding—cannot be located within the range of permissible decisions." United States v. Forbes, 790 F.3d 403, 406 (2d Cir. 2015) (internal quotation marks omitted).

HN32[] There are three components of a *Brady* violation: "(1) The evidence at issue must be favorable to the accused, either because it is exculpatory or because it is impeaching; (2) that evidence must have been suppressed by the [government], either willfully or inadvertently; and (3) prejudice must have ensued." United States v. Certified Envtl. Servs., Inc., 753 F.3d 72, 91 (2d Cir. 2014) (internal quotation marks omitted). Information is exculpatory if it relates to the defendant's guilt or innocence. United States v. Avellino, 136 F.3d 249, 255 (2d Cir. 1998). In order to show that he has been prejudiced, a defendant must demonstrate "a reasonable probability that, had the evidence been disclosed, the result of the proceeding would have been different, such that the failure to disclose undermines confidence in the verdict." Certified Envtl. Servs., Inc., 753 F.3d at 91 (internal quotation marks and alterations omitted). Thus, the prosecution **[**76]** "must disclose . . . exculpatory and impeachment information no later than the point at which a reasonable probability will exist that the outcome would have been different if an earlier disclosure had been made." Id. at 92 (internal quotation marks omitted). In general, a "prudent prosecutor will err on the side of transparency, resolving doubtful questions in favor of disclosure." Cone v. Bell, 556 U.S. 449, 470 n.15, 129 S. Ct. 1769, 173 L. Ed. 2d 701 (2009).

Although the agents' illegal behavior in connection with the Silk Road investigation is deeply troubling, the government's **[*113]** December 2014 disclosure of the Force investigation and the post-trial disclosure of Bridges's corruption did not violate Ulbricht's due process rights. Evidence concerning the agents' corruption is not *Brady* information because it is not exculpatory or impeaching of the government's trial evidence. For this reason, the government's failure to reveal the full extent of the investigations until after Ulbricht's trial did not prejudice him. As already explained, the fact that Force purloined Bitcoins from Silk Road and attempted to blackmail DPR does not relate to Ulbricht's guilt or innocence; the same logic applies to Bridges's similar behavior. The agents' corruption has nothing to do with **[**77]** whether Ulbricht operated the site as Dread Pirate Roberts. Ulbricht has not raised any credible doubts about the reliability of the evidence that the government presented at trial, nor has he explained why the agents' illegal actions relate to *his* guilt at all. Indeed, the government removed from its exhibit list the items relevant to Force, including communications between Nob (his authorized undercover username) and DPR. Those communications included an instance in which DPR hired Nob to kill Curtis Green (Flush) as punishment for using his administrator status to steal Bitcoins from Silk Road users. Ulbricht does not identify any particular evidence introduced by the government at trial that is traceable to either Force or Bridges, or the admissibility of which depends on either agent's integrity.

Ulbricht's arguments to the contrary largely rest on speculation. First, Ulbricht contends that the Silk Road investigations occurring in Baltimore and New York were "[c]oordinated and [c]ombined," suggesting that Force's corruption may have somehow infected the evidence that the New York office used in its prosecution. Appellant Br. 40. Ulbricht explains that the offices communicated frequently and shared information **[**78]** through emails and reports. Assuming that Ulbricht is correct, the fact that the Silk Road investigation took place in several offices, one of which employed two corrupt agents, does not alter our analysis. Ulbricht still has not shown how the agents' corrupt behavior is exculpatory as to him, even if Force and Bridges at times shared their work product with New York and that work product influenced the larger investigation. The relevant question, on which none of Ulbricht's arguments casts any light or raises any doubt, is whether any particular item of evidence was tainted in some way by the misconduct of Bridges or Force.

Next, Ulbricht surmises that the agents may have fabricated evidence suggesting that Ulbricht was DPR. In so arguing, Ulbricht implies that Force and Bridges may have had sufficiently high-level administrator access to Silk Road to manipulate the "financial, transactional, and communications infrastructure of the Silk Road site." Reply Br. 14. Nothing in the government's disclosures, and nothing that Ulbricht identifies in the record or has produced from any independent source, suggests that either Bridges or Force had such capacity. Absent further detail or evidence **[**79]** that Force and Bridges were able to infiltrate DPR's communications or transactions, Ulbricht's argument is simply too speculative to warrant a new trial. Ulbricht further claims that Bridges used sophisticated techniques to try to place blame on others for his corrupt conduct, reflecting a pattern of framing others for his own crimes. That fact alone does not suggest that Bridges fabricated any evidence against Ulbricht or attempted to frame him. That Bridges undertook to deflect blame for things *he* had done does not suggest any reason why Bridges would be motivated to frame Ulbricht for things that DPR had done. Nor does Ulbricht explain **[*114]** how Bridges's actions should undermine our confidence in any of the specific evidence on which the government relied at trial.[46]

Finally, Ulbricht submitted a supplemental appendix that included a newly-discovered, unredacted report from the Joint Automated Booking System ("JABS").[47] In that report, under the heading "Arrested or Received Information," Force is listed as the officer on the case, and the Baltimore DEA is listed as the relevant agency. Ulbricht apparently means to suggest that this report shows that Force played a more pervasive role in **[**80]** the investigation than the government has acknowledged. In response, the government argues that Force was simply the most recent person to make changes to the JABS report by updating it to include information about Ulbricht's family members and the pending charges in Maryland. In any event, the JABS report bearing Force's name does not show how information related to Force's corruption exculpates Ulbricht. It merely confirms that Force was a participant in the Baltimore Silk Road investigation and that he continued to be involved in the case after Ulbricht was arrested. In the face of the entire record of the trial, in which the provenance of the government's evidence was exhaustively displayed without indication that Force was responsible for any of it, this single report has little or no probative value.

In sum, we conclude that the Force and Bridges complaint did not contain *Brady* information because the agents' corruption does not bear on Ulbricht's guilt or innocence. Thus, any delay in the government's disclosure of their corruption did not violate Ulbricht's due process rights.

B. Preclusion of Defense Experts

The district court precluded both of Ulbricht's proposed expert witnesses **[**81]** from testifying because he did not timely or adequately disclose his intent to call them under Rule 16, Fed. R. Crim. P. **HN33**[↑] In general, the "defendant must, at the government's request, give to the government a written summary of any [expert] testimony that a defendant intends to use. . . . This summary must describe the witness's opinions, the bases and reasons for those opinions, and the witness's qualifications."[48] Fed. R. Crim. P. 16(b)(1)(C). The purpose of the expert disclosure requirement is to "minimize surprise that often results from unexpected expert testimony, reduce the need for continuances, and to provide the opponent with a fair opportunity to test the merit of the expert's testimony through focused cross-examination." Fed. R. Crim. P. 16, advisory committee's note to 1993 amendment. Indeed, "[w]ith increased use of both scientific and nonscientific expert testimony, one of counsel's most basic discovery needs is to learn that an expert is expected to testify." *Id.*

[*115] **HN34**[↑] If a party fails to comply with Rule 16, the district court has "broad discretion in fashioning a

[46] In a footnote, Ulbricht claims that failing to disclose the full extent of the agents' corruption deprived him of an opportunity to "attack[] the investigation as shoddy." Kyles v. Whitley, 514 U.S. 419, 442 n.13, 115 S. Ct. 1555, 131 L. Ed. 2d 490 (1995). Now that he has all of the relevant information, he still does not explain how he might have demonstrated deficiencies in the government's investigation of his or one of the other initial suspects' conduct that would undermine our confidence in the verdict.

[47] As the government explains, and Ulbricht does not dispute, JABS is a database maintained by the United States Marshals Service that catalogues information regarding alleged offenders who have been arrested and booked by federal, state, or local law enforcement agencies.

[48] It is undisputed that the government requested such disclosure on December 29, 2014, two weeks before trial began.

remedy," which may include granting a continuance or "ordering the exclusion of evidence." *United States v. Lee, 834 F.3d 145, 158 (2d Cir. 2016)* (internal quotation marks omitted); *see* *Fed. R. Crim. P. 16(d)(2)(A)-(D)* (a district court may order "any other [remedy] that is just under **[**82]** the circumstances"). We thus review the district court's choice of remedy for abuse of discretion. "In considering whether the district court abused its discretion, we look to the reasons why disclosure was not made, the extent of the prejudice, if any, to the opposing party, the feasibility of rectifying that prejudice by a continuance, and any other relevant circumstances." *Lee, 834 F.3d at 159* (internal quotation marks omitted).

The district court did not abuse its discretion in precluding the defense from calling its proposed experts. Not only were the disclosures late, more importantly, they were plainly inadequate. Both disclosures merely listed general and in some cases extremely broad topics on which the experts might opine. For example, the disclosures indicated that the experts would testify on general topics, including: "the origins of Bitcoin," "the various purposes and uses of Bitcoin," "the mechanics of Bitcoin transactions," "the value of Bitcoin over time since its inception," "the concepts of Bitcoin speculating and Bitcoin mining," "[g]eneral principles of internet security and vulnerabilities," the "import of some lines of PHP code provided to defense counsel in discovery," and "[g]eneral principles of **[**83]** public-key cryptography," among others. App'x 349, 360. They did not summarize the experts' opinions about those topics, let alone describe the bases for the experts' opinions.

Indeed, although the listed topics certainly pertained generally to Silk Road, the disclosures were so vague that it is difficult to discern whether the proffered expert testimony would have been at all relevant under *Rules 401* and *702(a), Fed. R. Evid.*[49] In his opposition to the government's motion to preclude Antonopoulos, Ulbricht described the expert's proposed testimony in more detail, but he still did not disclose the opinions that the expert intended to offer. For example, that supplemental disclosure indicated that an "[i]ndependent defense investigation has uncovered that" the government's claim that over 700,000 Bitcoins were transferred to Ulbricht's Bitcoin wallet "is implausible," and the expert would "dispute this finding." App'x 382. Although that is more specific, it is not a summary of Antonopoulos's opinion, nor does it identify the basis for that opinion. Thus, to this day Ulbricht has not described what opinions the experts would offer or explained the methods they used to arrive at any of those conclusions.

The district court also did **[**84]** not abuse its discretion in finding that the government would be prejudiced by the belated and inadequate disclosures, in part because the government was due to rest the following day, providing it with no time **[*116]** to prepare to respond to the experts. Moreover, the district court considered intermediate sanctions short of preclusion but found them to be inadequate. In rejecting a continuance as a possible remedy, the district court emphasized the "known issues with a continuance," especially in a lengthy trial. *Id.* at 369. Two of the jurors had time constraints, and a continuance might have caused the court to lose one or both of those jurors, especially if the continuance was lengthy. If it were to grant a continuance, the court would also need to perform its function as a gatekeeper of expert testimony under ***HN35***[↑] *Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592-93, 113 S. Ct. 2786, 125 L. Ed. 2d 469 (1993)*, which requires the district court to make a "preliminary assessment of whether the reasoning or methodology underlying the [expert] testimony is scientifically valid" and "can be applied to the facts in issue."[50] The district court cannot perform that complex

---

[49] In particular, Ulbricht's disclosures did not discuss, and he has not described on appeal, how one expert's proposed testimony on "[g]eneral principles of internet security and vulnerabilities" would have linked to the defense claim that the damning documentary evidence of Ulbricht's guilt found on his laptop was or could have been fabricated or planted. The jury was aware from other evidence, and indeed it is within ordinary lay experience, that various forms of hacking are possible. What was lacking, what the defense expert disclosures did not purport to address, and what Ulbricht still has not provided on appeal, is any explanation, let alone a credible explanation, of how the breadth and variety of information, from the laptop and other sources, could have been planted.

[50] We have explained that ***HN36***[↑] a *Daubert* reliability assessment requires a district court to consider the "extent to which [the expert's theory] has been subjected to peer review and publication," whether the technique is "subject to standards controlling the technique's operation," the "known or potential rate of error," and the "degree of acceptance within the relevant scientific community." *United States v. Romano, 794 F.3d 317, 330 (2d Cir. 2015)* (internal quotation marks omitted). That inquiry is a "flexible one," however, and *Daubert* is not a "definitive checklist or test" for the reliability of expert testimony. *Id.* (internal quotation marks omitted). Thus, "[w]hether *Daubert*'s specific factors are, or are not,

evaluation of an expert's proposed methodology without a clear articulation of what the expert's opinions are and, even more importantly, **[**85]** of the bases for those opinions. In light of the risk of losing jurors and the lack of a sufficiently compelling reason for the defense's clear violation of Rule 16, the district court was within its discretion when it determined that a continuance was not practical and that the appropriate remedy was to preclude the witnesses altogether.

Ulbricht's arguments to the contrary are not persuasive. First, Ulbricht argues that the two experts were necessary to rebut portions of the government's case that he was precluded from addressing during cross-examination, as well as the testimony of Ilhwan Yum, a government witness who analyzed transactions associated with Bitcoin wallets found on Ulbricht's laptop. Ulbricht now contends that portions of Yum's testimony were incorrect, including his description of what a "hot" Bitcoin wallet is.[51] Ulbricht does not, however, explain *how* Yum's testimony was incorrect, what contrary evidence his experts would have provided had they been allowed to testify, or how any purported correction of Yum's testimony would have affected the case against Ulbricht. Nor has he produced any summaries of his proposed expert testimony or described how **[**86]** that testimony would have been material to Ulbricht's guilt or innocence. In other words, Ulbricht has not shown that precluding Bellovin and Antonopoulos from testifying prejudiced him. Ulbricht's alternative argument that the **[*117]** disclosures were in fact adequate is incorrect for the reasons already explained.

Ulbricht next argues that preclusion was an unduly harsh remedy under the circumstances. Along those lines, he claims that certain exhibits, such as the summary chart on which Yum relied, were not produced until mid-trial. Thus, according to Ulbricht, he could not have known about his need for expert witnesses to counter specific trial exhibits until it was already too late to comply with Rule 16. In his view, the district court should not have held him so strictly to Rule 16's requirements because he could not have known until Yum testified that he would need to call an expert.

While Ulbricht is correct that excluding his experts was a harsh sanction and was not to be imposed lightly, the district court considered the possibility of granting a continuance or a more limited sanction and found those remedies **[**87]** to be inappropriate under the circumstances. Such HN37[↑] careful consideration of a range of possible sanctions short of preclusion is especially important in the atypical case where a criminal defendant, rather than the government, is precluded from putting on his case because of a Rule 16 violation. Limiting the defense's presentation of his case implicates the fundamental right of "an accused to present witnesses in his own defense." Chambers v. Mississippi, 410 U.S. 284, 302, 93 S. Ct. 1038, 35 L. Ed. 2d 297 (1973). However, the defendant must still "comply with established rules of procedure and evidence designed to assure both fairness and reliability in the ascertainment of guilt and innocence." *Id.* Here, Ulbricht did not comply with the procedural requirements associated with expert disclosures. The district court gave the issue due consideration and appropriately exercised its discretion in remedying the defense's Rule 16 violation.

Finally, Ulbricht cannot credibly argue that Yum's testimony was the first notice he had about the possible need for an expert witness to testify as part of his affirmative case. The Silk Road prosecution was uniquely laden with issues related to technology, computer servers, forensics, cyber security, digital currency, and myriad other issues that **[**88]** are indisputably "beyond the ken of the average juror." United States v. Mejia, 545 F.3d 179, 191 (2d Cir. 2008) (internal quotation marks omitted). Ulbricht surely knew from the outset that, in order to mount a meaningful attack on the government's voluminous and technically complex evidence, he would need to call his own expert. Indeed, in his opening statement, Ulbricht's counsel claimed that he would show that the Bitcoins in Ulbricht's wallet were from innocent transactions associated with Bitcoin speculation, rather than, as the government contended, related to Silk Road.[52]

---

reasonable measures of reliability in a particular case is a matter that the law grants the trial judge broad latitude to determine." Id. at 331 (internal quotation marks omitted).

[51] "The terms hot wallet and cold wallet derive from the more general terms hot storage, meaning online storage, and cold storage, meaning offline storage. A hot wallet is a Bitcoin wallet for which the private keys are stored on a network-connected machine (*i.e.*[,] in hot storage). By contrast, for a cold wallet the private keys are stored offline." Steven Goldfeder *et al., Securing Bitcoin Wallets via a New DSA/ECDSA Threshold Signature Scheme*, Princeton University 10, *available at* http://www.cs.princeton.edu/~stevenag/threshold_sigs.pdf .

[52] No evidence about the source of those Bitcoins was in fact presented by Ulbricht, and neither the expert disclosures

Ulbricht's opening statement also implied that BitTorrent's[53] security deficiencies could have allowed the true DPR to plant incriminating evidence on his laptop. It is difficult to fathom how he planned to advance those theories without relying on expert testimony.

[*118] In short, Ulbricht argues that the district court's preclusion of his proffered expert witnesses denied him a fair opportunity to present his defense. But the same failings that render Ulbricht's expert disclosures inadequate under *Rule 16* preclude us from finding the kind of prejudice he asserts. Ulbricht did not disclose to the district court, and has not presented **[**89]** on appeal, any explanation of what the proposed experts would have said that would have supported a nonspeculative basis for doubting the probative value of evidence from a variety of electronic and other sources identifying Ulbricht as DPR throughout the life of Silk Road. Thus, we cannot conclude that he was prejudiced by the experts' exclusion.

C. Curtailing Cross-Examination

Ulbricht contends that the district court erred in limiting his ability to cross-examine two government witnesses: Der-Yeghiayan and Kiernan. ***HN38***[↑] "We review a trial court's decision to limit the scope of cross-examination for abuse of discretion." *United States v. Cedeño, 644 F.3d 79, 81 (2d Cir. 2011)*. ***HN39***[↑] "A district court is accorded broad discretion in controlling the scope and extent of cross-examination." *United States v. James, 712 F.3d 79, 103 (2d Cir. 2013)* (internal quotation marks omitted); *see Fed. R. Evid. 611(a)*. Thus, "a district court may impose reasonable limits on cross-examination to protect against, *e.g.*, harassment, prejudice, confusion, and waste." *James, 712 F.3d at 103* (internal quotation marks omitted). In general, however, a "district court should afford wide latitude to a defendant in a criminal case to cross-examine government witnesses." *Id.* (internal quotation marks omitted). That is so because the *Confrontation Clause* gives "a defendant the right not only **[**90]** to cross-examination, but to effective cross-examination." *Id.* "[I]t does not follow, of course, that the *Confrontation Clause* prevents a trial judge from imposing *any* limits" on defense counsel's cross-examination of government witnesses. *Id.* (emphasis in original).

1. Agent Der-Yeghiayan

Ulbricht argues that the district court erred when it struck portions of Der-Yeghiayan's testimony that referenced his prior belief that Karpeles might be Dread Pirate Roberts. Ulbricht also challenges the striking of a similar but analytically distinct piece of testimony: Der-Yeghiayan's statement that Karpeles's attorney had offered information about Silk Road in exchange for Karpeles receiving immunity from prosecution. Ulbricht wanted the jury to infer that Karpeles had some criminal involvement in Silk Road that motivated him to pursue a cooperation agreement with the government.

Der-Yeghiayan answered the defendant's initial questions about those topics, and the government did not object to them until a later side bar. During the side bar, the district court expressed its initial view that the questions were proper, but requested written briefing on the subject. After reviewing the parties' submissions, the district **[**91]** court agreed with the government that neither Der-Yeghiayan's prior opinions about whether Karpeles was DPR nor Karpeles's offer of information about Silk Road was relevant to Ulbricht's case. The court thus directed the government to identify portions of Der-Yeghiayan's testimony to strike. After the government identified the improper testimony, the district court gave a general limiting instruction to the jury:

> You heard testimony while Mr. Der-Yeghiayan was on the stand regarding personal beliefs or suspicions he may have had about particular individuals at various points during his investigation. And I instruct you that what the agent suspected **[*119]** about others isn't evidence and should be disregarded. Now, consistent with all of the instructions I'm going to give you at the end of the case, there was other testimony that Mr. Der-Yeghiayan provided which you may consider during your deliberations and give it the weight that you deem that it deserves. So it's the suspicions, all right?

Tr. 974. Ulbricht contends on appeal that the district court erred in striking the testimony.

---

presented to the district court nor Ulbricht's arguments on appeal suggest that either Bellovin or Antonopoulos would have provided an analysis or explanation of Ulbricht's Bitcoin transactions that would have revealed a non-Silk Road source for Ulbricht's Bitcoins.

[53] BitTorrent is a peer-to-peer file sharing service that is used to transfer large files without disrupting Internet servers. It has both legitimate and illicit purposes. *See Next Phase Distribution, Inc. v. John Does 1-27, 284 F.R.D. 165, 167 (S.D.N.Y. 2012)*.

We disagree. The district court did not err in concluding that Der-Yeghiayan's prior beliefs about Karpeles as **[**92]** a possible DPR suspect were not relevant to the charges against Ulbricht. *HN40*[↑] In order to elicit testimony implicating an alternative perpetrator, a defendant "must show that his proffered evidence on the alleged alternative perpetrator is sufficient, on its own or in combination with other evidence in the record, to show a nexus between the crime charged and the asserted alternative perpetrator." *Wade v. Mantello, 333 F.3d 51, 61-62 (2d Cir. 2003)* (internal quotation marks omitted). Thus, to avoid a "grave risk of jury confusion," a defendant must offer more than "unsupported speculation that another person may have done the crime." *Id. at 62* (internal quotation marks omitted). An "agent's state of mind as the investigation progressed is ordinarily of little or no relevance to the question of the defendant['s] guilt." *United States v. Johnson, 529 F.3d 493, 501 (2d Cir. 2008)*. Thus, striking Der-Yeghiayan's testimony and instructing the jury to disregard his earlier opinions about Karpeles's possible guilt was not error.[54]

Further, any arguable error that occurred was harmless. Defense counsel continued to cross-examine Der-Yeghiayan and elicited admissible testimony about the earlier investigation into Karpeles; indeed, the district court took over cross-examination at several points to assist the defense **[**93]** in asking proper questions. *Cf. Cotto v. Herbert, 331 F.3d 217, 254 (2d Cir. 2003)* (in considering whether a *Confrontation Clause* violation is harmless, we consider, *inter alia*, "the extent of cross-examination otherwise permitted"). Moreover, Ulbricht discussed the investigation of Karpeles in his summation without objection. What was relevant at trial was any actual evidence pointing to Karpeles as the true Dread Pirate Roberts. The district court did not limit Ulbricht's cross-examination of Der-Yeghiayan as to his knowledge of such evidence. The district court directed the jury to disregard only testimony as to the agent's "suspicions," Tr. 974, a subject of "little or no relevance to . . . the defendant['s] guilt," *Johnson, 529 F.3d at 501*.

We similarly reject Ulbricht's contention that striking Der-Yeghiayan's testimony concerning Karpeles's offer to provide information about Silk Road in exchange for immunity was an abuse of discretion. Absent other evidence in the record regarding Karpeles, it was proper to exclude wholly speculative suggestions of an alternative perpetrator defense based on Karpeles's attorney's offer of information in exchange for his client's immunity. **[*120]** And even assuming, *arguendo*, that the district court erred in striking the testimony, any error **[**94]** was harmless. To the extent this testimony was stricken from the trial record, that ruling occurred outside the presence of the jury. All the jury was told was to disregard testimony about "what the agent suspected about others," Tr. 974, a category that hardly would be understood by the jury to encompass testimony about the actions of Karpeles's attorney. As explained in detail above, moreover, the evidence identifying Ulbricht as Dread Pirate Roberts was overwhelming and largely unchallenged. That Karpeles may have had information about Silk Road does not imply that he was DPR, only that he had some knowledge of or involvement with the site. Particularly given that Karpeles likely had some knowledge about Silk Road simply because of his operation of Mt. Gox, a prominent Bitcoin exchanger, any marginal probative value in the fact that he claimed to have such knowledge, and offered to provide it to the government, could not have meaningfully affected the balance of evidence available to the jury regarding the identity of DPR.

2. Agent Kiernan

Defense counsel cross-examined Kiernan extensively, and Ulbricht contends on appeal that the district court erred in preventing him from exploring **[**95]** certain topics during that cross-examination. Those excluded topics include: the meaning of various acronyms, the significance of a certain line of PHP code,[55] whether the FBI allowed Kiernan to run BitTorrent on his work computer despite its lack of security, and whether the Linux kernel[56] that Kiernan used on his work computer was the same as the one that Ulbricht installed on his laptop. Ulbricht explains that he was attempting to show

[54] Ulbricht also contends on appeal that the government's objection to the testimony, which occurred at a later sidebar, was untimely. He cites no law in support of that argument. In general, *HN41*[↑] an "objection should be made after the question has been asked but before an answer has been given." *Hutchinson v. Groskin, 927 F.2d 722, 725 (2d Cir. 1991)*. That "rule is not inflexible," *id.*, however, and we do not "necessarily find [a]n objection affirmatively waived because it might have been interposed a few questions earlier," *United States v. Pujana-Mena, 949 F.2d 24, 33 (2d Cir. 1991)*. Thus, although a contemporaneous objection is preferable, the district court was within its discretion to sustain the later objection and strike the testimony.

[55] PHP is a common computer programming language that is used primarily in website development.

[56] A kernel is an operating system's core, and it "is an essential part of the Linux operating system." Tr. 1070.

that Kiernan's conclusions about Ulbricht's laptop were inaccurate because they were based on unreliable information.

The district court sustained objections to those questions because, in its view, they were outside the scope of Kiernan's direct testimony. *See* Fed. R. Evid. 611(b) ("Cross-examination should not go beyond the subject matter of the direct examination and matters affecting the witness's credibility."); *Baker v. Goldman Sachs & Co., 669 F.3d 105, 110 (2d Cir. 2012)* (**HN42**[ ] "Once any direct examination is concluded, cross-examination within the scope of the direct follows.").

On appeal, Ulbricht claims that, because Kiernan testified about the operation of Tor Chat and other forensic computer issues during his direct testimony, the precluded questions were within that testimony's scope and should have been allowed. Even assuming **[**96]** that Ulbricht is correct, any error is harmless. Ulbricht was permitted to question Kiernan about whether Linux was customizable, and Kiernan admitted during cross that he did not know whether he used the same version of Tor Chat that Ulbricht had installed on his laptop. Ulbricht's counsel also asked several questions about the security vulnerabilities of BitTorrent, conveying to the jury that using BitTorrent might have rendered Ulbricht's computer susceptible to hacking. Thus, Ulbricht was able to elicit testimony supporting his proposed inference that Kiernan's conclusions based on the Tor Chat evidence were flawed. Ulbricht does not explain how he was prejudiced **[*121]** when the district court prohibited him from asking Kiernan certain other questions. We therefore identify no reversible error in the district court's limitations on Kiernan's cross examination.

D. Andrew Jones Hearsay Statement

The district court excluded a statement allegedly made by Andrew Jones, who was a Silk Road administrator under the username Inigo. Jones cooperated with the government and was on the government's witness list until the middle of trial, when the government decided not to call him. Defense counsel **[**97]** explored the possibility of calling Jones as a witness, but Jones's attorney advised Ulbricht that Jones would invoke the *Fifth Amendment* and refuse to testify if compelled to appear. In light of Jones's unavailability, Ulbricht sought to admit a December 29, 2014 letter from the government to defense counsel that described a statement that Jones made during one of his interviews.[57] The relevant portion of the government's letter is as follows:

> At some point in or about August or September 2013, Jones tried to authenticate that the Silk Road user "Dread Pirate Roberts" whom he was talking to at the time . . . was the same person with whom he had been communicating in the past with this username. Previously, . . . Jones and "Dread Pirate Roberts" had agreed upon a "handshake" to use for authentication, in which Jones would provide a certain prompt and "Dread Pirate Roberts" would provide a certain response. When, during the 2013 chat in question, Jones provided what he believed to be the designated prompt, "Dread Pirate Roberts" was unable to provide the response Jones thought they had agreed on. However, later in the chat, Jones asked "Dread Pirate Roberts" to validate himself by specifying the first **[**98]** job that "Dread Pirate Roberts" assigned to him (running the "DPR Book Club"), which "Dread Pirate Roberts" was able to do.

App'x 398. Ulbricht argues that the Jones statement[58] supports his theory that more than one person acted as Dread Pirate Roberts, because at one point DPR could authenticate his identity to Jones, but at another time he could not.

When it became clear that Jones was unavailable to testify, Ulbricht asked the government to stipulate that the Jones statement could be read to the jury. The government initially agreed, but then changed its mind and opposed admitting the Jones statement. The defense acknowledged that the statement was hearsay, but claimed that it was admissible under two hearsay exceptions: under *Rule 804(b)(3), Fed. R. Evid.*, as a statement against interest, and under *Rule 807*'s residual exception. The district court ruled that the statement was inadmissible, specifically addressing only *Rule 804(b)(3)*. On appeal, Ulbricht continues to argue that the statement was admissible under either

---

[57] The government did not concede that the statement was *Brady* information, but disclosed it "in an abundance of caution." App'x 398.

[58] What Ulbricht sought to introduce was the government's letter paraphrasing a statement made by Jones during an interview, not a verbatim transcript of what Jones had said. We refer to it as the "Jones statement" for the sake of simplicity.

exception. Neither of his theories is persuasive.[59]

[*122] HN44[] A district court's "ultimate decisions as to the admission or exclusion of evidence are reviewed for abuse of discretion, and will not be disturbed unless they are **[**99]** manifestly erroneous." Davis, 797 F.3d at 201 (internal quotation marks and citations omitted). HN45[] To invoke the 804(b)(3) exception for a statement against interest, the proponent of the statement "must show (1) that the declarant is unavailable as a witness, (2) that the statement is sufficiently reliable to warrant an inference that a reasonable man in [the declarant's] position would not have made the statement unless he believed it to be true, and (3) that corroborating circumstances clearly indicate the trustworthiness of the statement." United States v. Wexler, 522 F.3d 194, 202 (2d Cir. 2008) (internal quotation marks omitted). The exception applies "only if the district court determines that a reasonable person in the declarant's shoes would perceive the statement as detrimental to his or her own penal interest." United States v. Saget, 377 F.3d 223, 231 (2d Cir. 2004). The key to this inquiry is whether the statement is sufficiently "self-inculpatory," which the district court must evaluate on a "case-by-case basis." United States v. Williams, 506 F.3d 151, 155 (2d Cir. 2007).

The district court did not err in concluding that the Jones statement did not fall within Rule 804(b)(3)'s hearsay exception. There is no dispute that Jones was unavailable to testify because he planned to invoke his Fifth Amendment privilege. The court ruled that the Rule 804(b)(3) exception did not apply because Jones was under a cooperation **[**100]** agreement at the time that he made the relevant statement to the government and the chat did not have any particular impact on Jones's penal interests. On appeal, Ulbricht claims that the extent of Jones's criminal liability was unknown when he made the statement because he could still be vulnerable to prosecution in other jurisdictions, and he had not yet been sentenced when he made the statement to the government. *See* Mitchell v. United States, 526 U.S. 314, 326, 119 S. Ct. 1307, 143 L. Ed. 2d 424 (1999) (HN46[] in the Fifth Amendment context, there can be a "legitimate fear of adverse consequences from further testimony" where a sentence has not yet been imposed).

We are not persuaded that Jones's statement was against his penal interests. Given the cooperation agreement, the government's role at Jones's future sentencing, and the penalties for lying to the government, it is far from clear that it was against Jones's interest to disclose details of his criminal activities at the time the statement in question was made. Moreover, even to the extent that Jones's disclosures taken as a whole constituted inculpatory admissions, the particular statement in question had little adverse effect on Jones. Jones's inculpatory admissions to the government concern whether he committed crimes connected **[**101]** to Silk Road. His description of his "handshake" with DPR presupposes that he had already discussed his own crimes with the government. Whether DPR did or did not recognize Jones's identifying prompt does not bear on Jones's guilt of any crime associated with the site, since he had already confirmed his role working for DPR. The details of this conversation with DPR thus do not inculpate *Jones*; instead, they either help or hurt Ulbricht. Accordingly, the district court did not abuse its discretion in holding that Rule 804(b)(3) does not apply.

[*123] HN47[] *Rule 807* provides for a limited, residual exception to the rule against hearsay where no other exception applies. A hearsay statement may be admissible under *Rule 807* if: "(i) it is particularly trustworthy; (ii) it bears on a material fact; (iii) it is the most probative evidence addressing that fact; (iv) its admission is consistent with the rules of evidence and advances the interests of justice; and (v) its proffer follows adequate notice to the adverse party." United States v. Morgan, 385 F.3d 196, 208 (2d Cir. 2004) (internal quotation marks omitted). The "residual hearsay exception[] will be used very rarely, and only in exceptional circumstances." Parsons v. Honeywell, Inc., 929 F.2d 901, 907 (2d Cir. 1991) (internal quotation marks omitted).

The district court did not specifically **[**102]** address Ulbricht's request to admit the statement under *Rule 807*, but we conclude that the limited residual exception does not assist Ulbricht. We are loath to assume that a

[59] We note that the Jones statement is double hearsay, in that the defense sought to admit the government's subsequent characterization of Jones's interview, and both the government's letter and Jones's statement to the agents were out of court statements offered for their truth. HN43[] When confronted with "hearsay within hearsay, or double hearsay," courts must determine that "each part of the combined statement[]" is independently admissible. United States v. Williams, 927 F.2d 95, 100 (2d Cir. 1991). Because we conclude that no hearsay exception applied to the Jones statement at all, we need not address the double hearsay issue.

statement made by a criminal in debriefings to the government pursuant to a cooperation agreement is categorically "particularly trustworthy," as *Rule 807* requires. But even if Jones's statement meets that criterion, and was offered "as evidence of a material fact," we cannot say that it is "more probative on the point for which it is offered than any other evidence that the proponent can obtain through reasonable efforts." *Fed. R. Evid. 807(a)(2)-(3)*. Ulbricht has not attempted to explain how the Jones statement satisfies this requirement.

Finally, even if the district court erred in excluding the statement under either hearsay exception, any error was certainly harmless. The conversation between Jones and DPR in its totality was not actually helpful to Ulbricht. As explained, during the chat in question, DPR was at one point unable to provide the designated response, but later he identified himself to Jones's satisfaction. The statement thus contains the seeds of its own refutation. Since DPR's alleged failure to verify his identity and his subsequent **[**103]** remedy of that failure occurred during the same online chat, the interaction provides little or no support for the defense theory that different individuals acted as DPR at different times.

E. Cumulative Error

Ulbricht argues that the cumulative effect of the district court's evidentiary rulings deprived him of a fair trial. *See* United States v. Al-Moayad, 545 F.3d 139, 178 (2d Cir. 2008). We have exhaustively reviewed his contentions of trial error and have concluded that none of those contentions has merit. The challenged trial rulings were well within the district court's discretion, and the various exclusions did not prevent the defense from offering evidence probative of innocence. At the trial in this case, the government presented overwhelming evidence that Ulbricht was indeed Dread Pirate Roberts. The evidence that the defense was precluded from offering to refute that proof was excluded because it was speculative, unreliable, offered in contravention of the Federal Rules of Evidence or of Criminal Procedure, or otherwise inadmissible. The few instances in which the district court's rulings may be questioned, where we noted the relevance of the harmless error rule, involved minor and marginal points. Accordingly, whether considered separately **[**104]** or cumulatively, none of Ulbricht's evidentiary arguments lead us to doubt that he was found guilty after a fair trial.

III. Sentencing

HN48[↑] "[A] district court has broad latitude to impose either a Guidelines sentence or a non-Guidelines sentence." Rigas, **[*124]** 583 F.3d at 114 (internal quotation marks omitted). "Accordingly, the role of the Court of Appeals is limited to examining a sentence for reasonableness, which is akin to review under an 'abuse-of-discretion' standard." *Id.* "This standard applies both to the [substantive reasonableness of the] sentence itself and to the procedures employed in arriving at the sentence." *Id.* (internal quotation marks omitted). Ulbricht and *amici*[60] challenge his life sentence as both procedurally and substantively unreasonable.

A. Procedural Reasonableness

HN49[↑] "A sentence is procedurally unreasonable if the district court fails to calculate (or improperly calculates) the Sentencing Guidelines range, treats the Sentencing Guidelines as mandatory, fails to consider the § 3553(a) factors, selects a sentence based on clearly erroneous facts, or fails adequately to explain the chosen sentence." United States v. Jesurum, 819 F.3d 667, 670 (2d Cir. 2016) (internal quotation marks and emphasis omitted). To "hold that a factual finding is 'clearly erroneous,' **[**105]** we must be left with the definite and firm conviction that a mistake has been committed." United States v. DeSilva, 613 F.3d 352, 356 (2d Cir. 2010). Where "there are two permissible views of the evidence, the factfinder's choice between them cannot be clearly erroneous." United States v. Norman, 776 F.3d 67, 76 (2d Cir. 2015) (internal quotation marks omitted). In general, a "sentencing court has discretion to consider a wide range of information in arriving at an appropriate sentence." United States v. Prescott, 920 F.2d 139, 143 (2d Cir. 1990). "The district court's factual findings at sentencing need be supported only by a preponderance of the evidence." Norman, 776 F.3d at 76. "Where we identify procedural error in a sentence, but the record indicates clearly that the district court would have imposed the same sentence in any event, the error may be deemed harmless, avoiding the need to vacate the sentence and to remand the case for

[60] The *amici* who join Ulbricht's challenge to his life sentence include: the Drug Policy Alliance, Law Enforcement Against Prohibition, JustLeadershipUSA, and retired District Judge Nancy Gertner.

resentencing." *United States v. Jass, 569 F.3d 47, 68 (2d Cir. 2009)* (internal quotation marks omitted); *see also United States v. Cavera, 550 F.3d 180, 197 (2d Cir. 2008)* (en banc) (declining to reach claim that district court erred in relying on vague concern about gun violence because it was clear that the "district court would have imposed the same sentence had it relied solely on" the permissible concern about deterrence).

Ulbricht's only claim of procedural error is that it was improper for the district court to consider six drug-related deaths **[**106]** as relevant to his sentence because there was insufficient information connecting them with drugs purchased on Silk Road. In terms of our sentencing jurisprudence, Ulbricht claims that the district court relied on clearly erroneous facts in imposing sentence. We are not persuaded.

Ulbricht submitted an expert report in which Dr. Mark Taff wrote that the records associated with the six deaths were substantially incomplete. For example, many did not include full autopsies, rendering it difficult to discern the precise cause of death to a reasonable degree of medical certainty in five of the cases.[61] **[*125]** Equally importantly, Dr. Taff wrote that he could not conclusively connect the specific drugs that the decedents consumed with Silk Road, because it is impossible to "correlate the time of purchase/acquisition from an alleged Silk Road vendor" and the "time of usage of the alleged Silk road purchase" with the deaths.[62] S.A. 446. We assume for purposes of this opinion that Dr. Taff's conclusions are sufficiently sound to raise a genuine question about whether the deaths described in the PSR were caused by drugs purchased on Silk Road. As explained above, however, Ulbricht was not being prosecuted **[**107]** or punished for homicide on a theory that he personally caused those deaths. Nor did the fact of the deaths increase his offense level under the Guidelines. The question before the district court was whether the sale of large quantities of drugs on Silk Road created a sufficient risk of death to permit the district court to take the deaths into account in assessing the seriousness of Ulbricht's crimes when it considered the factors listed in *18 U.S.C. § 3553(a)*.

As with other facts relevant to sentencing, that question is for the district court to answer, based on the preponderance of the evidence. *Norman, 776 F.3d at 76*. Contrary to Ulbricht's claims, the district court did not summarily reject Dr. Taff's conclusions. Rather, it addressed his report carefully and acknowledged the evidentiary challenges of connecting the deaths to Silk Road. The court concluded that Dr. Taff's proposed "reasonable degree of medical certainty" standard was simply too high an evidentiary standard for purposes of including the deaths in the PSR. The court reasoned that it was "not asking whether the but for cause of death is drugs purchased on Silk Road," but rather "whether there is a connection between the purchase of drugs on Silk Road **[**108]** and [the] death" in the sense that the sale of those drugs created a risk of death. App'x 1476.

For those limited purposes and judged by that standard, the circumstantial evidence connecting the drug-related deaths to Silk Road was sufficient to consider them at Ulbricht's sentencing. To take the strongest example, one decedent was found in his apartment with a package torn open. His computer had the Silk Road site open, with chat messages from the vendor describing the heroin and prescription drug purchase as well as the package tracking information. The tracking number matched the information on the torn package in the apartment. A toxicology report determined that he died of an overdose of heroin combined with other prescription drugs. The facts connecting the other five deaths to Silk Road varied in strength. The available evidence was sufficient, however, to allow the district court find by a preponderance of the evidence that the deaths were connected to Silk Road; therefore, the court could consider the risk of death that the site created. Nothing in the sentencing transcript suggests that the court considered the information for any other purpose.

We are sensitive to the possibility **[**109]** that the evidence of the six deaths was emotionally **[*126]** inflammatory and risked implicitly escalating Ulbricht's

---

[61] In the sixth case, Dr. Taff concluded that the cause of death was ingesting multiple drugs coupled with a pre-existing heart condition. The original forensic reports concerning that death did not factor in the presence of drugs other than synthetic marijuana (obtained via Silk Road) and did not include the heart condition as a contributing cause.

[62] Sentencing *amici* make a similar argument, claiming that a complex array of causes are responsible for drug-related deaths, including societal failures. Assuming that is correct, the increased availability of drugs is certainly one of the causes of overdose and other drug-related accidental deaths. Thus, the district court did not err in concluding that Silk Road, which was by all accounts a market-expanding drug enterprise, contributed to the general social costs of drug trafficking. Those harms are numerous and include the risk of death.

responsibility from facilitating the sale of drugs to causing the deaths of several drug users.[63] But there is no indication that the deaths in question played such a role in the district court's sentencing determination. In urging the court to consider evidence of the deaths, the government explained that the deaths "illustrate the obvious: that drugs can cause serious harm, including death." App'x 902. *See* United States v. Pacheco, 489 F.3d 40, 48 n.5 (1st Cir. 2007) (observing that a defendant who "engaged in the commercial trade of potent substances . . . must have known [that such trade] could have dire consequences").

Of course, to the extent that the harms of the drug trade were obvious, there was no need to introduce evidence of these particular incidents, let alone to hammer the point home with unavoidably emotional victim impact statements by parents of two of the decedents.[64] No federal judge needs to be reminded of the tragic consequences of the traffic in dangerous substances on the lives of users and addicts, or of the risks of overdose and other ramifications of the most dangerous of illegal drugs. Those consequences are among **[**110]** the reasons why illegal drugs are prohibited and constitute a principal justification advanced for the extremely lengthy sentences provided by federal statutes and sentencing guidelines for trafficking in illicit substances. Absent reason to believe that a drug dealer's methods were unusually reckless, in that they enhanced the risk of death from drugs he sold beyond those already inherent in the trade, we do not think that the fact that the ever-present risk of tragedy came to fruition in a particular instance should enhance those sentences, or that the inability of the government to link a particular dealer's product to a specific death should mitigate them. The government's insistence on proceeding with this evidence generated an appellate issue that has taken on a disproportionate focus in relation to the reasons actually advanced by the district court in its lengthy and careful statement of the reasons for the sentence it imposed. App'x 1509-41.

We are not persuaded, however, that the introduction of the evidence in this case was error, although it may have been incautious for the government to insist on presenting it to the district court. As already explained, it was certainly **[**111]** appropriate for the district court to consider the risk of death from use of drugs in assessing the seriousness of the offense conduct, one of the factors that a judge must consider in imposing sentence. *See* 18 U.S.C. § 3553(a)(2)(A). That appears to be the only way the judge in this case used the evidence of the drug-related deaths. Emotionally wrenching as the statements of the decedents' parents were, we cannot and do not assume that federal judges are unable to put their sympathies for particular victims to one side and assess the evidence for its rational relationship to the sentencing decision. And here, the record makes clear that the district court did not use the evidence of the drug-related deaths to enhance Ulbricht's sentence, either as a formal matter under the Guidelines or otherwise. For all the extensive litigation of the **[*127]** propriety of including this information in the PSR, in imposing sentence the district court did not refer to the drug-related deaths as an aggravating factor. Indeed, the only mention of that evidence at all was a passing reference to "facts brought out in connection with [those] death[s]" that "provide evidence of first-time and expanded [drug] usage." App'x 1521-22. This reference **[**112]** occurred in the entirely appropriate context of a lengthy discussion of the general social harms of Ulbricht's massive drug-trading marketplace. *Id.* at 1522-28.

That discussion was particularly germane to this case for several reasons. First, Ulbricht claimed that Silk Road reduced the harms associated with the drug trade in several ways. For example, he argued that trafficking in drugs over the Internet reduced violence associated with hand-to-hand transactions and the societal stigma of drug use, and Silk Road's vendor rating system ensured that customers had access to better quality drugs and more information about the drugs that they were purchasing. Those arguments prompted the district court to reflect broadly on the costs of the drug trade and discuss Silk Road's participation in those harms. Reasonable people may and do disagree about the social utility of harsh sentences for the distribution of controlled substances, or even of criminal prohibition of their sale and use at all. It is very possible that, at some future point, we will come to regard these policies as tragic mistakes and adopt less punitive and more effective methods of reducing the incidence and costs of drug use.

At this point **[**113]** in our history, however, the

[63] Ulbricht does not argue that the evidence related to the accidental overdose deaths should have been excluded due to its emotional nature; his argument is based solely on the claim that the evidence was irrelevant because the deaths were not sufficiently linked to Silk Road.

[64] Ulbricht does not challenge the propriety of those statements apart from his general argument that it was procedurally unreasonable to consider the six deaths as relevant to his sentence.

democratically-elected representatives of the people have opted for a policy of prohibition, backed by severe punishment. That policy results in the routine incarceration of many traffickers for extended periods of time. This case involves a defendant who stood at one remove from the trade, who did not for the most part dirty his hands with the actual possession and sale of drugs and other contraband that his site offered. But he did take a cut of the proceeds, in exchange for making it easier for such drugs to be purchased and sold, in a way that may well have expanded the market by allowing more people access to drugs in greater quantities than might otherwise have been available to them. In the routine instances of sentencing drug sellers, the dangerous aspects of the trade are close to the surface and require little emphasis. In this case, a reminder of the consequences of facilitating such transactions was perhaps more necessary, particularly because Ulbricht claimed that his site actually made the drug trade safer, and he appeared to contest the legitimacy of the laws he violated.[65]

[*128] Finally, we need look no further than the district court's express **[**114]** reasons for imposing sentence to conclude that drug-related deaths played little part in dictating the sentence imposed. As tragic as they are, and as foreseeable in light of the volume of dangerous drugs trafficked through Silk Road, those deaths were accidents. In light of the overwhelming evidence, discussed below, that Ulbricht was prepared, like other drug kingpins, to protect his profits by paying large sums of money to have individuals who threatened his enterprise murdered, it would be plainly wrong to conclude that he was sentenced for accidental deaths that the district court discussed only in passing in imposing sentence. Even were we to conclude that the evidence of the Silk Road-related deaths should not have been received, any error would be harmless, because the record is absolutely clear that the district court, after finding that Ulbricht commissioned five murders, would have imposed the same sentence if the evidence of the drug-related deaths had been excluded.

The sentencing *amici* advance one additional argument: that the district court's consideration of the drug-related deaths violated the *Fifth* and *Sixth Amendments* because the fact of those deaths was not charged in the Indictment **[**115]** and proven to the jury. "While ***HN50***[ ] we are not required to address arguments raised only by an *amicus*," *Am. Atheists, Inc. v. Port Auth. of N.Y. & New Jersey, 760 F.3d 227, 237 n.11 (2d Cir. 2014)*, we do so here in an excess of caution. The argument is without merit under *Apprendi v. New Jersey, 530 U.S. 466, 120 S. Ct. 2348, 147 L. Ed. 2d 435 (2000)*, and its progeny.

HN51[ ] A district court may consider as part of its sentencing determination uncharged conduct proven by a preponderance of the evidence as long as that conduct does not increase either the statutory minimum or maximum available punishment. *See United States v. Stevenson, 834 F.3d 80, 85 (2d Cir. 2016)*; *United States v. Ryan, 806 F.3d 691, 693-94 (2d Cir. 2015)*. The Supreme Court has "long recognized that broad sentencing discretion, informed by judicial factfinding, does not violate the *Sixth Amendment*." *Alleyne v. United States, 133 S. Ct. 2151, 2163, 186 L. Ed. 2d 314 (2013)*. Here, the six drug-related deaths (and more importantly, Ulbricht's attempted murders for hire) were uncharged facts that did not increase either the statutory twenty-year minimum or the maximum life sentence

[65] In a footnote in his reply brief, Ulbricht raises for the first time an additional argument: that the district court improperly gave him a life sentence because of the political and philosophical beliefs that led him to start Silk Road in the first instance. Ulbricht argues that reliance on political beliefs at sentencing is prohibited by the *Guidelines, U.S.S.G. § 5H1.10*, and the *First Amendment*. The district court reflected on Ulbricht's philosophy, however, only in the course of discussing his character and his reasons for committing the offense. *See 18 U.S.C. § 3553(a)(1)*. That discussion was relevant to sentencing. Ulbricht, as the district court concluded, "viewed Silk Road both as above the law and the laws didn't apply." App'x 1515. He appeared to believe that his personal views about the propriety of the drug laws and the paramount role of individual liberty entitled him to violate democratically-enacted criminal prohibitions. For example, some of his Silk Road posts "discuss the laws as the oppressor" and proclaim that "each transaction is a victory over the oppressor." *Id.* at 1516. That Ulbricht believes that drug use should be legalized is not relevant to sentencing; that he believes he is entitled to break the laws that prohibit certain substances is relevant to his likelihood of recidivism, a mandated sentencing consideration. *18 U.S.C. § 3553(a)(2)(C)*. The district court therefore did not sentence Ulbricht based on any prohibited characteristic, nor did the court place more weight on that factor than the facts warranted. *Cf. United States v. Jenkins, 854 F.3d. 181, 2017 WL 1371399 (2d Cir. 2017)* (vacating a sentence as substantively unreasonable where the district court relied exclusively on the defendant's "disdain for the law" in "dramatically increasing" a defendant's sentence for child pornography offenses). Ulbricht's disrespect for the law was simply one factor that the district court considered in imposing sentence, along with many others, and was not accorded undue weight in determining the sentence.

applicable to the crimes of which he was found guilty, beyond a reasonable doubt, by the jury. Thus, the district court did not violate the Constitution when it found by a preponderance of the evidence that the six deaths were connected to Silk Road and that they were relevant to Ulbricht's sentence because they were part of the harm that the site caused.

In sum, we might not, in the prosecutors' shoes, have chosen to offer **[**116]** this evidence at sentencing, or have admitted it as district judges. We conclude, however, (1) that the district court did not clearly err **[*129]** when it found by a preponderance of the evidence that the six deaths were connected to Silk Road; (2) that it did not abuse its discretion in determining that it was appropriate to consider those acts as bearing on the seriousness of the narcotics offenses of which Ulbricht was convicted, one of many factors the district court was required to consider in exercising its discretion under *§ 3553(a)*; and (3) that the evidence in question in fact played a minimal role, if any, in the actual sentencing, and that in light of the reasons given by the district court for its sentencing decision, we can be absolutely certain that the same sentence would have been imposed if the evidence had not been received. Ulbricht's sentence was therefore not procedurally unreasonable.

B. Substantive Unreasonableness

HN52[] "We will . . . set aside a district court's substantive [sentencing] determination only in exceptional cases where the trial court's decision cannot be located within the range of permissible decisions." *Cavera, 550 F.3d at 189* (emphasis and internal quotation marks omitted). Our review is **[**117]** "deferential," and this Court does "not consider what weight we would ourselves have given a particular factor." *Rigas, 583 F.3d at 122*. "Rather, we consider whether the factor, as explained by the district court, can bear the weight assigned it under the totality of the circumstances in the case." *Id.* Our role in "patrolling the boundaries of reasonableness" is modest. *United States v. Broxmeyer, 699 F.3d 265, 289 (2d Cir. 2012)* (alterations and internal quotation marks omitted). Accordingly, we "will set aside only those outlier sentences that reflect actual abuse of a district court's considerable sentencing discretion." *United States v. Messina, 806 F.3d 55, 66 (2d Cir. 2015)*.

In light of the deferential standard of review, we cannot say that Ulbricht's life sentence was substantively unreasonable. The district court identified numerous facts that made Ulbricht's case extraordinary, in its view rendering a life sentence "sufficient, but not greater than necessary, to comply with the purposes" of sentencing. *18 U.S.C. § 3553(a)*. The court described the crime as a "planned, comprehensive, and deliberate scheme . . . which posed serious danger to public health and to our communities." App'x 1511-12. Silk Road was a "worldwide criminal drug enterprise with a massive geographic scope." *Id.* at 1512. The fact that Ulbricht operated the site from behind **[**118]** a computer, rather than in person like a more prototypical drug kingpin, does not make his crime less serious or less dangerous. Moreover, Silk Road uniquely expanded the drug market by providing an easy avenue for people to become first-time drug users and dealers. Because drugs were shipped to customers in the mail, Silk Road brought "drugs to communities that previously may have had no access to such drugs . . . in such quantities." *Id.* at 1522.

The quantity and nature of the drugs sold on Silk Road are staggering. According to the PSR, from 2011 through 2013, Silk Road customers transacted in approximately $183 million worth of illegal drugs. At the time the government shut down Silk Road on October 2, 2013, there were approximately 13,802 listings for controlled substances on the website. Of those listings, there were 643 listings for cocaine-based products, 305 for LSD products, and 261 for methamphetamine products. The drugs were sold mostly for individual, personal use, but some drugs such as heroin and cocaine were also available in "multi-kilogram quantities." PSR ¶ 26. The available drugs were not limited to heroin, narcotics, synthetic marijuana, and other dangerous but recreational **[**119]** substances. For **[*130]** example, after being told that cyanide was "the most well known assassination suicide [*sic*] poison out there," Ulbricht allowed vendors to sell it on Silk Road despite its singular, deadly purpose. App'x 1519. As the district court noted, despite earlier protestations that Silk Road would not allow the sale of products that could be used to inflict deliberate harm on others, it took Ulbricht all of six minutes to decide "that it is okay to sell cyanide," *id.*, in exchange for the customary cut of the proceeds.

The drug offenses alone—ignoring all other illicit materials sold on the site[66]—yielded a calculated

[66] As explained, Silk Road also trafficked in illegal goods such as counterfeit identification documents and computer hacking tools and services. When the government shut down Silk

offense level of 50. Of that calculation, only two levels are attributable to Ulbricht's "credible threats of directed violence" associated with the murders for hire. PSR ¶ 94. Thus, even without considering that enhancement, the drug convictions yielded an offense level of 48, which is higher than the maximum offense level recognized by the Guidelines, for which a sentence of life imprisonment is recommended even for someone who, like Ulbricht, has no prior criminal convictions. Ulbricht does not challenge the accuracy of the Guidelines calculation or of the fact-findings **[**120]** on which it is based.

HN53[] That the sentence imposed accorded with the Guidelines recommendation does not automatically render it reasonable. *See* *United States v. Dorvee, 616 F.3d 174, 182 (2d Cir. 2010)*. The Guidelines are, however, themselves a factor that Congress has directed district courts to consider. *18 U.S.C. § 3553(a)(4)(A)*. Moreover, as the considered judgment of the United States Sentencing Commission, they bear on the other factors that Congress has required courts to evaluate, including the need to reflect the seriousness of the offense, *id.* *§ 3553(a)(2)(A)*, to provide adequate deterrence, *id.* *§ 3553(a)(2)(B)*, and, because they are considered by all judges throughout the federal system, the need to "avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct," *id.* *§ 3553(a)(6)*.

Accordingly, while a life sentence for selling drugs alone would give pause, we would be hard put to find such a sentence beyond the bounds of reason for drug crimes of this magnitude.[67] But the facts of **[*131]** this case involve much more than simply facilitating the sale of narcotics. The district court found by a preponderance of the evidence that Ulbricht commissioned at least five murders in the course of protecting Silk Road's anonymity, a finding that Ulbricht does **[**121]** not challenge in this appeal.[68] Ulbricht discussed those anticipated murders callously and casually in his journal and in his communications with the purported assassin Redandwhite. For example, in connection with the first hit, he wrote to Redandwhite that "FriendlyChemist is a liability and I wouldn't mind if he was executed." Tr. 1822. In the course of negotiating the price for the killing, DPR claimed that "[n]ot long ago, I had a clean hit done for $80k," *id.* at 1883, but that he had "only ever commissioned the one other hit, so I'm still learning this market," *id.* at 1884. He then paid $150,000 in Bitcoins for the murder, and he received what purported to be photographic documentation if its completion. Ulbricht then wrote in his journal that he "[g]ot word that the blackmailer was executed," *id.* at 1887, before returning quickly to other tasks associated with running the site.

In negotiating the other four killings, Ulbricht initially resisted multiple murders. He instructed Redandwhite to "just hit Andrew [usernames Tony76 and nipplesuckcanuck] and leave it at that." *Id.* at 1897. Redandwhite said he could do it for "150 just like last time," but that he would not be able to recover any of DPR's money if he killed only **[**122]** one person because he would have to commit the murder outside of

---

Road, there were 156 listings for forged identity documents on the site. The specific computer hacking tools available included software for compromising usernames and passwords of electronic accounts, including email and Facebook; Remote Access Tools ("RATs") that allow hackers to obtain remote access to a victim's computer, including turning on and using the computer's webcam; keyloggers, which allow a user to monitor keystrokes inputted by a victim to discern their passwords and other sensitive information; and Distributed Denial of Service ("DDoS") tools, which allow hackers to disable websites by flooding networks with malicious Internet traffic. Silk Road also offered money laundering services through vendors who sold U.S. currency and anonymous debit cards. Because the adjusted offense levels for those groups of offenses were substantially lower than the offense level for the drug group, they did not contribute to Ulbricht's overall offense level. In assessing the substantive reasonableness of the sentence imposed, however, it is well to remember that the sentence encompassed Ulbricht's role not only in the distribution of controlled substances, but in a wide variety of other criminal offenses as well.

[67] Note that such a sentence is *mandatory* under federal law for selling just five kilograms of cocaine after two prior convictions for *any* felony narcotics offense, *see* *21 U.S.C. § 841(b)(1)(A)*, and the Supreme Court has upheld against constitutional challenge a mandatory sentence of life imprisonment for selling 650 grams of cocaine, *Harmelin v. Michigan, 501 U.S. 957, 111 S. Ct. 2680, 115 L. Ed. 2d 836 (1991)*.

[68] Ulbricht does not mention his orders for the commission of those murders until his reply brief. Even there, he does not argue that the district court erred in concluding that he deliberately commissioned those murders; rather, he claims instead only that the murders did not support a life sentence because they did not actually take place. But in evaluating Ulbricht's character and dangerousness, the most relevant points are that he wanted the murders to be committed, he paid for them, and he believed that they had been carried out. The fact that his hired assassin may have defrauded him does not reflect positively on Ulbricht's character. Commissioning the murders significantly justified the life sentence.

the victim's home or office where he stored his funds. *Id.* If Ulbricht wanted him to recover money, the self-professed assassin claimed, he would have to kill not only Tony76, but also his three associates. DPR responded that he would "defer to [Redandwhite's] better judgment and hope[d] [to] recover some assets" from the hit. *Id.* at 1899. He then sent $500,000 in Bitcoins, the agreed-upon price for four killings, to Redandwhite. As the district court stated in discussing Ulbricht's journal entries concerning these projected murders, his words are "the words of a man who is callous as to the consequences or the harm and suffering that [his actions] may cause others." App'x 1521.

The record was more than sufficient to support the district court's reliance on those attempted murders in sentencing Ulbricht to life in prison. The attempted murders for hire separate this case from that of an ordinary drug dealer, regardless of the quantity of drugs involved in the offense, and lend further support to the district court's finding that Ulbricht's conduct and character were exceptionally destructive. That he was able to distance himself from the **[**123]** actual violence he paid for by using a computer to order the killings is not mitigating. Indeed, the cruelty that he displayed in his casual and confident negotiations for the hits is unnerving. We thus cannot say that a life sentence was outside the "range of permissible decisions" under the circumstances. *Cavera, 550 F.3d at 189*.

[*132] Ulbricht's arguments on appeal have rhetorical power because of the sheer magnitude of his sentence, but they do not provide a legal basis for vacating that sentence as substantively unreasonable. He contends that the district court ignored the letters submitted on his behalf, thus failing to consider his positive contributions to his family and society as well as his potential productivity should he be released from prison. To the contrary, however, the district court "read each and every one of [the letters] with care," some "more than once." App'x 1534. Recognizing that the letters were "beautiful" and "profoundly moving," the district court observed that they reveal Ulbricht's human complexity. *Id.* at 1534-35. Nothing in the record supports the claim that the district court failed to recognize the importance of the letters, incorrectly discounted Ulbricht's more favorable characteristics, **[**124]** or otherwise inappropriately dismissed their role in its sentencing determination.

Similarly, Ulbricht's argument that the district court ignored his contention that Silk Road reduced the harmful effects of drug crimes must be rejected. The district court thoroughly discussed Doctor X's role at Silk Road and Ulbricht's claims that the site reduced violence, overdoses, and other harms associated with drug trafficking, and concluded that they were unpersuasive. We see no error in its analysis, and Ulbricht's arguments concerning harm reduction do not render his sentence substantively unreasonable.

Ulbricht also claims that there is an unwarranted disparity between his sentence and the approximately 17-month sentence that Peter Nash, a Silk Road administrator, received. Again, however, the district court considered the arguments concerning Nash's sentence and found them to be irrelevant to Ulbricht's crime because Nash was a low-level site administrator who pleaded guilty and cooperated with the government. Along those same lines, Ulbricht notes that Silk Road drug dealers received lower sentences than he did. For example, one such drug dealer received a ten-year sentence. The fact that **[**125]** different people involved with the site received dramatically lower sentences does not mean that Ulbricht's own sentence was substantively unreasonable on the individual facts of his case.[69] Ulbricht was the creator and head administrator of the site. That fact alone distinguishes his case from that of any individual seller or employee who used or worked for the site. Ulbricht profited from every sale on Silk Road, and he facilitated the acts of each drug dealer and drug organization that used it. Moreover, he attempted to commission at least five murders to protect his criminal enterprise. Those facts render his case distinguishable from those who committed other crimes using Silk Road or otherwise facilitated its operation.

Ulbricht next reiterates his argument that he was more like someone running a crack house than like a drug kingpin because he created the online platform that *others* used to sell drugs and was not himself a drug dealer.[70] That argument also understates the vast extent of Silk Road's drug market, which had thousands of customers and trafficked in about $183 **[*133]**

[69] In his reply, Ulbricht references other instances in which people involved with Silk Road (and its apparent reincarnation, Silk Road 2.0) received significantly lower sentences. Ulbricht does not provide sufficient detail about those individuals' conduct, however, to permit meaningful comparisons with his case.

[70] Ulbricht did sell drugs on Silk Road for at least some brief period of time, when he grew and sold hallucinogenic mushrooms to drum up interest in the site.

million in illegal drugs. People may differ about whether "respectable" people who, acting as property owners, **[**126]** money launderers, or other facilitators of crime for personal gain are less guilty than those who personally handle the narcotics. We cannot fault the district court for rejecting the argument that Ulbricht's contribution to the narcotics trade was inherently less culpable than that of the dealers who paid him to use Silk Road to complete their transactions.

Both the sentencing *amici* and Ulbricht further contend that the district court placed too much weight on the notion of general deterrence in meting out the life sentence. Specifically, Ulbricht fears that resorting to "general deterrence without any confining principles . . . guarantees that [the sentence] will create disparity." Appellant Br. 139. *Amici* also observe that academic studies counsel against placing too much emphasis on general deterrence in sentencing because severe criminal punishments do not actually decrease either supply or demand for illegal drugs. Further, according to *amici*, the threat of a long sentence does not deter criminal conduct more effectively than the threat of a shorter sentence. In his reply, Ulbricht identifies several lucrative dark markets that have emerged since Silk Road's demise in 2013. In **[**127]** his view, the existence of multiple copycat Tor-based illegal marketplaces proves that general deterrence is illusory and that the district court placed too much weight on that factor.

Although those arguments have some support among scholars and researchers, ***HN54***[⬆] the ability of a sentence to "afford adequate deterrence to criminal conduct" is a factor that district courts are *required* by Congress to consider in arriving at the appropriate sentence. *18 U.S.C. § 3553(a)(2)(B)*; *see United States v. Tran, 519 F.3d 98, 107 (2d Cir. 2008)*. Congress, moreover, has not concluded that the persistence of narcotics crimes is a reason to abandon the efforts to deter them by lengthy sentences. The district court observed that "general deterrence plays a particularly important role" in Ulbricht's case because Silk Road is "without serious precedent" and generated an unusually large amount of public interest. App'x 1532-33. The court thus carefully analyzed the role that general deterrence played in Ulbricht's individual case. At the same time, it is evident from the sentencing transcript that general deterrence was "just one element in the [district court's] analysis," *id.* at 1533, and the district court considered many other factors before sentencing Ulbricht to life in prison. Thus, the **[**128]** factor of general deterrence, "as explained by the district court, can bear the weight assigned it under the totality of circumstances in this case." *Rigas, 583 F.3d at 122*.

Finally, Ulbricht and *amici* point out that life sentences are rare in the federal system, typically reserved for egregious violent crimes, thus rendering Ulbricht's sentence substantively unreasonable.[71] Moreover, according to *amici*, life sentences are normally imposed in cases where that is the district judge's only sentencing option. Thus, they claim that Ulbricht's life sentence is substantively unreasonable in the context of the federal system, where life sentences are particularly rare for those with no criminal history **[*134]** who are convicted of drug crimes.[72]

We agree with Ulbricht that life sentences are extraordinary and infrequent, which is as it should be. But the rarity of life sentences does not mean that the imposition of such a sentence in this case is substantively unreasonable under our law. Each case must be considered on its own facts and in light of all of the circumstances of a particular offense as well as other relevant conduct, which, in this case, includes five attempted murders for hire. As we have **[**129]** described, the district court carefully considered Ulbricht's offense, his personal characteristics, and the context for his crimes, recognizing that only exceptional cases justify such a severe sentence. Although we might not have imposed the same sentence ourselves in the first instance, on the facts of this case a life sentence was "within the range of permissible decisions" that the district court could have reached. *Rigas, 583 F.3d at 122*.

---

[71] *Amici* also claim that Ulbricht's life sentence violates the *Eighth Amendment's* ban on cruel and unusual punishment. That argument is plainly incorrect in light of binding Supreme Court precedent to the contrary. *See Harmelin, 501 U.S. 957, 111 S. Ct. 2680, 115 L. Ed. 2d 836*.

[72] In his reply, Ulbricht raises a distinct but related argument for the first time. He argues that "concurrences from Supreme Court opinions and dissents from denials of certiorari suggest[] that judicial factfinding violates a defendant's constitutional right to a jury trial where the factfinding renders reasonable an otherwise substantively unreasonable sentence." Reply Br. 60. For that proposition, he cites *United States v. Hebert, 813 F.3d 551, 563 (5th Cir. 2015)*, *cert. denied*, ***137 S. Ct. 37, 196 L. Ed. 2d 26 (2016)***, *Jones v. United States, 135 S. Ct. 8, 190 L. Ed. 2d 279 (2014)* (Scalia, J., dissenting from denial of certiorari), and *United States v. White, 551 F.3d 381, 386 (6th Cir. 2008)* (Merritt, J., dissenting). His argument, however, has no support in existing law.

We do not reach our conclusion lightly.[73] A life sentence is the second most severe penalty that may be imposed in the federal criminal justice system. "The size of [Ulbricht's] sentence alone [therefore] counsels our careful, searching review of it." *United States v. Brown, 843 F.3d 74, 85 (2d Cir. 2016)* (Sack., J., concurring). Courts have the power to condemn a young man to die in prison, and judges must exercise that power only in a small number of cases after the deepest thought and reflection. Of course, any "sentencing proceeding is a solemn occasion at which the judge has the weighty duty of determining the fate of another human being." *United States v. Alcantara, 396 F.3d 189, 199 (2d Cir. 2005)*. We must be especially sensitive to that duty where the most severe sentences are in question. The district court gave Ulbricht's sentence the thorough consideration that it required, **[**130]** reviewing the voluminous sentencing submissions, analyzing the factors required by law, and carefully weighing Ulbricht's mitigating arguments. The extraordinarily detailed sentencing transcript shows that the district court appreciated its important responsibility in considering a sentence of such magnitude and carried out that responsibility with care and prudence. Under the law, we cannot say that its decision was substantively unreasonable.

[*135] CONCLUSION

For the foregoing reasons, we AFFIRM the judgment of the district court in all respects.

End of Document

---

[73] The life sentence is particularly severe because, as in all federal cases, Ulbricht will never be eligible for parole. Unlike state sentences in jurisdictions permitting a sentence of, for example, "25 years to life," there is no automatic reconsideration of this sentence, or of whether an offender has reformed, after any lengthy period of incarceration. We note that, particularly in the case of a young offender, the prisoner will all but certainly change (for better or worse) after many years of incarceration. In a system without parole, however, a sentencing court is forced to exercise its best judgment to predict whether a sentence of life imprisonment or one of 25, 30, or 50 years is required to serve the purposes of sentencing, without the option of deferring that judgment to a point at which the effects of incarceration, and the passage of time, will be more apparent.

256 F.Supp.3d 355
United States District Court, S.D. New York.

UNITED STATES of America,
v.
Benjamin WEY, Defendant.

15–CR–611 (AJN)
|
Filed 06/13/2017
|
Signed June 14, 2017

Synopsis

Background: Defendant was charged with securities and wire fraud, as well as money laundering. Defendant moved to suppress.

Holdings: The District Court, Alison J. Nathan, J., held that:

[1] warrants to search defendant's business and apartment failed to identify suspected crimes;

[2] warrants set forth expansive categories of generic items subject to seizure without linking to suspected criminal activity;

[3] warrants lacked temporal limitation;

[4] all records exception did not apply;

[5] warrants were overbroad; and

[6] good faith exception to exclusionary rule did not apply.

Motion granted.

West Headnotes (25)

[1] **Criminal Law** Persons entitled to object

A defendant seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment generally must show that he had a legitimate expectation of privacy in the place searched. U.S. Const. Amend. 4.

[2] **Criminal Law** Persons entitled to object

Where the premises searched is a business, defendants seeking suppression must establish both that they are associated with the business and that they have a legitimate expectation of privacy in the part of the business that was searched. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[3] **Searches and Seizures** Particularity or generality and overbreadth in general

The Fourth Amendment's particularity requirement for a warrant is necessarily tied to the probable cause requirement; that is because by limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. U.S. Const. Amend. 4.

3 Cases that cite this headnote

[4] **Searches and Seizures** Form and Contents of Warrant; Signature

In assessing the Constitutional sufficiency of any warrant, courts must be mindful that the ultimate touchstone of the Fourth Amendment is reasonableness. U.S. Const. Amend. 4.

[5] **Searches and Seizures** Particularity or generality and overbreadth in general

Courts implement the Fourth Amendment particularity requirement by insisting that warrants not leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized; put differently, a warrant must be sufficiently specific to permit the rational exercise of judgment by the executing officers in selecting what items to seize. U.S. Const. Amend. 4.

2 Cases that cite this headnote

[6] **Searches and Seizures** Particularity or generality and overbreadth in general

To comport with the Fourth Amendment's particularity requirement, a warrant must satisfy three criteria: first, it must identify the specific offense for which the police have established probable cause; second, the warrant is required to describe the place to be searched; third, it must specify the items to be seized by their relation to designated crimes. U.S. Const. Amend. 4.

5 Cases that cite this headnote

[7] **Searches and Seizures** Form and Contents of Warrant; Signature

A court may construe a warrant with reference to a supporting application or affidavit only if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant. U.S. Const. Amend. 4.

[8] **Searches and Seizures** Form and Contents of Warrant; Signature

For an attached affidavit properly to be incorporated into a warrant, the warrant must contain deliberate and unequivocal language of incorporation; language in a warrant that simply references an underlying affidavit does not suffice. U.S. Const. Amend. 4.

[9] **Searches and Seizures** Particularity or generality and overbreadth in general

The doctrine of overbreadth represents, in a sense, an intersection point for probable cause and particularity principles: it recognizes, in pertinent part, that a warrant's unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[10] **Searches and Seizures** Particularity or generality and overbreadth in general

A warrant is overbroad if its description of the objects to be seized is broader than can be justified by the probable cause upon which the warrant is based. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[11] **Searches and Seizures** Objects or information sought

Where property to be searched is a computer hard drive, the Fourth Amendment's particularity requirement assumes even greater importance; that is because the seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[12] **Searches and Seizures** Time of Execution

The Fourth Amendment requires the government to complete its review of seized electronically stored information, that is, execute the warrant,

within a reasonable period of time. U.S. Const. Amend. 4; Fed. R. Crim. P. 41(e)(2)(B).

4 Cases that cite this headnote

[13] **Searches and Seizures** Particularity or generality and overbreadth in general

Warrants to search defendant's business and apartment failed to identify suspected crimes, and therefore, lacked particularity required by the Fourth Amendment, where warrants did not cite criminal statutes or describe suspected criminal conduct, supporting affidavits that did set forth such information were not attached or incorporated into warrants, and references in warrants to documents that were consistent with an investigation into securities fraud, for which defendant was eventually charged, were broad enough to be consistent with any form of financial crime. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[14] **Searches and Seizures** Objects or information sought

Warrants to search defendant's business and apartment set forth expansive categories of generic items subject to seizure without linking to suspected criminal activity, and therefore, lacked particularity required by the Fourth Amendment, where warrant authorized seizure of, among other things, financial records, notes, and photographs, property listed was generally lawful to use in substantial quantities, specific items listed were used as illustrations, and only purported limitation on executing officers' seizure authority was that items "concern," "relate" to or be connected to the individuals and entities set forth in the warrants, which was not a limit as that permitted seizure of items pertaining to defendant and the business without any suspicion of a crime. U.S. Const. Amend. 4.

3 Cases that cite this headnote

[15] **Searches and Seizures** Objects or information sought

Warrants to search defendant's business and apartment lacked temporal limitation, and therefore, lacked particularity required by the Fourth Amendment, where warrants lacked any reference to relevant timeframe or dates of interest. U.S. Const. Amend. 4.

[16] **Searches and Seizures** Objects or information sought

When there is probable cause to believe that an entire business is pervaded or permeated with fraud, seizure of all records of the business is appropriate, and broad language used in a search warrant will not offend the particularity requirement; this principle is commonly referred to as the all-records exception to the particularity requirement. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[17] **Searches and Seizures** Objects or information sought

For the all-records exception to apply, an affidavit in support of a search warrant need not necessarily lay out specific factual evidence demonstrating that every part of an enterprise in question is engaged in fraud; rather, it must only set forth sufficient factual evidence of fraudulent activity from which a magistrate could infer that those activities are just the tip of the iceberg. U.S. Const. Amend. 4.

[18] **Searches and Seizures** Objects or information sought

The Fourth Amendment requires more than mere extrapolation to activate the all-records principle to seize all records of a business suspected of fraud; courts assessing the applicability of the exception must satisfy themselves that the Government provided the magistrate judge with

sufficient probable cause to believe that the entire business operation is a scam. U.S. Const. Amend. 4.

[19] **Searches and Seizures** Objects or information sought

Applications for search warrants for defendant's business and apartment did not provide sufficient probable cause to believe that defendant's entire business operation was permeated with fraud, as required for all-records exception to apply to permit seizure of evidence despite lack of particularity in warrants; warrant affidavits described business in terms that suggested legitimacy of business, affidavits only implicated five or six discrete deals, and affidavits did not make explicit assertions that business was permeated by fraud or explicitly request permission to execute all-records seizure. U.S. Const. Amend. 4.

[20] **Searches and Seizures** Objects or information sought

Search warrants for defendant's apartment and business were overbroad in violation of the Fourth Amendment, where warrants did not include meaningful guidelines to search agents, and warrants authorized seizure of all documents. U.S. Const. Amend. 4.

1 Cases that cite this headnote

[21] **Criminal Law** Particular cases

Good faith exception to exclusionary rule did not apply to prevent exclusion of evidence seized from defendant's apartment and business based on law enforcement reliance on unparticularized warrants; warrants were facially unparticularized as they did not identify crimes under investigation and authorized seizure of multiple expansive categories of records, including notes and photographs, without linking evidence to suspected criminal conduct, there was no exigency as warrant application took place over the course of weeks, warrant provided 10 day window for execution, supervising agent did not ensure that items seized were within scope of approved search, 20 agents involved in search did not review the warrant affidavits prior to searches in order to take notice of limits not contained in warrants, searching agents were told to exercise their discretion in following the warrant, rather than to follow the affidavits or briefings, agents seized materials purely personal in nature, including medical records, government continued to retain seized items, and government subjected electronics to continuing and expanding searches for years. U.S. Const. Amend. 4.

4 Cases that cite this headnote

[22] **Criminal Law** Reliance on statute, ordinance, or precedent; mistake of law

Criminal Law Exceptions Relating to Defects in Warrant

The good faith exception to the exclusionary rule provides that evidence obtained by officers in objectively reasonable reliance on a warrant subsequently invalidated by a reviewing court is not generally subject to exclusion; likewise government agents act in good faith when they perform searches conducted in objectively reasonable reliance on binding appellate precedent. U.S. Const. Amend. 4.

[23] **Criminal Law** Exceptions Relating to Defects in Warrant

For the good faith exception to the exclusionary rule to apply, officers' reliance on a warrant must actually be objectively reasonable; that requirement generally demands that the officer exhibit reasonable knowledge of what the law prohibits. U.S. Const. Amend. 4.

[24] **Criminal Law** Exceptions Relating to Defects in Warrant

When multiple officers are involved in an illegal search, it is necessary to consider the objective reasonableness of reliance on a warrant, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination. U.S. Const. Amend. 4.

[25] **Criminal Law** Exceptions Relating to Defects in Warrant

The good faith exception cannot shield even an officer who relies on a duly issued warrant in at least four circumstances: (1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable. U.S. Const. Amend. 4.

Attorneys and Law Firms

***359** Andrew Caldwell Adams, Brooke Elizabeth Cucinella, Ian Patrick McGinley, Michael Ferrara, Sarah Kathleen Eddy, Brendan Francis Quigley, United States Attorney's Office, New York, NY, for United States of America.

Barry McNeil, Haynes and Boone, LLP, Dallas, TX, Joseph Craig Lawlor, Sarah Elizabeth Jacobson, David Mark Siegal, Haynes and Boone, LLP, New York, NY, for Defendant.

OPINION & ORDER [CORRECTED]

ALISON J. NATHAN, District Judge:

Defendant Benjamin Wey faces an eight-count indictment charging him with securities fraud, wire fraud, conspiracy to commit securities and wire fraud, money laundering, and failure to disclose beneficial ownership of publicly traded companies. Before the Court is Wey's motion to suppress evidence seized during Government searches of his residence and the offices of his consulting firm, New York Global Group, Inc., both conducted on January 25, 2012. For the reasons set forth below, Wey's motion is GRANTED.

I. Background

A. The Indictment

Wey is charged in an eight-count indictment returned on September 8, 2015. Dkt. No. 2 (the "Indictment"). The Indictment alleges that between approximately 2007 and 2011, Wey, along with co-Defendant Seref Dogan Erbek (who remains at large) and unindicted co-conspirators known and unknown, orchestrated a scheme whereby Wey—through various non-party entities, family members, and associates (the "Nominees")—covertly amassed beneficial ownership of substantial portions of the equity stock of certain publicly traded companies (the "Issuers"), manipulated the market price of the Issuers' stock, liquidated his holdings at artificially inflated prices, and then laundered millions of dollars in ill-gotten proceeds. *See, e.g.,* Indictment ¶¶ 7, 13, 18–22.

Specifically, according to the Indictment, Wey secretly caused the Nominees to acquire, on his behalf, substantial portions of the shares of certain U.S.-based over-the-counter-traded shell companies and then, ***360** through his consulting firm New York Global Group, Inc. ("NYGG") and its alleged affiliate in Beijing, China, facilitated so-called "reverse merger" transactions by which China-based operating companies merged into those shell companies, thus forming new publicly traded corporations—the Issuers. *Id.* ¶¶ 8–12. The Government alleges that the Nominees acquired and retained, for Wey's benefit, stock in the Issuers by virtue of their ownership of the target shell companies, and that these holdings together constituted more than five percent of the Issuers' outstanding shares. *Id.* ¶¶ 7, 13. Because Wey, among other things, purportedly exercised investment authority over the shares held by the Nominees, he was required to disclose his beneficial ownership under Section 13(d) of the Securities Exchange Act of 1934 and Rule 13d–1 promulgated thereunder within ten days of the acquisition of shares in excess of five percent. *Id.* ¶ 13.

The Government alleges that Wey was "well aware" of this reporting requirement but intentionally failed to file the required disclosures in order to conceal his ownership from the investing public. *Id.* ¶ 14.

Wey also, according to the Indictment, caused several of the Issuers, including SmartHeat, Inc. ("SmartHeat"), Deer Consumer Products, Inc. ("Deer"), and Clean Tech Innovations, Inc. ("CleanTech"), to apply for listings on the Nasdaq. *Id.* ¶ 15. In order to secure approval of these applications, Wey allegedly engaged in deception to artificially satisfy Nasdaq's so-called "round-lot" shareholder requirement—i.e., the requirement that every listed issuer has at least 300 shareholders each owning 100 or more shares of common stock. *Id.* ¶¶ 16–17. In particular, Wey purportedly facilitated deceptive transfers of shares of Issuer stock from Nominees to other Wey confederates, as well as issuances of round-lot blocks of shares in the names of individuals who never actually received such shares or were otherwise unaware of their ownership. *Id.* ¶¶ 15–17.

After successfully getting the Issuers listed on Nasdaq, the Government alleges, Wey proceeded to manipulate the demand for and price of Issuer stock. This was purportedly accomplished by, among other things: (i) causing Manhattan-based retail brokers to solicit their customers to purchase common stock of the Issuers, often on margin, while at the same time actively discouraging the sale of such stock; (ii) instructing Erbek to maintain the share prices of certain Issuers' stock held in various Nominees' accounts; and (iii) facilitating match trades in the Issuers' stock involving Nominees and/or other Wey confederates. *Id.* ¶¶ 18–19.

Contemporaneous with this market manipulation scheme, the Government alleges, Wey caused certain Nominees to sell shares of the Issuers' stock at artificially inflated prices. *Id.* ¶ 20. Wey then purportedly laundered the proceeds of these sales by causing them to be transferred from accounts located in the U.S. to Nominees' accounts located overseas, including in Switzerland and Hong Kong, before being repatriated back to the U.S. and into accounts controlled by Wey and his wife or otherwise held for Wey's benefit. *Id.* ¶¶ 20–22.

Wey is charged with one count of conspiracy to commit securities fraud and wire fraud under 18 U.S.C. § 371; one count of securities fraud under Section 10(b) of the Exchange Act and Rule 10b–5 promulgated thereunder, 15 U.S.C. §§ 78j(b) & 78ff, 17 C.F.R. § 240.10b–5; one count of securities fraud under 18 U.S.C. § 1348; one count of wire fraud under 18 U.S.C. § 1343 ("Count Four"); two counts —concerning Deer and CleanTech stock, respectively—of failure to disclose ***361** ownership in excess of five percent of a covered class of equity securities under Section 13(d) of the Exchange Act and Rule 13d–l, 15 U.S.C. §§ 78m(d) & 78ff, 17 C.F.R. § 240.13d–l; one count of money laundering under 18 U.S.C. § 1956(a)(l)(B)(i); and one count of money laundering under 18 U.S.C. § 1956(a)(2)(A). *See* Indictment ¶¶ 23–40.

B. The Search Warrant Affidavits

1. Affidavit Concerning NYGG's Offices

On January 24, 2012, Special Agent Matthew F. Komar of the Federal Bureau of Investigation ("FBI") swore out an affidavit in support of an application for a warrant to search NYGG's Manhattan offices located at 40 Wall Street, Suite 3800. *See* July 8, 2016 Declaration of Matthew F. Komar Ex. 1, Dkt. No. 54–1 (the "Komar Affidavit" or "Komar Aff."). The Komar Affidavit described an ongoing FBI investigation of Wey, Wey's sister (a Chinese citizen apparently employed by NYGG or its purported Beijing-based counterpart), and NYGG itself—which it characterized as a "corporate advisory firm" founded by Wey in approximately 2004 that specialized in "introducing middle-market Chinese operating companies to the U.S. capital markets." *See, e.g.,* Komar Aff. ¶¶ 2–7, 16. It asserted that there was probable cause to believe that fruits, instrumentalities, and evidence of violations of the federal securities, mail, and wire fraud laws were located within the subject premises. *See, e.g., id.* ¶¶ 2–7.

Based on the investigation to date, including information obtained from current and former NYGG employees, the Komar Affidavit detailed a suspected "fraud and market manipulation scheme" perpetuated by Wey, acting through NYGG and other entities. *See, e.g., Id.* ¶¶ 4–14. Komar's description of the purported scheme broadly tracked, in substantial measure, the allegations set forth in the Indictment and discussed above. As outlined in the Komar Affidavit, the scheme involved Wey retaining undisclosed beneficial ownership of Issuers created through reverse merger transactions facilitated by NYGG and then artificially inflating the Issuers' round-lot shareholder bases to secure

Nasdaq listings and manipulating demand for the Issuers' stock by encouraging a "a hand-picked team of retail stock brokers" to "aggressively solicit purchases" of the Issuers' securities. Wey would then, according to the Affidavit, effectuate the sale of Nominee-held shares at inflated prices and launder the proceeds, including through fund transfers to Wey's wife. *See, e.g., id.* ¶¶ 8–14, 18–29.

Notwithstanding its length, the Komar Affidavit is notable for its focus on Wey's connection to a handful of specific companies. Like the Indictment, the Komar Affidavit principally addressed SmartHeat, Deer, and CleanTech. *Id.* ¶¶ 11–12, 18–20, 35–36. With respect to SmartHeat and Deer, the Affidavit discussed particular purported misrepresentations made by the Issuers, and by Wey, to Nasdaq in the course of the listing application process and described serial transactions by which Wey allegedly inflated the Issuers' round-lot shareholder bases in 2008 and 2009. *Id.* ¶¶ 18–19. It further set out alleged market manipulation tactics undertaken in 2009 through 2010 by the broker group over which Wey purportedly exercised influence, including improper high-pressure promotion of Issuer securities and misrepresentations concerning the future value of the stocks. *Id.* ¶¶ 20–25. A $350,000 kickback allegedly paid to the broker group in connection with its promotion of Deer, at least, was described in some detail. *Id.* ¶ 26. The Affidavit also discussed, to some extent on a transaction-level basis, the ***362** Nominees' sales, in 2009 and 2010, of large blocks of Issuer shares at purportedly inflated prices and the wiring of the sale proceeds to accounts linked to Wey confederates and family members in Switzerland and Hong Kong and, ultimately, back to the U.S. *Id.* ¶¶ 27–29.

As to CleanTech, the Affidavit described Wey's purported facilitation in 2010 and 2011 of the placement of Issuer stock with individuals and entities formerly used as Nominees with respect to Deer and SmartHeat. *Id.* ¶ 36. It also identified documents allegedly demonstrating Wey's indirect control over CleanTech, and discussed Nasdaq's decision to delist CleanTech based on its alleged failure to disclose materials revealing its financial connection to Wey.[1] *Id.* The Affidavit further recounted information from an FBI source within NYGG suggesting that Wey facilitated CleanTech management's preparation of inflated revenue forecasts, and identified a pattern of active trading in CleanTech stock by Wey's alleged retail broker team. *Id.*

Of note, the Komar Affidavit also identified by name dozens of individuals and entities potentially involved, directly or indirectly, in Wey's suspected schemes. These included, among others, the U.S.-based broker-dealer team purportedly working at Wey's direction and several firms at which its members were employed, senior employees of the Issuers, suspected Nominees and other Wey associates and family members in both the United States and China, and NYGG personnel. *Id.* ¶¶ 12, 14, 18–19, 24, 26–29, 33, 36.

The Affidavit also connected Wey, more briefly, to several other specific companies of evident interest to the Government. It described, for example, Wey's and NYGG's facilitation of a reverse merger transaction involving Bodisen Biotech, Inc., as well as that company's subsequent delisting by the then-American Stock Exchange for, among other things, failure to properly disclose its relationship with and payments to NYGG. *Id.* ¶ 17. It also recounted Wey's alleged involvement in an accounting fraud scheme perpetuated by AgFeed Industries, Inc., a publicly-traded company born of another reverse merger transaction purportedly facilitated by Wey, and large-scale sales of AgFeed stock by investors believed to be Wey Nominees. *Id.* ¶¶ 30–34. Finally, the Affidavit asserted that Wey exercised undisclosed control over Nova Lifestyle, Inc. (yet another product of a Wey-linked reverse merger transaction), that he wielded that control to effectuate share transfers to Nominees, and that he directed NYGG employees to improperly solicit purchases of the company's stock. *Id.* ¶ 37.

In addition, the Komar Affidavit included a short section devoted to Wey's personal background and alleged history of participating in fraudulent activities, including within the securities industry. It asserted, among other things, that Wey was sanctioned by both the Oklahoma Department of Securities and then-National Association of Securities Dealers based on misconduct during Wey's time working as a registered investment adviser in Oklahoma in the mid to late 1990s and early 2000s. It further averred that Wey engaged in various forms of tax and other financial fraud and forgery during roughly the same period. *Id.* ¶ 15.

Based on these submissions, and as discussed further below, the Komar Affidavit formally requested permission to seize from NYGG's offices twelve expansive ***363** categories of materials set forth on an appended exhibit, with the limitation

that the materials concern at least one of an independently appended list of approximately 220 named individuals and entities believed to be in some way connected to Wey's purported scheme. *Id.* ¶¶ 35, 38–42, 46–47, Exs. A–B. It also sought court approval to seize, copy, and/or digitally image computers and related electronic equipment believed to contain such materials and to conduct offsite searches of the devices' contents. According to the Komar Affidavit, in view of the highly technical and specialized procedures and substantial time investment required to effect thorough searches of the potentially voluminous data contained within this equipment—including deleted, concealed, or encrypted files—and extract relevant material while maintaining the integrity of the evidence, it would in many cases be impractical, if not impossible, to effectively do so onsite. *Id.* ¶¶ 43–47, Ex. C. As such, the Affidavit attached a third exhibit setting forth a proposed methodology for reviewing and seizing such equipment and, if necessary, executing offsite searches. *Id.* Ex. C.

2. Affidavit Concerning Wey's Residence

As discussed further below, during the course of the Government's search of the NYGG offices the following day, it decided to apply for a warrant to search the Manhattan apartment that Wey shared with his wife, Michaela, and their children (the "Wey Apartment"). Accordingly, on January 25, 2012, Special Agent Keith Garwood of the FBI swore out another affidavit. *See* July 8, 2016 Declaration of Matthew F. Komar Ex. 4, Dkt. No. 54–4 (the "Garwood Affidavit" or "Garwood Aff"). The Garwood Affidavit—which relied heavily upon and expressly incorporated by reference the Komar Affidavit—explained that FBI personnel had interviewed NYGG employees during the search of the firm's offices earlier that day and learned that Michaela Wey served as NYGG's "office manager" and "bookkeeper" but generally worked out of the Wey Apartment, where she would, among other things, perform accounting and payroll functions and mail checks. Garwood Aff. ¶¶ 2, 7–11. It also cited assertions in the Komar Affidavit that Wey caused certain Issuer stock certificates for new round-lot shareholders to be sent to the Wey Apartment, that certain Nominees had wired substantial sums of money to accounts held in the name of Michaela Wey, and that Michaela Wey had once been listed in an SEC filing as an executive officer of NYGG. *Id.* ¶¶ 6, 9, 12.

Based on that information, the Garwood Affidavit urged that there was probable cause to believe that fruits, instrumentalities, and evidence of securities, mail, and wire fraud would be found within the Wey Apartment and sought permission to seize from the Apartment substantially the same categories of materials, pertaining to substantially the same individuals and entities, listed in the Komar Affidavit. Garwood Aff. ¶ 4, 13–16, 20, Exs. A–B. It also sought approval of substantially the same protocol as that proposed in the Komar Affidavit for searching computers and related equipment offsite, citing similar practicality concerns. *Id.* 17–20, Ex. C.

C. The Search Warrants

1. The NYGG Warrant

United States Magistrate Judge Michael H. Dolinger approved the Government's application with respect to the NYGG offices and issued a corresponding search warrant on January 24, 2012. *See* May 27, 2016 Declaration of David Siegal ("Siegal Dec.") Ex. 8, Dkt. No. 46–9 (the "NYGG Warrant"). The NYGG Warrant identified the premises to be searched as "[t]he office ***364** of [NYGG] at 40 Wall Street, 38th Floor, Suite 3800, New York, New York, and any closed or locked cabinets, briefcases, and other containers kept therein, including computers and electronic storage devices, excluding the individual office of James Baxter, Esq." *Id.* Ex. A.

The property to be seized pursuant to the NYGG Warrant was defined through the interplay between two attached exhibits (both of which had originally been included in the Government's application in substantially identical form). Specifically, Exhibit A to the NYGG Warrant set forth, by category, the types of materials subject to seizure along with illustrative lists, and imposed the additional requirement that the actual materials to be seized relate in some way to at least one of a list of individuals and entities included in Exhibit B. The scope of Exhibit A is best illustrated by reproducing it in full, with top-line categories emphasized relative to their non-exhaustive supporting lists, as applicable:

1. **Financial records concerning the individuals and entities listed in Exhibit B** ... including banking and brokerage firm account statements, checks, and transactions records, wire transfer instructions and similar documents concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

2. **Personal financial records of any individuals named in Exhibit B or of any employees, agents, or shareholders of any of the entities listed in Exhibit B,** including banking and brokerage firm account statements, checks, and transaction records, wire transfer instructions and similar documents concerning or reflecting movements of funds, account and account holder information, check numbers, account numbers and Federal Reserve routing numbers;

3. **Telephone bills, telephone message pads, notes, memoranda and other records of internal and external communications between, among, or relating to any of the individuals and entities listed in Exhibit B;**

4. **Correspondence, audio tapes, and video tapes concerning any of the individuals and entities listed in Exhibit B;**

5. **Hotel, airline and credit card receipts reflecting the dates and locations of meetings or travel to meetings concerning any of the individuals and entities listed in Exhibit B;**

6. **Photographs, address books, Rolodexes, diaries, income tax returns and calendars concerning the operations and management of any of the individuals and entities listed in Exhibit B;**

7. **Computers, flash drives, internal and external hard drives, diskettes and other magnetic storage media, and files, data and information contained thereon, used to store names, telephone numbers and addresses, and other information,** including but not limited to personal digital assistants such as iPhones, iPads, Blackberrys, smartphones, and cellphones, as well as drafts and final versions of documents and correspondence, used by, or used in connection with the individuals and entities listed in Exhibit B....;

8. **Marketing materials relating to any of the individuals and entities listed in Exhibit B,** including offering materials, private placement memoranda, sales scripts, investor "lead" lists, investment agreements, financial statements, and other documents concerning, ***365** [or] relating to, the purchase or sale of securities;

9. **Documents identifying shareholders or investors in the entities listed in Exhibit B,** including transfer agent records, stock certificates, investor lists, investor files, investment subscription agreements, copies of checks received from or sent to investors, copies of account statements sent to investors, copies of correspondence sent to or received from investors, Federal Express, DHL or other records reflecting mailings by private commercial carriers and the U.S. Postal Service, and other documents concerning or reflecting the identities and participation of investors in such schemes;

10. **Documents reflecting the ownership by the individuals and entities listed in Exhibit B of real properties and personal property purchased with the proceeds of fraud,** including but not limited to houses, apartments, cars, boats, and jewelry, including purchase and sale agreements, deeds, mortgage documents, and other real estate or other property closing documents;

11. **Identification documents and other documents which may reflect the identities of persons listed in Exhibit B or persons affiliated with the entities listed in Exhibit B**; and

12. **Corporate documents reflecting the ownership or structure of, or relationship between and among, any of the entities listed in Exhibit B,** including incorporation documents, inter-company agreements, lists of partners and stockholders, organizational charts, and corporate resolutions and bylaws.

NYGG Warrant Ex. A.

Exhibit B to the NYGG Warrant, in turn, named the same approximately 220 individuals and entities identified in Exhibit B to the Komar Affidavit. Of great significance, the list included among its first two entries NYGG itself (whose offices, of course, would be the subject of the search) and Wey himself. *See* NYGG Warrant Ex. B. Reading Exhibits A and

B together, then, the NYGG Warrant authorized the seizure from NYGG's offices of, for example, all "financial records," "internal and external communications," "correspondence," and other things concerning NYGG.

Beyond the requirement that the materials subject to seizure relate to at least one of the Exhibit B individuals/entities, the NYGG Warrant imposed no substantive limitations. It did not specify the crimes under investigation, whether by statutory citation or otherwise, or discuss any particular conduct of interest. It did not set out any date ranges or other timeframe-based criteria. Importantly, the NYGG Warrant also did not attach, incorporate, or otherwise expressly reference the Komar Affidavit.

With respect to any "computers, computer-related equipment, and other electronic devices" found on the premises, the NYGG Warrant provided that the FBI would employ substantially the same search and seizure methodology proposed in the Komar Affidavit, which it described in another attached Exhibit (essentially, a copy of Exhibit C to the Komar Affidavit). *See* NYGG Warrant Exs. A, C. That methodology contemplated, in sum and substance, that FBI personnel trained in searching and seizing computer data would conduct an initial onsite review of any such items. *Id.* Ex. C. If a determination were made that a given item could not be searched onsite "within a reasonable amount of time and without jeopardizing the ability to preserve data," then the FBI could either (i) copy its data for offsite review (if the device were found not to contain contraband) or (ii) seize the device ***366** for transportation to a law enforcement laboratory for offsite review (if the device were found to contain contraband or onsite data review or copying would be impractical). *Id.* In searching these items or their copies, the FBI would be permitted "to examine all of the data contained" but only "to view their precise contents and determine whether the data falls within the items to be seized as set forth" elsewhere in NYGG Warrant. *Id.* In other words, the procedures for searching computer equipment and electronic devices did not purport to expand or restrict the scope of the materials subject to seizure; rather, data from these items could ultimately be seized only if it fell within the "strictures"—such as they were—of Warrant Exhibits A and B. During these searches, the FBI would be required to "have procedures in place to segregate any potentially privileged materials or files." *Id.* If it were determined that any confiscated devices were "no longer necessary to retrieve and preserve the data" and that the "items [were] not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(b)," the Government would be required to "return these items, upon request, within a reasonable period of time." *Id.*

2. The Wey Apartment Warrant

Magistrate Judge Dolinger also approved the Government's application to search the Wey Apartment, issuing a warrant on January 25, 2012 (during the course of the Government's search of the NYGG offices, as discussed further below). *See* Siegal Dec. Ex. 24, Dkt. No. 46–25 (the "Apartment Warrant"). Other than its description of the premises to be searched, the Apartment Warrant was substantially identical in all material respects to the NYGG Warrant, right down to its incorporation of copies of the same three Exhibits. *Id.* & Exs. A–C. Of particular note in the context of the forthcoming search of the Wey Apartment, Exhibit B (the list of relevant individuals and entities) included not only Wey himself but also Michaela Wey. Thus, the Apartment Warrant authorized the seizure from the Wey Apartment of, for example, all "financial records," "internal and external communications," "correspondence," "photographs," "audio tapes," and "video tapes" concerning either of the Apartment's two adult occupants.

D. The Searches

After Wey filed the instant suppression motion, the Court made a preliminary determination that a hearing was warranted to address whether the Government acted in good faith in executing the NYGG Warrant and the Apartment Warrant and whether the Government acted reasonably and in good faith in executing off-site searches of computers and computer-related equipment recovered during the execution of the Warrants. Dkt. No. 69. Accordingly, the Court conducted a two-day suppression hearing on January 23 and January 24, 2017 (the "Hearing"), at which it heard live testimony from former Assistant United States Attorney David Massey, Special Agent Komar, Special Agent Thomas McGuire, Special Agent Elizabeth Miller, forensic examiner and information technology specialist Brian Booth. [2]

What follows for the remainder of this Opinion constitutes the Court's findings of fact and conclusions of law. They are

based upon the evidence taken at the hearing—with ***367** the benefit of supplemental post-hearing briefing and oral argument—as well additional evidentiary submissions by the parties in support of their original and supplemental briefs.

1. Preparation for the NYGG Search

The Government's investigation into Wey and NYGG was already at least several months old when the Government applied for the NYGG Warrant on January 24, 2012. Hearing Tr. 30:11–14. The investigation was led, during that period of time, by Agent Komar and then-AUSA David Massey. Hearing Tr. 14:16–20, 29:9–12, 120:11–15. AUSA Massey testified that the decision to apply for the NYGG Warrant was made "at least" several weeks—and "perhaps" even months—before the Government submitted its application. *Id.* at 30:23–31:4.

In preparation for the Government's search of the NYGG offices, Agent Komar prepared an "operations order form" for circulation to the FBI search team (the "Operations Order"), which was comprised of approximately twenty agents predominantly from the C–43 securities fraud squad and/or the Computer Analysis Response Team ("CART"), along with personnel from the FBI's photography unit. Hearing Tr. 119:21–120:2, 122:10–123:16, 185:18–186:5, 236:22–237:4; Gov't Exs. 1 (Operations Order), 5 (FBI Crime Scene Sign–In Log for Search of NYGG). The Operations Order contained a "synopsis of the case," authored by Komar, which asserted that there was probable cause to believe that Wey, acting through NYGG, had "committed securities fraud and manipulated the market for the securities of various small-capitalization issuers." Hearing Tr. 122:25–123:4; Gov't Ex. 1 at 1. The Operations Order then proceeded to outline in a brief paragraph the basic contours of the suspected scheme, substantially consistent with the Komar Affidavit:

> Wey introduces Chinese companies to the U.S. markets and arranges reverse mergers and assists these companies [in] get[ting] listed on markets such as Nasdaq. It appears he has artificially inflated the number of round-lot shareholders for the purpose of meeting listing requirements. Wey then retains undisclosed beneficial ownership and/or control of large blocks of shares of the Chinese companies that are held in the name of nominees. Wey creates an artificial demand for the securities by working directly with a hand-picked team of retail stock brokers ... to aggressively solicit purchases of the Chinese companies' securities. Once the artificial demand is created and the stock price goes up, Wey sells the large block of nominee held shares.

Id. In a separate section, the Operations Order described the forthcoming operation as a search "for documents related to Wey assisting Chinese reverse mergers [to] falsify their records to meet listing standards for Nasdaq" and "control[ing] the trading volume in these Chinese companies, through a number of associated broker dealers." *Id.* at 5. The Operations Order did not reference or name any of the specific Issuers implicated in Wey's alleged scheme. Nor did it discuss any of the entities or individuals listed on Exhibit B to the NYGG Warrant (apart from NYGG and Wey) or explain their purported connections to the suspected criminal activities.

Late in the afternoon of January 24, 2012—the same day that the NYGG Warrant issued and the day before it was to be executed—Agent Komar and AUSA Massey conducted a pre-operation briefing attended by all members of the FBI search team. Hearing Tr. 15:6–16:3, 122:1–4, 123:19–124:–2. The briefing lasted approximately 45 minutes to an hour. *Id.* 240:24–25. ***368** During the briefing, AUSA Massey explained the nature of the scheme under investigation, using the Komar Affidavit as a reference, and described the "types of documents" that the team would be "looking for." *Id.* 68:25–71:17, 124:11–15; 239:7–21. Agent Komar summarized "some parts" of the investigation to date but primarily briefed the team on operational logistics for the coming search. *Id.* 124:19–23. Special Agent Thomas Maguire—who attended the briefing, participated in the search of the NYGG offices, and later took over for Agent Komar as the case agent on the Wey investigation

—characterized the briefing as providing a "big-picture overview" of what was presented as a "fairly typical securities fraud case." *Id.* at 239:17–21.

At the Hearing, Agent Komar could not recall any instructions or guidance provided to the search team as to any sorts of items that should *not* be seized during the forthcoming search. *Id.* 190:13–16. The team was instructed, however, that the office of NYGG's in-house legal counsel was off-limits and could not be searched during the operation. *Id.* 239:22–240:2.

Also during the pre-search briefing, Agent Komar shared copies of the Operations Order with each member of the search team, and communicated to the team that the NYGG Warrant and the Komar Affidavit were "available" if anyone would like to review them personally. *Id.* 123:15–16, 125:2–126:6, 240:6–22. There is no credible evidence, however, that any agent other than Komar himself did in fact review the Komar Affidavit in advance of the search. Agent Komar testified that he "did not hand out copies" of the Komar Affidavit to the team, and "did not make sure every single person read" it. *Id.* 125:13–126:4. In addition, while Komar first testified at the Hearing to his vague belief that he at some point e-mailed the Komar Affidavit to members of the FBI team, subsequent searches by the Government identified no such e-mail communications. *Id.* 125:13–22, 228:14–230:4. AUSA Massey, for his part, expressed "doubt" that he read any portion of the Komar Affidavit directly to the search team. *Id.* 68:25–71:17. Agent Komar testified generally that at least one (unidentified) member of the search team did in fact review some portion of the Komar Affidavit; AUSA Massey, on the other hand, had no such recollections. *Id.* 68:25–71:17, 126:5–7, 185:12–20. The Government called no witnesses —other than Komar himself—who could definitively testify that they personally reviewed the Komar Affidavit prior to the search operation, and the Court cannot find that any such review took place.

Agent Komar conceded at the Hearing that the planned search of the NYGG offices could have been scheduled on any date up to 10 days after the briefing to afford all members of the search team an opportunity to review the Komar Affidavit, but that the FBI elected to go forward with the search the following morning. *Id.* 186:6–25.

2. Search of NYGG Offices

On the morning of January 25, 2012, the search team assembled for a final pre-operation briefing at the FBI's Manhattan offices to discuss logistics for the search. Hearing Tr. 126:10–16. AUSA Massey did not attend that meeting. *Id.* 126:17–18.

The search of the NYGG offices (the "NYGG Search") began shortly before 9:30 AM. *Id.* 126:19–127:1; Gov't Ex. 5. NYGG's suite consisted of an outer reception area surrounded on two sides by approximately nine individual offices, conference rooms, and a kitchen, together forming an "L" shape. Gov't Ex. 4 (NYGG Office Layout Diagram); Hearing Tr. 243:13–16. Wey and all other NYGG employees present in the office when the ***369** NYGG Search began were gathered into one of the conference rooms by FBI personnel and interviewed briefly to obtain basic contact information and background on their roles at NYGG. Hearing Tr. 127:4–9, 131:21–132:8, 243:18–23. Members of the FBI search team had copies of the NYGG Warrant, including its attachments, with them onsite, *id.* 127:23–25, 244:13–18, but there is no evidence that anyone other than Komar himself had a copy of the Komar Affidavit. Neither Wey nor any other employee on the scene was provided with a copy of the Komar Affidavit. *Id.* 46:8–17.

Agent Komar, serving as the team leader, personally searched the reception area in the outer portion of the office and then remained in that area, ostensibly to field any questions from other agents. Although Komar himself testified generally that team members asked him questions on several occasions, he recalled only one specific inquiry as to whether a particular document fell within the scope of the NYGG Warrant. *Id.* 128:1–19, 130:7–131:6, 132:9–10. The Government presented no other evidence at the Hearing suggesting that the searching agents addressed questions to Agent Komar. The Court is likewise aware of no evidence that Agent Komar in any way directly supervised, reviewed, or spot-checked the team's seizure decisions.

AUSA Massey was not onsite during the NYGG Search but communicated during the course of the Search with, at least, Agent Komar. *Id.* 16:4–8. At the Hearing, AUSA Massey could not recall having any discussions with Agent

Komar or his team as to whether particular items fell within the scope of the NYGG Warrant, and agreed that it was generally up to the searching agents' "discretion" to make any such determinations. Hearing Tr. 67:18–68:20. From his own perspective, AUSA Massey testified, "all records of [NYGG] ... were in play," *id.* 14:8–10, largely because the Government "needed to understand the entire business, even if some part of the business was legitimate," in order to properly assess its role as a source of income to Wey, *see, e.g., id.* 36:1–12 (citing Government's suspicion that Wey was "making way too much money to be accounted for by [NYGG's advisory fees])." When pressed to cite any types of materials *not,* in his view, covered by the NYGG Warrant, AUSA Massey offered only medical prescriptions, illegal drugs and paraphernalia, child pornography, and terrorist manifestos. *Id.* at 47:17–48:10. (Although Massey also later testified that he would deem "a bag of heroin ... found on the premises" that "said New York Global Group" on it "within the scope of the warrant." *Id.* 50:13–16.)

Approximately twelve or thirteen of Komar's colleagues conducted the physical searches of NYGG's individual offices and other rooms. *See, e.g., id.* 127:10–22, 243:24–244:9; Gov't Ex. 1; Gov't Ex 5. Of these agents, only Agent McGuire testified at the Hearing. Agent McGuire recalled personally searching one of NYGG's "larger" individual offices and deciding whether to seize documents by comparing their contents to the list of individuals and entities set forth in Exhibit B to the NYGG Warrant (which, of course, included NYGG itself). He testified that, while it was possible that he sought a second opinion from another agent on the search team at some point, he did not recall "coming across documents where [he] had a difficult time determining whether it was covered by the search warrant." *Id.* 243:17–247:23. Asked whether he remembered deciding *not* to seize any particular materials, Agent McGuire testified that he recalled determining that a set of resumes belonging to people who were apparently applying for jobs at NYGG were "not pertinent to the ***370** investigation." *Id.* 245:18–248:19. He also testified that he made that determination without consulting any of his colleagues, agreeing that it was a "clear decision" that such documents were "not responsive." *Id.* 298:13–299:1. Notwithstanding Agent McGuire's conclusion, resumes of NYGG applicants (whose names did not appear in the NYGG Warrant or Komar Affidavit) were in fact seized during the course of the NYGG Search. *See, e.g.,* Supplemental Memorandum of Law in Support of Defendant Benjamin Wey's Motion to Suppress, Dkt. No. 95 ("Def. Supp. Br.") Ex. B.

According to Agent Komar, the total volume of paper records found in the NYGG offices was—consistent with the Government's expectations going in—less than substantial. *Id.* 133:14–134:13. He testified that the team had sufficient time during the NYGG Search to review essentially every page of every document found, and estimated that, in total, the team ultimately seized approximately 4,500 pages of hard-copy documents. *Id.; see also* Gov't Ex. 6 (Evidence Recovery Log from NYGG Search noting seizure of approximately thirteen redwelds, boxes, envelopes, and discs). Komar personally recovered only one redweld of documents; the balance was seized by other members of the search team. Gov't Ex. 6. Asked at the Hearing to compare the hard-copy search fruits to the overall volume of paper records found or reviewed, Agent Komar could not provide specifics but testified: "We didn't take every single piece of paper, but there really wasn't much paper to start with either." Hearing Tr. 134:5–13.

Computer equipment and electronic devices found during the NYGG Search were assessed by CART personnel to determine whether onsite searches or data copying would be feasible. *Id.* 134:14–135:13. The team ultimately deemed these options impractical with respect to the vast majority of the items. *Id.; see also* Gov't Ex. 7 (CART On–Site Search Form for NYGG Search). With the exception of Wey's cell phone, which the search team seized, CART personnel copied or digitally imaged the cell phones of all NYGG employees present in the office during the NYGG Search. The balance of the electronic materials found, however, including all laptop computers, flash drives, and hard drives from desktop computers, were seized for offsite review. Hearing Tr. 134:14–135:13, 175:22–177:6; Gov't Ex. 7. In total, the team copied or seized approximately 24 pieces of computer or other electronic equipment. Gov't Ex. 7. With respect to NYGG employees' cell phones, at least, the search team did not make any onsite determination as to whether the devices related in any way to the individuals and entities set forth in Exhibit B to the NYGG Warrant; rather, the cell phones of all those present in the office were indiscriminately imaged (or seized) for later review. Hearing Tr. 176:2–6.

The NYGG Search lasted approximately four to five hours, concluding shortly before 3:00 PM. Hearing Tr. at 181:7–9; Gov't Ex. 5.

3. Search of Wey Apartment

At the time it applied for the NYGG Warrant, the Government had reason to believe, at least, that stock certificates potentially implicated in Wey's purported scheme had at some point been sent to the Wey Apartment. Hearing Tr. 181:24–l 82:11 (Agent Komar acknowledging that the Komar Affidavit asserted as much). It did not, however, seek a search warrant for that location until the NYGG Search was in progress. *Id.* As alluded to above, at some point during the "early stages" of the NYGG Search, Agent Garwood of the FBI learned from interviews of NYGG employees that Michaela Wey served as NYGG's bookkeeper and office manager and generally ***371** completed her work from the Wey Apartment. Hearing Tr. 16:15–25, 135:14–24, 182:8–11. Upon receiving that additional information and with the NYGG Search having turned up none of the stock certificates of interest, AUSA Massey, along with Agent Garwood, drafted the Garwood Affidavit and applied for the Apartment Warrant. Hearing Tr. 17:1–18, 135:25–136:5, 181:10–183:23.

With the application process in motion, Agent Komar instructed FBI personnel, including several agents already onsite at the Wey Apartment, to serve grand jury subpoenas on Michaela Wey, to secure the exterior of the Wey Apartment in order to ensure that no evidence would be removed or discarded. Hearing Tr. 136:6–13, 138:15–20, 253:9–254:7; Def. Ex. 16 (February 22, 2012 Memorandum of Agent Komar). The Court is aware of no evidence, however, that Komar or anyone else had any basis to believe that such activities were likely to take place.

After the Apartment Warrant issued, FBI personnel entered the Wey Apartment at approximately 4:30 PM and commenced a search (the "Apartment Search"). Hearing Tr. 138:8–24, 254:8–18; Gov't Ex. 12 (FBI Crime Scene Sign–In Log for Apartment Search); Def. Ex. 16. Ultimately, approximately seventeen FBI agents participated in the Apartment Search in some capacity. Gov't Ex. 12. Most, but not all, of these individuals had also participated in the NYGG Search. *Compare* Gov't Ex. 5 *with* Gov't Ex. 12. No pre-operation briefing was conducted in advance of the Apartment Search. Hearing Tr. 300:18–20. There is also no evidence that any operations order or similar document was prepared to help guide the team in executing that Search.

Agent McGuire, who conducted an initial walkthrough at the outset of the Apartment Search, testified that he "briefly" reviewed the Apartment Warrant before beginning the Apartment Search. *Id.* 254:12–25, 257:2–9. He did not, however, review the Garwood Affidavit, and testified that he was not aware of any FBI personnel possessing a copy of the Garwood Affidavit during the course of the Apartment Search. *Id.* 301:3–10. Agent McGuire testified repeatedly that, to his understanding at least, the team was authorized to seize from the Wey Apartment, among other things, "any record we would find related to [Wey] finances," regardless "of date or time frame." Hearing Tr. 276:12–20, 304:11–14, 306:18–19.

Once again, Agent Komar, who arrived on the scene at approximately 4:50 PM, functioned as the team leader during the Apartment Search. Hearing Tr. 138:25–139:1; Gov't Ex. 12. And once again, Agent Komar testified generally at the Hearing that he was asked unspecified questions by unnamed agents about whether unidentified documents were "relevant to the search warrant." Hearing Tr. 139:2–139:10. As in the context of the NYGG Search, however, the Government called no members of the search team who could testify to having consulted Komar with respect to seizure decisions.

Within the Wey Apartment, the search team identified one "office area" with a "large amount of documents," but otherwise did not locate any rooms with a "substantial" number of hard-copy documents. Hearing Tr. 139:5–140:3. Agent Komar personally assisted in searching "what appeared to be a guest room" and the rooms of Wey's children and then "focused [the team's] attention on the office area." *Id.* 139:14–25. AUSA Massey, once again, was not onsite for the Apartment Search, but did communicate with unidentified agents conducting the search by phone and e-mail. Hearing Tr. 19:13–16.

***372** During the course of the Apartment Search, the search team did not review every document that it encountered. Instead, the searching agents would "flip through" any given box or other container to see if it contained at least a "subset" or "sampl[e]" of relevant documents, and, if so, they would

seize the entire container. *See* 146:5–147:9, 155:2–156:21 (Agent Komar also describing the process as allowing the team to "get a little bit of comfort" that it was not seizing documents "outside of the scope" of the Apartment Warrant). At the Hearing, Agent Komar attributed that strategy to "the sense of urgency" purportedly created by the FBI's desire not to "disrupt someone's life," especially with the Weys' children apparently expected back at the Wey Apartment sometime in the late afternoon or early evening. *Id.* Agent McGuire likewise testified that Michaela Wey "was upset about th[e] search and ... very concerned about her kids coming soon," and that, "towards the end of the search there was some tension because she wanted the search to wrap up" and the agents "out of her apartment." *Id.* 255:5–9, 257:13–20. To address the concerns about the children, Agent McGuire and his colleagues ordered the Apartment Search to target the children's bedrooms and play area first, so that the children could be "segregated" from the search of the remainder of the Wey Apartment's rooms once they returned home with their nanny. *Id.* 255:19–256:4.

Ultimately, the search team seized approximately 4,000 hard-copy documents from the Wey Apartment. Komar Dec. ¶ 13. That represented something less than the total number of documents found during the Apartment Search. Hearing Tr. 147:6–9; *see also* Gov't Exs. 15, 15A–15H (FBI entry and exit photographs of Wey Apartment). As cataloged by the FBI, the total hard-copy take from the Wey Apartment consisted of approximately twenty-eight discrete sets of materials, including boxes, redwelds, discs, videos, a suitcase, and other things. Gov't Ex. 13 (Evidence Recovery Log from Apartment Search). As presented to the Court at the Hearing, the hard-copy materials taken from the Wey Apartment partially filled 17 boxes, as well as additional manila envelopes, redwelds, and a suitcase. Hearing Tr. 257:25–261:12. Agent Komar personally recovered only one of these sets of documents. Gov't Ex. 13. Agent McGuire did not participate in the search for "individual items" and did not personally recover anything. *Id.*; Hearing Tr. 257:2–9.

Several documents were seized, at least occasionally in tom or otherwise physically compromised form, from wastebaskets and from a trash bag that was located within the noted suitcase, which itself was found in a hallway closet. Hearing Tr. 142:10–145:4, 155:19–156:21, 160:9–18. The team encountered certain documents in these locations that were intermingled with trash, difficult to decipher, or otherwise "burdensome" to analyze onsite, and responded by removing entire sets of documents for offsite review, pursuant to a decision reached by Agent Komar, his supervisor, and AUSA Massey. *Id.* 142:10–145:4, 155:19–156:21, 160:9–18, 167:21–168:11. Although the FBI later sorted out from these sets certain materials that it deemed beyond the scope of the Apartment Warrant, it maintained custody of those materials and to date has not returned them to the Weys. *Id.* 169:23–170:6.

Documents taken from the Wey Apartment included many of a personal nature, such as pharmaceutical prescriptions and related documents; materials reflecting information on medical appointments and examinations; X-rays of Wey family members; Wey's living will and health care directives; recreational sports schedules; documents, photographs and other mementos ***373** from Michaela Wey's secondary school, collegiate and law school careers; children's scholastic records and test scores; divorce papers from Wey's first marriage dating to the late 1990s; passports belonging to the Weys' children and other apparent family members; family photographs; and photographs of rural landscapes, among other things. *See, e.g.,* Hearing Tr. at 167:4–169:19, 265:24–276:11; Def. Supp. Br. Exs. A, C. During the Hearing, Government witnesses offered post-hoc justifications for some of these seizures that the Court found unpersuasive. For example, AUSA Massey testified that a medical prescription information sheet for the Weys' child would have been within the scope of the Apartment Warrant if it reflected "pricing information" or "cost information" because they could go to the Weys' "personal expenses." Hearing Tr. 55:13–57:7. He also asserted that PSAT scores of the Weys' child would have been seizable if the score report "indicated where he would attend school." *Id.* 58:24–59:5. Additionally, newspaper clippings on Michaela Wey's collegiate tennis career were within the scope of the Apartment Warrant as long as they were found in a file with other documents that showed how the Weys first met in Oklahoma. *Id.* 59:25–60:7. Agent Komar found a document confirming a dentist appointment for Michaela Wey responsive to the Warrants because "Michaela Wey's address is of relevance." *Id.* 167:10–18. Agent McGuire, for his part, characterized divorce records from Wey's prior marriage seizable "if they talk about financial arrangements" because "then they would relate to financial records." *Id.* 304:24–305:5.

With regard to certain other personal documents, Agent McGuire (who was not the individual who made the seizure determinations during the Apartment Search) noted that they were found mixed in boxes or redwelds with financial and other documents that he would have deemed responsive to the Apartment Warrant and explained that seizure of the entire container would be justified to ensure the "integrity" of the documents. Hearing Tr. 265:24–276:11. Still other personal documents—most notably, medical X-rays and related records—were simply conceded by Government witnesses to fall outside the scope of the Apartment Warrant. *See, e.g., id.* 59:6–9, 277:9–19.

Most, if not all, of the electronic devices and computer equipment found within the Wey Apartment, including Michaela Wey's personal cell phone, were seized; any others were copied or imaged onsite. *See, e.g.,* Komar Dec. ¶ 14; Hearing Tr. 178:5–179:15; Def. Ex. 16. By the Court's count, at least 25 devices or pieces of equipment were seized or copied in total, including cell phones, personal computers, laptops, and flash drives. Def. Ex. 14 (in pertinent part, FBI Receipts for Property Received/Returned/Released/Seized from Wey Apartment); Komar Dec. ¶ 14. The FBI's effort to image or copy electronic evidence onsite was at least somewhat more limited than it had been during the NYGG Search earlier that day, in part due to the fact that only one CART agent participated in the Apartment Search—several fewer than had participated in the NYGG Search. Hearing Tr. 178:5–179:15.

The Apartment Search concluded at approximately 9:00 PM. Hearing Tr. 257:10–12; Gov't Ex. 12.

4. Post–Search Developments

a. Retention or Return of Seized Materials

In approximately February 2012, the FBI, at least partially in response to requests from NYGG's and Wey's counsel, copied all electronic devices and computer equipment seized during the NYGG Search and the Apartment Search (together, ***374** the "Searches") and returned either the original devices or images of their data to NYGG and Wey. Komar Dec. ¶ 15; Hearing Tr. 20:23–21:18, 147:13–148:14. In May 2012, counsel further requested in writing the return of all hard-copy materials taken from both locations. *See* Siegal Dec. Ex. 37, Dkt. No. 46–39. Copies of at least some of the hard-copy materials were provided to counsel for Wey and NYGG by the prosecution team sometime in the fall or winter of that year. Komar Dec. ¶ 16; Hearing Tr. 169:23–170:6, 219:10–221:14; Def. Ex. 5 (internal Government e-mail correspondence discussing status of copying effort). The FBI retained custody of—and, to the Court's understanding, does to this day—substantially all original hard-copy materials and all electronic data, regardless of whether it had deemed them responsive to the relevant Warrant. *See, e.g.,* Hearing Tr. 99:12–100:11, 169:23–170:6, 180:11–24, 334:20–335:21.

b. Processing, Review, and Handling of Electronic Materials

After copying the seized electronic devices for return to NYGG and Wey, the FBI CART team processed the digital data and loaded it onto its review platform. *See, e.g.,* Hearing Tr. 21:19–22:6, 148:15–20. Due to the sheer volume of the electronic search take—which Agent Komar estimated to include about eighteen terabytes of data—Agent Komar worked with the CART team to process and load the documents on a rolling basis according to tranches of priority. *Id.* 148:21–149:9.

Based on its understanding that NYGG and/or the Weys could have potential privilege claims with respect to some of this material, AUSA Massey and Agent Komar organized a so-called "taint review" by an FBI wall team to segregate non-privileged from potentially privileged documents in advance of the case team's substantive review of the material. *See, e.g., id.* 22:12–25:13, 82:3–83:10, 149:10–25, 193:25–195:4, 280:1–10. To that end, Massey and Komar compiled—with substantial written input from NYGG's and/or Wey's counsel—a lengthy list of the names and e-mail addresses of attorneys who had at some point represented NYGG or the Weys. *Id.*; Gov't Exs. 17–18 (e-mail correspondence concerning attorney list); Komar Dec. ¶ 18. Correspondence between NYGG's counsel and Massey pertaining to the list lasted until at least early June 2012, and the list itself, which grew to include dozens if not hundreds of attorneys, was still subject to revision as of at least early August 2012. Gov't Exs. 17–18; Hearing Tr. 23:4–24:1, 280:20–281:5. The taint review itself was conducted by three FBI agents working on an intermittent

basis between June 2012 and approximately December 2012. Komar Dec. ¶¶ 19–20; Hearing Tr. 24:25–25:13, 150:7–152:11, 195:5–7. AUSA Massey testified that, during this period of time, he was concerned about the pace at which the review was proceeding, especially in light of emergent district court case law requiring the Government to review and make use of digital search takes within a reasonable period of time. *Id.* 24:2–13, 84:13–18, 86:1–8 (citing Judge Irizarry's then-recent decision in *United States v. Metter,* 860 F.Supp.2d 205 (E.D.N.Y. 2012)). Nevertheless, it is evident from the record that the taint review proceeded slowly. Massey e-mailed his supervisor on August 28, 2012, for example, to note, among other things, "We seized the NYGG hard drives etc. seven months ago and this privilege review is nowhere near finished." Def. Ex. 5.

As the taint review was completed on a rolling basis, the Government began, in late 2012 or early 2013, to conduct a substantive review of the non-privileged materials. Hearing Tr. 25:14–23, 152:2–11; Komar Dec. ¶ 21; *see also* Def. Ex. 6 ***375** (January 15, 2013 e-mail from AUSUA Massey to colleagues noting that "[t]he FBI has now started reviewing the electronic records after a long delay."). In the first instance, Agent Komar personally attempted to search the materials using keywords, some of which may "very well" have not appeared on Exhibit B to the Warrants (the list of individual and entities to which, theoretically, materials would have to relate in order to be seizable). Komar Dec. ¶ 21; Hearing Tr. 152:13–16, 201:10–14. He quickly encountered "difficulty" in using the search program available, however. Komar Dec. ¶ 21; Hearing Tr. 152:13–16. In response, he shifted gears and began a "file-by-file review" of some of the seized flash drives, making determinations as to the "pertinence" of individual documents. Komar Dec. ¶ 21; Hearing Tr. 152:16–21, 153:10–20. Agent Komar was not assisted in his review by any other agents, and was never given any sort of deadline for completion. Hearing Tr. 199:12–200:5. Ultimately, he was unable to make notable headway before he was transferred in February 2013 to a position at FBI headquarters in Washington, D.C. Komar Dec. ¶¶ 21–22; Hearing Tr. 153:7–8, 153:21–154:3, 198:18–199:11.

Following Komar's transfer, Agent McGuire took over as case agent. Komar Dec. ¶ 22; Hearing Tr. 154:4–5. To familiarize himself with the broader investigation, Agent McGuire reviewed the case file and Komar and Garwood Affidavits, among other things. Hearing Tr. 279:10–19. By sometime in March 2013, McGuire was prepared to begin his own substantive review of the non-privileged electronic materials taken during the Searches. Hearing Tr. 281:11–14.

To facilitate Agent McGuire's review of the electronic materials, AUSA Massey developed a list of search terms. Hearing Tr. 26:1–27:10, 282:3–18; Gov't Ex. 19 (search term list as of May 3, 2013). Massey developed the list by "start[ing]" with Exhibit B to the Warrants and then "add[ing] names that [Massey] believed were tied directly or tied to the names in the search warrant." Hearing Tr. 26:18–20; *see also* Def. Ex. 10 (May 3, 2013 e-mail from Massey to McGuire and others noting that the "majority of the [search] terms are in the search warrant application," and the "others are directly related to items listed in the search warrant"). As Massey conceded at the Hearing, however, he assessed "relatedness" with the "benefit of 15 month[s'] more investigation time" following the Searches themselves. Hearing Tr. 113:10–15. Indeed, Massey testified, for example, that to the extent he "learned ... information" about individuals identified in the Warrants "in the intervening period" between the Searches and the development of the search term list, it would have been "acceptable to add that [information] to the list." *Id.* 114:2–10. There is no dispute that Massey's list, which was provided to Agent McGuire in early May 2013, included dozens (if not more) of names that were not included in Exhibit B to the Warrants or that Agent McGuire was well aware of that when he received the list. *See, e.g.,* Def. Ex. 10, Hearing Tr. 91:5–92:1, 98:6–10, 283:3–18, 310:14–311:2, 315:22–316:11. For example, the name of Wey's co-Defendant in this matter, Seref Dogan Erbek, appeared on Massey's search term list but did not appear on Exhibit B. *See* Gov't Ex. 19; Hearing Tr. 93:7–94:15. The search term list developed by Massey was not submitted to a Magistrate Judge for approval as an expansion of the original Searches. Hearing Tr. 92:2–16.

At approximately the same time that he provided the search term list to Agent McGuire to aid in his review of the electronic Search fruits, AUSA Massey also shared, at McGuire's request, an e-mail ***376** memorandum summarizing the Government's possible charging theories with respect to Wey as of May 2013 (almost 16 months after the Warrants were executed). Def. Exs. 10, 22 (May 2013 e-mails between Massey and McGuire, among others);

Hearing Tr. 312:11–314:8. McGuire asked for the summary to help guide his review of the electronic documents and to assist him in identifying "the most critical evidence" or "hot docs." Hearing Tr. 313:13–314:8, 361:24–362:12. Massey's memorandum highlighted, in addition to the " '[b]eneficial [o]wnership' fraud" theory described in sum and substance in the Komar Affidavit and the Operations Order, an "alternate" theory of "tax evasion" in connection with fund transfers between Wey's sister and Wey's wife. Def. Ex. 22. Notably, neither the Komar Affidavit, nor the Warrants, nor the Operations Order referenced any active investigation of Wey pertaining to tax evasion or tax fraud. [3] Indeed, Agent McGuire testified that he personally suggested the new tax fraud theory to the prosecution team after taking over as case agent in 2013 (more than a year after the Searches), and that he had discussions about the theory with Internal Revenue Service personnel during that timeframe. Hearing Tr. 353:7–358:3. Massey's memorandum also noted that "much of the evidence" marshalled therein came from proffer sessions that—according to Agent McGuire's Hearing testimony —"probably" took place sometime after the Warrants were executed. Hearing Tr. 326:6–327:4; Def. Ex. 22.

In early May 2013, after receiving the search terms and theories-of-the-case memorandum from AUSA Massey and rereading at least one of the Warrants, Agent McGuire began his review of the electronic materials. Hearing Tr. 284:9–15, 315:19–21. Notwithstanding Agent Komar's limited foray into a portion of the electronic documents, Agent McGuire "started from scratch," and did a "complete review" of the confiscated materials. *Id.* 307:16–308:16. His review took place predominantly at FBI offices in New Jersey across the span of ten full-day sessions. 284:16–285:5, 286:11–14, 289:25–290:7. McGuire testified at the Hearing that, to his understanding, his task was to use the search terms provided by AUSA Massey to locate and "tag" as "pertinent" any documents within the electronic Search fruits that were "covered by the search warrant." Hearing Tr. 283:19–284:8, 308:17–309:4. Such documents could include, for example, any "financial records related to [NYGG]" or any "e-mails with NYGG." *Id.* 293:6–18. There is no evidence that Agent McGuire referenced or otherwise considered the Komar or Garwood Affidavit while conducting his review.

Agent McGuire worked systematically through the May 2013 list of search terms ***377** provided by AUSA Massey, running each term across two separate FBI databases containing materials recovered from NYGG and the Wey Apartment, respectively. *See, e.g.,* Gov't Ex. 16 (list of search terms with Agent McGuire's contemporaneous handwritten notes); Hearing Tr. 327:5–329:19. On occasion, Massey supplemented the list with additional search terms, and McGuire also developed novel terms based on his review of the documents. Hearing Tr. 330:10–17, 331:11–20. Sometimes McGuire determined that certain search terms yielded "too many false positives" in its returns and were thus ineffective and should be discarded. *Id.* 286:15–288:10, 293:23–294:3; *see also* Gov't Ex. 16. Conversely, if Agent McGuire made a preliminary determination based on "10 or 15" documents that a particular search term appeared to reliably return documents that actually pertained to the search term's intended referent, he would then proceed to tag all documents returned by the relevant search as pertinent, without necessarily engaging in further substantive review on a document-by-document basis. Hearing Tr. 289:1–20; 292:9–294:3. At least one of the novel search terms that McGuire ran was intended to identify tax-related documents and was developed in cooperation with IRS personnel. *Id.* 353:7–358:3.

Agent McGuire testified that running the search terms across the two databases was a lengthy process, with each individual search through one of the databases taking as long as two to three minutes. *Id.* 290:1–22. Like Agent Komar before him, Agent McGuire performed his review without substantive assistance or support from any other agents. *Id.* 291:2–5.

McGuire completed his review in approximately early September 2013. *Id.* 291:6–8, 330:21–331:1, 333:22–334:2. In total, he tagged approximately 14,000 electronic documents from the Apartment Search and slightly over 90,000 electronic documents from the NYGG Search as pertinent. *Id.* 291:22–292:2, *see also id.* 334:14–16 (estimating overall total of about 105,000). He provided copies of all such documents to the prosecution team. 291:9–21, 329:21–25.

Wey was not indicted for another two years. During that time and to this day, the FBI retained all electronic materials taken from NYGG and the Wey Apartment (whether in original or copied form), regardless of whether they had been identified as pertinent during McGuire's review. The Government did

not introduce any evidence at the Hearing that would help explain the reasons for such broad retention.

In the weeks leading up to Wey's indictment (roughly late August to early September 2015), FBI personnel conducted additional searches across all electronic materials recovered from both locations. Those searches were the subject of substantially inconsistent Hearing testimony by the FBI agents involved. Agent McGuire, who remained the case agent during the relevant timeframe, testified in sum and substance that in August or September 2015, the FBI was seeking in anticipation of Wey's indictment to prepare clean "evidence copies" of specific pertinent documents that had been identified during the 2013 review, but learned that the materials taken during the Searches had apparently lost their electronic privilege and pertinence tags due to a technical malfunction. Hearing Tr. 337:6–341:7, 349:6–353:1, 358:8–361:4. Agent McGuire concluded that it would be inappropriate for agents involved in the investigation to personally conduct searches through the unsegregated FBI databases as of 2015, and decided instead to recruit an uninvolved taint agent, Elizabeth Miller, to ***378** perform the necessary searches instead. *Id.* According to McGuire, Agent Miller was specifically tasked with finding electronic copies of only certain of the "exact same document[s]" that the FBI had already deemed pertinent and non-privileged in 2013 and, to that end, he provided her with hard copies of all the relevant documents and instructed her to run search terms consisting of direct "quote[s]" and other "snippets" from those documents, many of which pertained to Defendant Erbek. *Id.* McGuire testified that Agent Miller did not identify any additional documents of interest through this effort beyond what the FBI had tagged as pertinent in 2013. *Id.*

In response to Agent McGuire's testimony at the Hearing, the defense called Agent Miller, who had not expected to testify and initially was not present in the courthouse. Agent Miller agreed that she was brought in nominally as a taint agent in 2015—having had no prior involvement in the investigation of Wey—in order to run searches through the FBI's preexisting databases. She testified, however, that Agent McGuire provided her with five to ten search terms, each approximately one to two words in length, along with "only a few ... examples" of documents "that could potentially have information that they would want" and directed her to search for "similar" documents within the databases. Hearing Tr. 368:13–375:23, 377:3–9. She specifically recalled that Defendant Erbek's name was among the search terms provided by Agent McGuire. *Id.* When asked about using Erbek's name as a search term, Agent McGuire testified that, in his view, all documents referencing Erbek were responsive to the Warrants—notwithstanding that, as noted, neither the Affidavits nor the Warrants made any reference to him—because McGuire "learned through the investigation in review of the documents" that Erbek had facilitated financial transactions for Wey and his sister and, as such, materials bearing his name would constitute "financial records relating to Benjamin Wey." *Id.* 350:14–351:23.

Agent Miller testified that, prior to commencing the requested searches, she "was given just a very brief summary of the case" and thus "had some knowledge of what [she] ... should be looking for," but "was not given a full scope of what the search warrant entailed." *Id.* 376:1–8. Ultimately, according to Agent Miller, she identified and electronically tagged "possibly" as many as fifty or more documents in the databases that she viewed as similar to the examples provided. *Id.* 374:13–375:23. A contemporaneous e-mail authored by Agent McGuire suggests that Agent Miller "located" as many as "150 documents" of relevance, subject to further privilege review. Def. Ex. 20 (August 20, 2015 e-mail from McGuire to AUSAs and others). Agent Miller did not, however, play any role in transmitting any of those documents to McGuire or the prosecution team and was unsure if any such transmission ever occurred. *Id.* 378:14–379:18.

The Court is unable to reconcile Agent McGuire's version of these events with that of Agent Miller. Having observed both witnesses at the Hearing and after careful consideration of their respective testimony, the Court credits the testimony of Miller, an agent with no particular professional stake in this matter who offered clear and internally consistent recollections despite being called to the stand unexpectedly and testifying with negligible preparation and unaware of the questions bearing on Wey's motion. McGuire, by contrast, served as case agent on the FBI's Wey investigation and was featured at the Hearing as one of the Government's primary witnesses, evincing thorough preparation—including on this particular point—and ***379** a keen sensitivity to the legal issues in play throughout the proceedings.

As noted, Wey was indicted in early September 2015. The instant motion was filed along with a slew of other pretrial

motions—which the Court has resolved by separate Order—in mid–2016.

II. Discussion

[1] **[2]** Wey contends primarily that the fruits of the Searches must be suppressed because the Warrants are insufficiently particularized, overbroad "general warrants," and because the Government's lengthy (and continuing) retention and indiscriminate review of the vast trove of confiscated electronic materials must be deemed unreasonable under the circumstances. [4]

A. Constitutional Requirements for Search Warrants

The Fourth Amendment to the United States Constitution provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV.

[3] **[4]** "The Fourth Amendment's requirements regarding search warrants are not 'formalities.' " *United States v. Voustianiouk,* 685 F.3d 206, 210 (2d Cir. 2012) (quoting *McDonald v. United States,* 335 U.S. 451, 455, 69 S.Ct. 191, 93 L.Ed. 153 (1948)). "The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.' " *United States v. Galpin,* 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York,* 445 U.S. 573, 583, 100 S.Ct. 1371, 63 L.Ed.2d 639 (1980)). "To prevent such 'general, exploratory rummaging in a person's belongings' and the attendant privacy violations, the Fourth Amendment provides that a 'warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity.' " *Id.* (internal citations omitted) (quoting *Coolidge v. New Hampshire,* 403 U.S. 443, 467, 91 S.Ct. 2022, 29 L.Ed.2d 564 (1971); *Kentucky v. King,* 563 U.S. 452, 459, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011)). The particularity requirement "is necessarily tied to the ... probable cause requirement." *In re 650 Fifth Ave. & Related Props.,* 830 F.3d 66, 98 (2d Cir. 2016). That is because " '[b]y limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character ***380** of the wide-ranging exploratory searches the Framers intended to prohibit.' " *Id.* (quoting *Maryland v. Garrison,* 480 U.S. 79, 84, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987)). In assessing the Constitutional sufficiency of any warrant, courts must be mindful that "the ultimate touchstone of the Fourth Amendment is 'reasonableness.' " *Brigham City, Utah v. Stuart,* 547 U.S. 398, 403, 126 S.Ct. 1943, 164 L.Ed.2d 650 (2006) (internal citation omitted).

1. Particularity

[5] "Courts implement the particularity requirement by insisting that warrants not 'leave to the unguided discretion of the officers executing the warrant the decision as to what items may be seized.' " *United States v. Zemlyansky,* 945 F.Supp.2d 438, 453 (S.D.N.Y. 2013) (quoting *United States v. Riley,* 906 F.2d 841, 844 (2d Cir. 1990) (citations omitted)). Put differently, "[a] warrant must be 'sufficiently specific to permit the rational exercise of judgment [by the executing officers] in selecting what items to seize.' " *United States v. Shi Yan Liu,* 239 F.3d 138, 140 (2d Cir. 2000) (brackets in original) (quoting *United States v. LaChance,* 788 F.2d 856, 874 (2d Cir. 1986) (internal quotation marks omitted)).

[6] The Second Circuit has recognized that, to comport with the Fourth Amendment's particularity requirement, a warrant must satisfy three criteria. *See* *Galpin,* 720 F.3d at 445; *see*

also *United States v. Ulbricht*, 858 F.3d 71, 98–99 (2d Cir. 2017). First, it must "identify the specific offense for which the police have established probable cause." *Galpin,* 720 F.3d at 445; *see also* *650 Fifth Ave.*, 830 F.3d at 99 ("[F]or a warrant to meet the particularity requirement, it must identify the alleged crime for which evidence is sought."); *United States v. George*, 975 F.2d 72, 75–76 (2d Cir. 1992) (warrant permitting seizure of evidence "relating to the commission of a crime" was constitutionality infirm because "[n]othing on the face of the warrant tells the searching officer for what crimes the search is being undertaken"). Second, the warrant is required to "describe the place to be searched." *Galpin*, 720 F.3d at 445–46. And third, it must "specify the items to be seized by their relation to designated crimes." *Id.* at 446 (internal quotation marks omitted) (citing, *inter alia*, *United States v. Buck,* 813 F.2d 588, 590–92 (2d Cir. 1987) (warrant authorizing seizure of "any papers, things or property of any kind relating to [the] previously described crime" was insufficiently particularized insofar as it "only described the crimes—and gave no limitation whatsoever on the kind of evidence sought")); *United States v. Rosa,* 626 F.3d 56, 62 (2d Cir. 2010) (warrant "defective in failing to link the items to be searched and seized to the suspected criminal activity" because it "thereby lacked meaningful parameters on an otherwise limitless search"); *see also* *Ulbricht,* 858 F.3d at 98–99 (reciting same three requirements). [5]

***381** In addition to the foregoing, courts in this Circuit have identified certain "circumstance-specific considerations" that may bear on whether a given warrant lacks particularity, even if they do not constitute formal, universal requirements. *Zemlyansky,* 945 F.Supp.2d at 454. Many courts, for example, " 'have found warrants for the seizure of [business] records constitutionally deficient where they imposed too wide a time frame or failed to include one altogether.' " *Id.* (quoting *United States v. Cohan,* 628 F.Supp.2d 355, 365–66 (E.D.N.Y. 2009) (citing "general agreement that a time frame is *relevant*" even if not necessarily "required")); *see also* *United States v. Levy,* 11–cr–62, 2013 WL 664712, at *11 n.7 (S.D.N.Y. Feb. 25, 2013) ("Several courts in this Circuit have recognized the constitutional questions that are raised by the lack of a specific date range in a warrant for documentary records and warned the Government to include one when possible."); *cf.* *United States v. Hernandez*, 09–cr–625, 2010 WL 26544, *9 (S.D.N.Y. Jan. 6, 2010) ("A failure to indicate a time frame could render a warrant constitutionally overbroad because it could allow the seizure of records dating back arbitrarily far and untethered to the scope of the affidavit which ostensibly provided probable cause.") (internal quotation marks and alterations omitted).

Of some significance here, the Supreme Court established in its 2004 decision in *Groh v. Ramirez* that the Fourth Amendment "requires particularity in the warrant, not in the supporting documents," and, accordingly, "the fact that the warrant *application* adequately described the 'things to be seized' does not save the *warrant*" from failure to satisfy that requirement. 540 U.S. 551, 557, 124 S.Ct. 1284, 157 L.Ed.2d 1068 (2004) (emphasis in original). That is because the " 'presence of a search warrant serves a high function,' and that high function is not necessarily vindicated when some other document, somewhere, says something about the objects of the search, but the contents of that document are neither known to the person whose home is being searched nor available for her inspection." *Id.* (internal citation omitted) (quoting *McDonald,* 335 U.S. at 455, 69 S.Ct. 191). Included in that "high function" is not only the "prevention of general searches," but also the " 'assur[ance] [to] the individual whose property is searched or seized of the lawful authority of the executing office, his need to search, and the limits of his power to search.' " *Id.* (quoting *United States v. Chadwick,* 433 U.S. 1, 9, 97 S.Ct. 2476, 53 L.Ed.2d 538 (1977), *abrogated on other grounds,* *California v. Acevedo,* 500 U.S. 565, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991)).

[7] **[8]** Accordingly, "a court may construe a warrant with reference to a supporting ***382** application or affidavit" only "if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant." *Id.* at 557–58, 124 S.Ct. 1284. And, as the Second Circuit has concluded, "for an attached affidavit properly to be incorporated into a warrant, the warrant must contain 'deliberate and unequivocal language of incorporation'

"—"[l]anguage in a warrant that simply references an underlying affidavit" does not suffice. *650 Fifth Ave.*, 830 F.3d at 99–100 (quoting *United States v. Walker*, 534 F.3d 168, 172–73 & n.2 (2d Cir. 2008) (*per curiam*)); *see also* *Rosa*, 626 F.3d at 64 (recognizing that after *Groh*, courts "may no longer rely on unincorporated, unattached supporting documents to cure an otherwise defective search warrant").

2. Probable Cause and Overbreadth

"The Supreme Court has explained that 'probable cause is a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.' " *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Illinois v. Gates*, 462 U.S. 213, 232, 103 S.Ct. 2317, 76 L.Ed.2d 527 (1983)). "In evaluating probable cause in any given case, a judge must make a practical common-sense decision whether, given all the circumstances set forth in the affidavit before him, there is a fair probability that contraband or evidence of a crime will be found in a particular place.' " *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (internal quotation marks and ellipsis omitted) (quoting *Gates*, 462 U.S. at 238, 103 S.Ct. 2317; *Falso*, 544 F.3d at 117). "Due to this subjective standard, a reviewing court generally accords 'substantial deference to the finding of an issuing judicial office that probable cause exists,' limiting [the] inquiry to whether the office 'had a substantial basis' for his determination." *Id.* at 113 (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir. 1993)). "Nevertheless, under this standard, [courts] 'may properly conclude that ... a warrant was invalid because the [magistrate judge's] probable-cause determination reflected an improper analysis of the totality of circumstances.' " *Falso*, 544 F.3d at 117 (internal brackets omitted) (quoting *United States v. Leon*, 468 U.S. 897, 915, 104 S.Ct. 3405, 82 L.Ed.2d 677 (1984)).

[9] **[10]** The doctrine of overbreadth represents, in a sense, an intersection point for probable cause and particularity principles: it recognizes, in pertinent part, that a warrant's unparticularized description of the items subject to seizure may cause it to exceed the scope of otherwise duly established probable cause. Thus, "a warrant is overbroad if its 'description of the objects to be seized ... is broader than can be justified by the probable cause upon which the warrant is based.' " *United States v. Lustyik*, 57 F.Supp.3d 213, 228 (S.D.N.Y. 2014) (quoting *Galpin*, 720 F.3d at 446); *see also* *Ulbricht*, 858 F.3d at 102 ("breadth and particularity are related but distinct concepts" and a "warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material," without necessarily "violating the particularity requirement"); *Zemlyansky*, 945 F.Supp.2d at 464 ("In determining whether a warrant is overbroad, courts must focus on 'whether there exists probable cause to support the breadth of the search that was authorized.' ") (quoting *Hernandez*, 2010 WL 26544, *8).

3. Additional Considerations in the Context of Electronically Stored Information

[11] The fact that the Warrants at issue in this motion targeted—and the ***383** Search fruits ultimately consisted overwhelmingly of—electronically stored information implicates at least two additional considerations. First, as the Second Circuit has recognized, "[w]here ... the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance." *Galpin*, 720 F.3d at 446. That is because the "seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure." *United States v. Ganias*, 824 F.3d 199, 217 (2d Cir. 2016) (*en banc*). As such, "[t]he potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous"—a "threat [that] is compounded by the nature of digital storage." *Galpin*, 720 F.3d at 447. Indeed, the Government, once it has obtained authorization to search a hard drive, may in theory "claim that the contents of every file it chose to open were in plain view and, therefore, admissible even if they implicate the defendant in a crime not contemplated by the

warrant," thus presenting a " 'serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.' " *Id.* (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010)) (*en banc*) (*per curiam*); *cf. Riley v. California*, —— U.S. ——, 134 S.Ct. 2473, 2489–91, 189 L.Ed.2d 430 (2014) (recognizing that cell phones "differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person" owing to their "immense storage capacity" and their ability to "contain[ ] in digital form" both "many sensitive records previously found in the home" and "a broad array of private information never found in a home in any form—unless the phone is"); *Ganias*, 824 F.3d at 231 (Chin, J., dissenting) (noting that "[v]irtually the entirety of a person's life may be captured as data" on a computer or smartphone). Accordingly, a "heightened sensitivity to the particularity requirement in the context of digital searches" is necessary. *Galpin*, 720 F.3d at 447.

[12] There is also the matter of the execution of a warrant targeting electronically stored information. Under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant may—as the Warrants at issue did here—"authorize the seizure of electronic storage media or the seizure or copying of electronically stored information." Fed. R. Crim. P. 41(e)(2)(B). The Rule provides that "[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant." *Id.* Although "there is no established upper limit as to when the government must review seized electronic data to determine whether the evidence falls within the scope of a warrant," courts have recognized that "the Fourth Amendment requires the government to complete its review, *i.e.*, execute the warrant, within a 'reasonable' period of time." *Metter*, 860 F.Supp.2d at 215 (collecting cases); *see also United States v. Alston*, 15–cr–435, 2016 WL 2609521, at *3 (S.D.N.Y. Apr. 29, 2016) ("While Rule 41 prescribes no particular time period for data extraction in these circumstances, the time needed to complete off-site copying or review is subject to the rule of reasonableness."); *Lustyik*, 57 F.Supp.3d at 230 ("[l]ike all activities governed by the Fourth Amendment, the execution of a search warrant must be reasonable" and "[l]aw enforcement officers therefore must execute a search warrant," including when applicable review of recovered electronic communications, "within a reasonable ***384** time"); *cf. In the Matter of a Warrant for All Content and Other Information Associated with the Email Account xxxxxxx@ gmail.com Maintained at Premises Controlled by Google, Inc.*, 33 F.Supp.3d 386, 392 (S.D.N.Y. Aug. 7, 2014) (noting that courts have developed a "flexible approach" for assessing the execution of warrants for electronic evidence, applying a general standard of "reasonableness") (internal quotation marks omitted).

B. The Search Warrants Do Not Comport with the Requirements of the Fourth Amendment

1. The Search Warrants Lack Particularity

The Court has little difficulty concluding that, for several reasons, both the NYGG Warrant and the Apartment Warrant fail to describe the items to be seized with the requisite particularity. Because the Warrants are, as discussed above, substantially identical in their description of the items subject to seizure, the Court does not distinguish between them for purposes of this analysis.

a. Failure to Identify Suspected Crimes

[13] First, on their face, both Warrants fail to set forth the crimes under investigation. As noted, they neither cite criminal statutes nor in any way describe any suspected criminal conduct. Clearly, such matters are set forth in the supporting Affidavits, but because those documents are neither attached to nor incorporated into the Warrant themselves, the information they provide does not "cure an otherwise defective search warrant." *Rosa*, 626 F.3d at 64. Under the settled Circuit law set forth above, failure to reference the suspected crimes would alone be enough to render the Warrants insufficiently particularized. *See 650 Fifth Ave.*, 830 F.3d at 99 ("for a warrant to meet the particularity requirement, it must identify the alleged crime for which evidence is sought"); *George*, 975 F.2d at 76 (warrant permitting search of evidence "relating to the commission of a crime" lacked particularity because "[n]othing on the face of the warrant tells the searching

officer for what crime the search is being undertaken"); *see also United States v. Romain*, 678 Fed.Appx. 23, 25, 2017 WL 442175, at *1 (2d Cir. 2017) (Summary Order) ("[T]he government concedes that the warrant was facially deficient for failing to reference the criminal statutes that [defendant] was accused of violating even though the supporting document did contain that information.").

The Government argues, however, that explicit references to the crimes under investigation is unnecessary because the categories of documents subject to seizure make it "plain ... that this is a financial fraud case involving securities fraud in particular." Opp. at 28–29. That is unavailing for at least two reasons. First, the Government offers no authority, and the Court is aware of none, for the proposition that a warrant lacking an express reference to any crime or criminal conduct nonetheless satisfies the particularity requirement simply because the suspected crimes are arguably "inferable," Opp. at 29, from the warrant's remaining provisions. If anything, the Court of Appeals has rejected a similar argument, concluding in *George* that a warrant's inclusion of a list of seizable items that featured a McDonald's uniform, McDonald's management materials, a firearm, and a purse, did not mean that the otherwise "broad catch-all" phrase "any other evidence relating to the commission of ***a crime***" referred with particularity to a recent McDonald's robbery when "read in context." 975 F.2d at 74–76 (emphasis added).

***385** Second, the Government's factual premise is faulty. While it is true that the Warrants authorize seizure of categories of documents that conceivably could be consistent with an investigation into securities fraud, those categories are sufficiently broad and numerous as to be consistent with an investigation into almost *any* form of financial crime (or even concealment of the fruits of some non-financial crime). *See e.g.,* NYGG Warrant Ex. A (making subject to seizure "financial records," "correspondence," "records of internal and external communications," shareholder and investor records, marketing materials, and documents reflecting corporate ownership or structure). Nothing about these categories would make it "plain" to a reader that securities fraud in particular was necessarily the subject of the search and limit the executing officers' discretion accordingly. [6]

The Government also urges that "no crime-identification requirement applies or should apply where ... (1) the subject warrant does not include a blanket permission to seize 'all evidence' or 'all documents' and (2) the categories of evidence to be seized are otherwise described with particularity." Opp. at 30. The binding case law in this Circuit simply reflects no such caveats, however, and, in any event and as explained further below, the items made subject to seizure in the Warrants are by no means "otherwise described with particularity." To the contrary, once the structure of the Warrants is taken into account, it is clear that their description of the items to be seized is essentially the functional equivalent of the very sort of "all-documents" authorization that, according to the Government, would make explicit reference to the crimes under investigation all the more important.

b. Expansive Categories of Generic Documents without Linkage to Suspected Criminal Conduct

[14] The last point segues directly to the second reason why the Warrants are insufficiently particularized. Exhibit A to each of the Warrants sets forth expansive categories of often generic items subject to seizure—several of a "catch-all" variety—without, crucially, any linkage to the suspected criminal activity, or indeed any meaningful content-based parameter or other limiting principle. Importantly, the property listed is hardly, by "its particular character, contraband." See 2 Wayne R. LaFave, *Search and Seizure: A Treatise on the Fourth Amendment* § 4.6(a) (5th ed. 2012). Rather, it is, from top to bottom, "the type of property" that is "generally in lawful use in substantial quantities," and, therefore, even "[g]reater care in description [i]s ... called for." *Id.* (also noting that "[a] more particular description than otherwise might be necessary is required when other objects of the same general classification are likely to be found at the particular place to be searched") (endnote citations omitted); *cf. United States v. Morisse,* 660 F.2d 132, 136 n.1 (5th Cir. 1981) (if the "nature of the [suspected illegal] activity does not allow for [the] ***386** ready segregation" of illegal items from "legal items," then "the "magistrate should take care to assure the warrant informs the law enforcement agent as to how he should distinguish between the illegal paraphernalia and the items that are held legally").

Specifically, Exhibit A authorizes seizure of, for example, the following buckets of material: "financial records,"

"notes," "memoranda," "records of internal and external communications," "correspondence," "audio tapes[ ] and video tapes," "photographs," "documents which may reflect the identifies of persons listed in Exhibit B or persons affiliated with the entities listed in Exhibit B," and others. *See, e.g.,* NYGG Warrant Ex. A. Several of these top-level categories are followed by sub-lists of more specific types of items, but, as the Government concedes, those do not purport to be in any way exhaustive or exclusionary and instead serve only an "illustrative" function. Opp. at 27. And, in any event, "even the most specific descriptions" on the sub-lists (e.g., "documents concerning or reflecting the movement of funds," "checks," "transaction records," "Rolodexes," "diaries," "calendars," etc.") are themselves "fairly general." *See* *United States v. Cardwell,* 680 F.2d 75, 78–79 (9th Cir. 1982); NYGG Warrant Ex. A.

Indeed, the only Warrant provisions that purport to place actual limitations or constraints of any sort on the executing officers' authority to seize items falling into these otherwise capacious buckets are those requiring that items to be seized "concern," "relate" to, or bear some similar generalized connection to at least one of the individuals and entities set forth in Exhibit B to the Warrants. The problem is that Exhibit B, as discussed, includes among its first few entries that very corporate entity (NYGG) whose premises was the subject of the first Warrant and Search and those very individuals (Benjamin and Michaela Wey) whose residence was the subject of the second. The result of that circular structure is that the would-be constraint imposed by Exhibit B is no constraint at all. Instead, the impact of the interplay between Exhibit A (the list of items to be seized) and Exhibit B (the list of relevant individual and entities) is that the Warrants broadly authorize the seizure from NYGG's offices of all "financial records," "notes," "memoranda," records of "communications," "correspondence," "tapes," "photographs," etc. *pertaining to NYGG itself.* So, too, they authorize seizure from the Wey Apartment of all such materials *pertaining to the Weys themselves*. By the Warrants' terms, then, no connection to any suspected crime or to any other individual or entity listed on Exhibit B is necessary to render the expansive list of items set forth in Exhibit A seizable.

Lacking, accordingly, any practical tool to guide the searching agents in distinguishing meaningfully between materials of potential evidentiary value and those obviously devoid of it; the Warrants are—in function if not in form—general warrants. Indeed, insofar as any document located within a home or office at least arguably pertains in some way to the occupant or owner of the premises, the Court would struggle to conceive of any documents found within NYGG or the Wey Apartment that would *not* colorably fall within the scope of that authorization (and, as discussed further below, so too did the Government agents in charge of the Searches).

This deficiency, while concerning under any circumstances, is only exacerbated by the fact that the Warrants target, in significant measure, the contents of electronic devices, such as computers, internal and external hard drives, and smartphones. ***387** *See, e.g.,* NYGG Warrant Ex. A. As the Court of Appeals observed just days ago, especially given the practical risk that "every warrant for electronic information will become, in effect, a general warrant," a warrant that "lack[s] meaningful parameters on an otherwise limitless search of a defendant's electronic media"—including in its "fail[ure] to link the evidence sought to the criminal activity supported by probable cause"—does "not satisfy the particularity requirement." *Ulbricht,* 858 F.3d at 99–100 (internal quotation marks and alterations omitted) (quoting *Galpin,* 720 F.3d at 447; *Rosa,* 626 F.3d at 62)

In sum, the Warrants authorize the seizure of sweeping categories of materials, regardless of their potential connection (or lack thereof) to any suspected criminal activities and limited only by the requirement that they relate in some generalized way to the owner/occupant of the very premises subject to search. The conferral of such unfettered discretion on the executing officers, particularly in light of the Warrants' independent failure to identify any crime under investigation, is inconsistent with the Fourth Amendment's particularity requirement. [7]

c. Lack of Temporal Limitation

[15] Finally, to the extent that lack of temporal limitation constitutes an independent factor militating against a determination of particularity, the Warrants undisputedly fail to limit the items subject to seizure by reference to any relevant timeframe or dates of interest. They do so despite

the underlying Affidavits—and, ultimately, the Indictment—identifying timeframes, and often rather precise timeframes at that, for suspected criminal activity in relation to each of the Issuers purportedly implicated in Wey's suspected scheme. *See, e.g.,* *United States v. Abboud,* 438 F.3d 554, 576 (6th Cir. 2006) (" 'Failure to limit broad descriptive terms by relevant dates, when such dates are available to the police, will render a warrant overbroad.' ") (quoting *United States v. Ford,* 184 F.3d 566, 576 (6th Cir. 1999)); *United States v. Kow,* 58 F.3d 423, 427 (9th Cir. 1995) (warrant "not sufficiently ***388** particular" in part because the "government did not limit the scope of the seizure to a time frame within which the suspected criminal activity took place"); *United States v. Abrams,* 615 F.2d 541, 545 (1st Cir. 1980) (deeming warrant insufficiently particularized and noting, among other things, that "[a] time frame should also have been incorporated into the warrant"); *United States v. Jacobson,* 4 F.Supp.3d 515, 526 (E.D.N.Y. 2014) ("a warrant's failure to include a temporal limitation on the things to be seized may, in certain circumstances, render a warrant insufficiently particular").

The Court recognizes that the "complexity and duration of the alleged criminal activities" discussed in the Affidavits may well make the Warrants' lack of a temporal limitation somewhat "less significant" of a factor in determining their constitutional sufficiency than it otherwise might be. *See* *Hernandez,* 2010 WL 26544, at *11. Still, the "absence of such a limit reinforces the Court's conclusion" that the Warrants are insufficiently particularized. *Zemlyansky,* 945 F.Supp.2d at 459–60; *Vilar,* 2007 WL 1075041, at *23 (the "lack of particularity is only compounded by the absence of any date restriction on the items to be seized"); *United States v. Triumph Capital Grp., Inc.,* 211 F.R.D. 31, 58 (D. Conn. 2002) (recognizing a "temporal limitation" as "one indicia of particularity").

d. The All–Records Exception Does Not Save the Warrants From Their Lack of Particularity

The Government contends that, even if the Warrants lack particularity, they fall within the so-called "all-records exception" and thus do not run afoul of the Fourth Amendment. Opp. at 36–37. The Court concludes otherwise.

i. Legal Standard for the All–Records Exception

[16] Courts in the Second Circuit have recognized that "[w]hen there is probable cause to believe that an entire business is 'pervaded' or 'permeated' with fraud, seizure of all records of the business is appropriate, and broad language used in a search warrant will not offend the particularity requirement." *United States v. D'Amico,* 734 F.Supp.2d 321, 360 (S.D.N.Y. 2010). Under those limited circumstances, "broad language used in warrants will not offend the particular requirements." *U.S. Postal Serv. v. C.E.C. Servs.,* 869 F.2d 184, 187 (2d Cir. 1989). This principle is commonly referred to as the "all-records exception to the particularity requirement." *D'Amico,* 734 F.Supp.2d at 360 (internal quotation marks omitted) (citing *United States v. Burke,* 718 F.Supp. 1130, 1139 (S.D.N.Y. 1989)); *see also* *United States v. Smith,* 05–cr–293A, 2007 WL 2088938, at *3 (W.D.N.Y. Jul. 19, 2007) ("Although the particularity requirement of the Fourth Amendment creates a general presumption against 'general' or 'all-records' warrants, courts, including the Second Circuit, have recognized an exception where there is probable cause to believe that criminal activity permeates the business to be searched."). From a strictly analytical perspective, however, "it is not so much an 'exception' to the particularity requirement ... as a recognition that a warrant—no matter how broad—is, nonetheless, legitimate if its scope does not exceed the probable cause upon which it is based." *United States v. Bowen,* 689 F.Supp.2d 675, 683 n.6 (S.D.N.Y. 2010) (internal quotation marks omitted); *cf.* *Hickey,* 16 F.Supp.2d at 241 ("The more extensive the probable wrongdoing, the greater the permissible breadth of the warrant.").

[17] **[18]** For the all-records exception to apply, the affidavit in support of the ***389** search warrant need not necessarily lay out "specific factual evidence demonstrating that every part of the enterprise in question is engaged in fraud"; rather, it must only set forth "sufficient factual evidence of fraudulent activity from which a magistrate could

infer that those activities are 'just the tip of the iceberg.' " *Burke,* 718 F.Supp. at 1139–40 (additional internal quotation marks omitted) (quoting *United States v. Offices Known as 50 State Distrib. Co.,* 708 F.2d 1371, 1375 (9th Cir. 1983)). Still, "[t]he Fourth Amendment requires more than mere extrapolation to activate the [all-records] principle." *Hickey,* 16 F.Supp.2d at 241. And courts assessing the applicability of the exception must satisfy themselves that "the Government ... provided the magistrate judge with sufficient probable cause to believe that the *entire* business operation is a scam." *Zemlyansky,* 945 F.Supp.2d at 461 (internal quotation marks and alterations omitted) (emphasis in original); *United States v. Paccione,* 738 F.Supp. 691, 708 (S.D.N.Y. 1990) ("Courts have consistently held that where a business is *totally illegal,* a search warrant may properly authorize the seizure of all documents of the business.") (emphasis added).

ii. The All–Records Exception Does Not Apply Here

[19] First, a preliminary observation: while the probable cause showing necessary to invoke the all-records exception is always substantial, the Government faces an even higher hurdle than usual in attempting to apply it to the Apartment Warrant. Indeed, as several Circuits have recognized, "it would require extraordinary proof to demonstrate that an individual's entire life is consumed by fraud and that *all* records found in the home were subject to seizure." *United States v. Falon,* 959 F.2d 1143, 1148 (1st Cir. 1992); *United States v. Humphrey,* 104 F.3d 65, 69 n.2 (5th Cir. 1997) ("the issuance of all records searches of homes" will be upheld "only in extreme cases"); *see also United States v. Cherna,* 184 F.3d 403, 409 (5th Cir. 1999) ("[I]it is more difficult to demonstrate probable cause for an 'all records' search of a residence than for other searches."). For that reason, even "when an individual's allegedly fraudulent business activities are centered in his home," the " 'all records' doctrine must be applied with caution" in the context of a home search, and, absent "unusual proof," any "broad categories of items ... must be sufficiently linked to the alleged criminal activity so as to distinguish them from innocent personal materials." *Falon,* 959 F.2d at 1148; *see also United States v. Ostrowski,* 822 F.Supp.2d 66, 71 (D. Mass. 2011) ("[E]ven pervasive fraud cannot justify seizure of every record from an individual's home."). While the Second Circuit does not appear to have addressed this issue directly, its decisions on the subject strongly signal that the all-records exception is generally limited to the seizure of "*business* records" and applicable only when there is probable cause to believe that a "*business* was permeated with fraud." *Nat'l City Trading Corp. v. United States,* 635 F.2d 1020, 1026 (2d Cir. 1980) (emphasis added); *C.E.C. Servs.,* 869 F.2d at 187 (same).

Even assuming, however, that the all-records exceptions could conceivably save both the NYGG Warrant and the Apartment Warrant, the Court finds that both Warrant applications fell short of providing Magistrate Judge Dolinger with "sufficient probable cause to believe that [Wey's] *entire* business operation [was] a scam." *Zemlyansky,* 945 F.Supp.2d at 461 (internal quotation marks and alterations omitted) (emphasis in original); *see also D'Amico,* 734 F.Supp.2d at 360 (all-records doctrine applies where "there is probable cause to believe that an entire business is ***390** 'pervaded' or 'permeated' with fraud"). As noted above, the Komar Affidavit—and, by extension, the Garwood Affidavit—described NYGG, in terms suggesting some measure of presumed legitimacy, as a "corporate advisory firm" with a "special[ty]" in "introducing middle-market Chinese operating companies to the U.S. capital markets." *See, e.g.,* Komar Aff. ¶ 16. Accounting for all of the substantial evidence marshalled across the Komar Affidavit's nearly 100 pages, it connected NYGG and Wey to a scheme implicating, at most, five or six discrete deals involving specifically identified Issuers, with the alleged misconduct pertaining to each company occurring in some at least roughly defined timeframe. *See* Reply Memorandum of Law in Further Support of Defendant Benjamin Wey's Motion to Suppress, To Dismiss the Indictment, and For Other Relief, Dkt. No. 62 ("Reply"), at 19–20. The Komar Affidavit did not set forth any evidence, explicit or implicit, that the scheme either constituted just the "tip of iceberg" with respect to fraudulent activity involving NYGG or the Wey Apartment, or that the scheme itself constituted the entirety—or even a substantial portion—of NYGG's or Wey's overall business operations. It made no showing, for example, that NYGG was merely a front for the scheme or that the scheme infused or was otherwise "inseparable" from the balance of NYGG's

corporate advisory activities. *Burke,* 718 F.Supp. at 1141. Nowhere, more generally, did it suggest that NYGG was a so-called "boiler room" operation or similar sham enterprise. *Id.* at 1140–41.

Indeed, the Komar Affidavit, as the Government concedes, "candidly acknowledged," Opp. at 36, that there were "legitimate aspects of [NYGG's] business," Komar Aff. ¶ 35(b) n.11, but it made no effort to characterize the scope of the suspected fraud relative to NYGG's apparently above-board operations. *See Zemlyansky,* 945 F.Supp.2d at 463 ("The affidavit offers no information about the size or scope of [the subject] business, its clients, whether only part of the office deals with the kind of billing at issue in the alleged scheme, [or] the manner in which or degree to which it is controlled by the [relevant] scheme...."). To the contrary, Komar admitted that he lacked the necessary information to do so, averring that the NYGG Search would help provide the FBI with "background" information to better understand the "scope" of the suspected fraudulent scheme as "compared to [NYGG's] overall business." Komar Aff. ¶ 35(b) n.11.

True, the fact that a business "engaged in *some* legitimate activity" may not necessarily "defeat the all-records exception" on its own. *D'Amico,* 734 F.Supp.2d at 360 (emphasis in original). Thus, for example, an enterprise demonstrated by the FBI to have been specifically created to serve as a front to launder organized crime proceeds could not invalidate an expressly approved all-records application by pointing to some potentially legitimate sales activity on the side. *Id.* at 356–62. But clear acknowledgment, of the sort offered by Komar, that an affiant is essentially in the dark as to how a suspected fraud fits into a broader "legitimate" business is inconsistent with a demonstration of probable cause that the fraud entirely permeates the enterprise.

In fact, the Komar Affidavit recognized the relative narrowness of its actual probable cause showing, consistently asserting, for example, that there was probable cause to believe that "documents and other evidence *relating to the SmartHeat, Deer, and AgFeed schemes*" would be found at the NYGG offices. Komar Aff. ¶ 35; *see also id.* ¶ 38 ("There [is] probable cause to believe that the [NYGG offices] currently contain evidence *of Wey's use of nominees to conceal his ownership in CleanTech and Nova Lifestyle.*") (emphasis added); ***391** *see also Burke,* 718 F.Supp. at 1141 (rejecting all-records argument pertaining to art gallery in part because the affidavit itself made clear that there was "probable cause to believe that mail fraud and wire fraud *involving the sale of purported fine art prints by Salvador Dali,* had been committed" by the subject gallery) (emphasis in original) (internal quotation marks and alterations omitted).

The Garwood Affidavit, for its part, fell especially short of making the heightened showing required to authorize the seizure of all records from the Wey Apartment. Even incorporating as it did the Komar Affidavit, the Garwood Affidavit nowhere approached a "demonstrat[ion]" from which one could draw the reasonable inference that Wey's "entire life [was] consumed by fraud." *Falon,* 959 F.2d at 1148. Nor did it aver that NYGG's allegedly fraudulent business activities were in any way "centered" on the Wey Apartment, *id.,* or that there "was considerable overlap between [Wey's] personal and business lives," *Cherna,* 184 F.3d at 409 (citing *Humphrey,* 104 F.3d at 68–69). To the contrary, the Garwood Affidavit's probable cause showing as to the Wey Apartment itself was, all things considered, relatively narrow, focusing principally on allegations that: (i) Michaela Wey often performed "bookkeeping" and "payroll" functions for NYGG from the Wey Apartment, where she "sometimes mail[ed] checks"; (ii) Deer stock certificates had been sent to the Wey Apartment in April 2009; and (iii) Wey's sister had purportedly executed suspicious electronic fund transfers to personal accounts in the name of Michaela Wey. Garwood Aff. ¶¶ 6–12. Such a showing might well justify the seizure of materials pertaining to the purported scheme outlined in the Komar Affidavit, but it most assuredly did not rise to the level of supporting an all-records authorization.

Further belying the suggestion that the all-records exception excuses the Warrants' lack of particularity, the evidence before the Court indicates that the Government neither intended to seek formal authority to seize all records from NYGG and/or the Wey Apartment nor understood itself at any time—until perhaps it joined issue on the instant motion—to be in possession of any such authority. The Komar and Garwood Affidavits nowhere made the explicit assertion that NYGG—or any other Wey-linked business operation for that matter—was permeated by fraud. They also did not explicitly request permission to execute an all-records seizure. *See,*

e.g., *Vilar,* 2007 WL 1075041, *21 ("[T]he Affidavit itself makes no explicit allegation that the [subject] entities were permeated with fraud."). Moreover, apart from AUSA Massey's somewhat rote incantations on direct examination at the Hearing that NYGG was "permeated with fraud" at the time of the Searches, Hearing Tr. 13:10–15—assertions that the Court found too rehearsed to be persuasive[8]—the Government's witnesses testified across the board that the Warrants covered something less than all records from either location (although, as discussed further below, they also struggled to articulate any limiting principle) and they had no recollection of actually applying for all-records authorization. *See, e.g., id.* 47:4–8 (**Q.** "Is it fair to say, sir, that Exhibit A was an attempt by you to cover basically every form or format of material that could be found in a location from notes, handwritten notes, scraps of paper, every form of item that could be found?" **A.** "No, that's not correct.") ***392** (Massey); *id.* 33:5–8 (**Q.** "What I'm trying to figure out from your testimony, sir, is whether you are testifying that you actually made the [Warrant] application pursuant to the [all-records] doctrine or not?" **A.** "I don't recall. I simply don't recall."); *id.* 188:16–18 (**Q.** "Never occurred to you that [the NYGG Warrant] might be a warrant that covered everything in the office?" **A.** "I don't feel it covered everything in the office.") (Komar); *see also id.* 40:4–10 (**Q**: "... do you believe that your understanding of the business gave you the right to seize every record at the home of Benjamin and Michaela Wey?" **A.** "No.") (Massey). As several courts outside this Circuit have recognized, "if the [G]overnment is relying upon the 'permeated with fraud' exception to support an application for an otherwise overly-broad search warrant, it should state so in the application rather than attempting a post-hoc rationalization." *United States v. Bridges,* 344 F.3d 1010, 1020 (9th Cir. 2003) (Thomas, J., concurring in pertinent part); *cf.* *Abrams,* 615 F.2d at 544 ("If, as the government urges, the affidavit information called for all ... of the Medicare-Medicaid records in the offices, then the warrant should have said so."); *United States v. Winn,* 79 F.Supp.3d 904, 920 (S.D. Ill. 2015) ("The bottom line is that if [the applying officer] wants to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to [Defendant's] criminal activity, and he did not do so.").

In all of these ways, the circumstances here are readily distinguishable from those presented in *D'Amico,* the case on which the Government relies to advance its all-records argument. Opp. at 36–37. There, the FBI not only expressly sought permission to seize "all documents relating to" the business to be searched, but it also established in its warrant application that the subject business, while perhaps engaging in some attempt to sell energy drinks as a side operation, had specifically been created to, and did, serve primarily as a front for the laundering of proceeds generated by illicit mafia operations. 734 F.Supp.2d at 356–62. For that matter, the circumstances here differ more generally from the typical cases in which the all-records exception is applied in this Circuit: those "involv[ing] rampant misconduct and little, if any, legitimate business activities." *Vilar,* 2007 WL 1075041, at *21 (collecting cases); *see also* *Zemlyansky,* 945 F.Supp.2d at 461 ("In cases where the all records exception has been applied, the affidavit submitted in support of the warrant contained detailed information that would provide reason to believe that all or nearly all of the business under investigation was illegal."); *Burke,* 718 F.Supp. at 1139–1140 (surveying case law and noting that evidence sufficient to invoke all-records exception tends to "consist of a large number of fraudulent transaction or of documentation—in the form of information gleaned from interviews with former employees or from undercover surveillance of the operation—that the entire operation is a scam").

More instructive here are cases like *Hickey* and *Burke.* In *Hickey,* four corporations were allegedly involved in a RICO, fraud, and money laundering scheme centered on controlling and exploiting commercial garbage operations in the Town of Islip, New York (the "Islip fraud"). 16 F.Supp.2d at 226. Law enforcement agents obtained warrants to seize "all business records" of each of the four entities. *Id.* at 237. The court invalidated the warrants, concluding as pertinent here that they were not salvageable under the all-records exception because the warrant application's probable cause showing focused on ***393** the "core criminality" targeted by the investigation—the "one overriding scheme" represented by the Islip fraud—and lacked sufficient information to suggest that the "other operations of the defendant corporations" were

"similarly corrupted." *Id.* at 240–241. And in *Burke,* the court refused to apply the all-records exception to warrants to search offices of Barclay Galleries, even though the underlying affidavits identified six fraudulent transactions involving Salvador Dali prints and several related fraudulent statements and misrepresentations, and averred, based on information from confidential sources, that the offices housed a "a boiler room operation." 718 F.Supp. at 1138–40. Judge Mukasey observed that "[n]otably absent" from the affidavits was "any indication that the government believed ... that Barclay's sale of non-Dali artwork was also fraudulent or that Barclay's sale of fraudulent Dali artwork represented just a sample of its pervasively fraudulent sales," and that the Government made no "showing that the sale of Dali prints was inseparable from the sale of print by other painters." *Id.* at 1140–41.

The instant facts are analogous. The Komar and Garwood Affidavits unquestionably establish probable cause to search for and seize *something*: for example, materials pertaining to the specific entities and individuals purportedly implicated as Issuers or Nominees in the five to six transactions on which the Affidavits focused. They fall short, however, of establishing the requisite probable cause to believe that Wey's entire business operation was a scam, so as to justify the seizure of all records from either NYGG or the Wey Apartment.

For the foregoing reasons, the Court concludes that both Warrants lack particularity and that shortcoming is not excused under the all-records exception.

2. The Search Warrants Are Overbroad

[20] As noted above, "breadth and particularity are related but distinct concepts." *Ulbricht,* 858 F.3d at 102. The former issue is "whether the items listed as 'to be seized' in the warrant were overboard because they lacked probable cause" and the second is "whether the warrant was sufficiently particularized on its face to provide the necessary guidelines for the search by the executing officers." *Hernandez,* 2010 WL 26544, at *7 (citations omitted); *see also* *Cohan,* 628 F.Supp.2d at 359 ("A warrant ... can be unconstitutionally infirm in two conceptually distinct but related ways: either by seeking specific material as to which no probable cause exists, or by giving so vague a description of the material sought as to impose no meaningful boundaries."). For many of the same reasons set forth above, the NYGG Warrant and the Apartment Warrant are constitutionally overbroad. Specifically, owing in large measure to their failure to impart meaningful guidelines to the searching agents (a particularity problem), the Warrants purport to authorize the seizure of, essentially, all documents from NYGG and the Wey Apartment. As demonstrated in the foregoing discussion of the all-records exception, however, such authorization exceeds the scope of the probable cause showing submitted to the Magistrate Judge. That is an independent (if related) overbreadth problem.

The Court is, of course, mindful of the deference generally owed to a magistrate's probable cause determinations, and it has no doubt that Magistrate Judge Dolinger was correct insofar as he found probable cause to believe that some subset of the materials likely located within the NYGG offices and the Wey Apartment could constitute evidence of criminal activity. But the sheer scope of the Warrants—reaching, ***394** as shown above, essentially all documents pertaining to NYGG and/or the Weys unlimited by relevance to criminal conduct or by timeframe—precludes a finding that the seizure authorization remained within the bounds of the Government's probable cause showing. The Court cannot agree, to take but a few straightforward examples, that the Affidavits support the sweeping seizure of all "notes" "relating to" NYGG, or all "correspondence" and "photographs" "concerning" either one of the Weys. *See* NYGG Warrant Exs. A–B; Apartment Warrant Exs. A–B. Simply put, the Warrants are, in essence, all-records warrants unsupported by probable cause to seize all records. That constitutes a violation of the Fourth Amendment.

C. The Good Faith Exception Does Not Save the Searches

[21] The Government argues strenuously that, even assuming the Warrants are constitutionally deficient, the good faith exception properly applies to the execution of both Searches, thus precluding suppression of the Search fruits. Opp. at 38–41; Supplemental Memorandum of Law in Opposition to Defendant's Motion to Suppress Evidence, Dkt. 86 ("Gov't Supp. Opp."), at 13–17. For the following

reasons, and based on its factual findings following the two-day Hearing, the Court rejects this argument.

1. Background Law on the Exclusionary Rule and the Good Faith Exception

The Fourth Amendment "contains no provision expressly precluding the use of evidence obtained in violations of its commands." *Arizona v. Evans*, 514 U.S. 1, 10, 115 S.Ct. 1185, 131 L.Ed.2d 34 (1995). Nevertheless, the Supreme Court has "establish[ed] an exclusionary rule that, when applicable, forbids the use of improperly obtained evidence at trial." *Herring v. United States,* 555 U.S. 135, 139, 129 S.Ct. 695, 172 L.Ed.2d 496 (2009). "[T]his judicially created rule is 'designed to safeguard Fourth Amendment rights generally through its deterrent effect.' " *Id.* at 139–40, 129 S.Ct. 695 (quoting *United States v. Calandra,* 414 U.S. 338, 348, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974)).

Still, "[t]he fact that a Fourth Amendment violation occurred —*i.e.,* that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rules applies." *Id.* at 140, 129 S.Ct. 695. To the contrary, the Supreme Court has repeatedly noted that "exclusion 'has always been our last resort, not our first impulse.' " *Id.* (quoting *Hudson v. Michigan,* 547 U.S. 586, 591, 126 S.Ct. 2159, 165 L.Ed.2d 56 (2006)). In keeping with that admonition, the Supreme Court has recognized several "important principles that constrain application of the exclusionary rule." *Id.* "First, the exclusionary rule is not an individual right and applies only where it 'results in appreciable deterrence' " of "Fourth Amendment violations in the future." *Id.* at 141, 129 S.Ct. 695 (additional internal quotation marks and brackets omitted) (quoting *Leon*, 468 U.S. at 909, 104 S.Ct. 3405); *see also Raymonda,* 780 F.3d at 117 ("Neither a personal constitutional right nor a means to redress the injury of an unconstitutional search, the exclusionary rule is designed to deter future Fourth Amendment violations.") (internal quotation marks omitted). And second, "the benefits of deterrence" must "outweigh" the often "substantial social costs" of "letting guilty and possibly dangerous defendants go free." *Herring,* 555 U.S. at 141, 129 S.Ct. 695 (internal quotation marks and citations omitted); *see also Pa. Bd. of Probation & Parole v. Scott,* 524 U.S. 357, 364–65, 118 S.Ct. 2014, 141 L.Ed.2d 344 (1998) (the exclusionary rule's "costly toll upon truth-seeking and law ***395** enforcement objectives presents a high obstacles for those urging application of rule") (internal quotation marks omitted). Thus, in order "[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring,* 555 U.S. at 144, 129 S.Ct. 695. Such deterrence interests are most often implicated by "deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." *Id.* Conversely, when police conduct "involves only simple, isolated negligence, exclusion simply cannot pay its way." *Raymonda,* 780 F.3d at 118 (internal quotation marks omitted).

[22] **[23]** **[24]** The so-called "good faith exception" to the exclusionary rule embodies these principles. That doctrine provides that "evidence obtained by officers in objectively reasonable reliance on a warrant subsequently invalidated by a reviewing court is not generally subject to exclusion." *Id.* (internal quotation marks omitted). "Likewise government agents act in good faith when they perform 'searches conducted in objectively reasonable reliance on binding appellate precedent.' " *Ganias,* 824 F.3d at 236 (quoting *Davis v. United States,* 564 U.S. 229, 232, 131 S.Ct. 2419, 180 L.Ed.2d 285 (2011)). Lest there be any doubt on the matter, the Second Circuit has recently admonished that "such reliance" must actually be "*objectively reasonable.*" *Id.* at 221 (emphasis in original). That requirement generally demands "that the officer exhibit 'reasonable knowledge of what the law prohibits.' " *Raymonda,* 780 F.3d at 119 (quoting *George,* 975 F.2d at 77); *see also Leon*, 468 U.S. at 919, 104 S.Ct. 3405 (" 'evidence obtained from a search should be suppressed only if ... the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional' ") (quoting *United States v. Peltier,* 422 U.S. 531, 95 S.Ct. 2313, 45 L.Ed.2d 374 (1975)). And the " 'inquiry is confined to the

objectively ascertainable question whether a reasonably well trained office would have known that the search was illegal' in light of 'all the circumstances.' " *Herring,* 555 U.S. at 145, 129 S.Ct. 695 (quoting *Leon,* 468 U.S. at 922 n.23, 104 S.Ct. 3405). [9]

[25] As a corollary of sorts to the objective reasonableness requirement, the good faith exception "cannot shield even an officer who relies on a duly issued warrant in at least four circumstances: '(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.' " *Raymonda,* 780 F.3d at 118 (quoting *United States v. Clark,* 638 F.3d 89, 100 (2d Cir. 2011)); *see also George,* 975 F.2d at 77 ("[r]easonable reliance does not allow an officer to conduct a search with complete disregard of the warrant's validity because the standard of reasonableness is an objective one") (internal quotation marks and alterations omitted).

" 'The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance' on an ***396** invalidated warrant." *Clark,* 638 F.3d at 100 (quoting *George,* 975 F.2d at 77).

2. Background Law on the Good Faith Exception in the Context of Insufficiently Particularized Warrants

The Supreme Court has long recognized that " 'a warrant may be so facially deficient—*i.e.,* in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.' " *Groh,* 540 U.S. at 565, 124 S.Ct. 1284 (quoting *Leon,* 468 U.S. at 923, 104 S.Ct. 3405). In *Groh,* the Supreme Court had occasion, in the context of a *Bivens* action, to apply that admonition.

Specifically, the *Groh* Court considered whether a federal agent was entitled to qualified immunity despite having executed a search warrant that was facially deficient for lacking a particularized description—or indeed any description at all—of the items to be seized. 540 U.S. at 557–65, 124 S.Ct. 1284. After noting that the "the same standard of objective reasonableness that [is] applied in the context of a suppression hearing ... defines the qualified immunity accorded an officer," the *Groh* Court answered in the negative, concluding that "[g]iven that the particularity requirement is set forth in the text of the Constitution, no reasonable officer could believe that a warrant that plainly did not comply with that requirement was valid." *Id.* & n.8 (internal quotation marks and citation omitted). Notably, and as discussed above, the *Groh* Court reached that conclusion after rejecting the defendant officer's argument that "the goals served by the particularity requirement" had been "otherwise satisfied" by particularized (but unincorporated) warrant application papers and by the agent's own "restraint" in keeping the "scope" of the ultimate "search [from] exceeding the limits set forth in the application." *Id.* at 557–62, 124 S.Ct. 1284. [10]

Six years later, in *Rosa,* the Second Circuit recognized that *Groh* had "disallow[ed] consideration of unattached and unincorporated supporting documents to cure an otherwise defective search warrant," and accordingly deemed the warrant in question insufficiently particularized on its face —notwithstanding that it had issued on the strength of a more detailed (but unincorporated) affidavit—because it "fail[ed] to link the items to be searched and seized to the suspected criminal activity." 626 F.3d at 58–59, 62–64 (2d Cir. 2010) (also noting that the warrant was "overbroad and provided the officers with no judicial limit on the scope of their search" and, accordingly, "fail[ed] for lack of particularity"). Nevertheless, the *Rosa* Court held that the good faith exception saved the fruits of the search from exclusion. *Id.* at 64–66. Citing the deterrence and culpability principles highlighted by the Supreme Court in its then-recent *Herring* decision (and discussed above), the Second Circuit concluded—on what has aptly been

described as the "highly unusual facts"[11] of the *Rosa* case—that even though the officers executed a warrant that on its face did not comply with the Fourth Amendment's particularity requirement, there was "nothing to suggest deliberateness and culpability on the [their] part," that ***397** they "acted reasonably" under the circumstances, and that the exclusionary rule would thus "serve little deterrent purpose" moving forward. *Id.*

In support of that determination, the *Rosa* Court pointed to several fact-specific considerations: (i) that the warrant application, issuance, and execution had all occurred under intense "time pressures" in "the three hours from 2:00 to 5:00 am" of a single morning; (ii) that the application's affiant led the execution team and was later responsible for searching recovered digital media; (iii) that there was "no evidence that ... [the] officers actually relied on the defective warrant, as opposed to their knowledge of the investigation and the contemplated limits of the town justice's authorization, in executing the search"; and (iv) that there was "no evidence that the team of officers searched for, or seized, any items that were unrelated to the crimes for which probable cause had been shown" in the application. *Id.* Emphasizing repeatedly that it operated "[u]nder the facts" and the "circumstances of th[is] case" and that "application of the exclusionary rule will vary in accordance with the facts of each case," the Court found the "requisite levels of deliberateness and culpability justifying suppression" to be "lacking." *Id.*

In *Zemlyansky,* a district court opinion issued three years after *Rosa,* Judge Oetken engaged in a thoughtful and persuasive synthesis of the *Groh,* *Herring,* and *Rosa* decisions. Ultimately, *Zemlyansky* concluded, "the culpability standards and deterrence considerations that form the heart of *Herring's* good faith inquiry will ordinarily, though not always, be satisfied where a police officer acted in an objectively unreasonable manner by violating clearly established Fourth Amendment law," but there are at least "some circumstances" in which "there will be daylight between (1) a finding that an officer acted in an objectively unreasonable manner and (2) a finding that the deterrence and culpability concerns identified in *Herring* weigh in favor of suppression." 945 F.Supp.2d at 469–70 (also cautioning that "these factors will likely align in the vast majority of cases where the applicable Fourth Amendment law is clearly established"). Accordingly, in Judge Oetken's view, "courts must independently test each requirement before suppressing." *Id.* at 469. That is, the "Court must first consider whether the officers in this case acted in an objectively reasonable manner. If the answer to that question is no, and if the officers violated clearly established law, then the Court must determine whether the officers nonetheless fall into the narrow gap described in *Rosa* between violations of clearly established law and circumstances where an officer's conduct nonetheless constituted isolated negligence." *Id.* at 472.

This Court finds the *Zemlyansky* framework to be consistent with the repeated signals from the Court of Appeals in recent years that objective unreasonableness and deterrence value are independent (though related) factors to be considered separately, and that the absence of either one may suffice to bring police conduct within the good faith exception. *See, e.g.,* *Ganias,* 824 F.3d at 236–37 (exclusionary rule will not apply if government agents acted in "objectively reasonable good faith reliance" on a warrant or binding appellate precedent or if the "benefits of deterring the Government's unlawful actions" do not "appreciably outweigh" the costs of suppression); *see also Romain,* 678 Fed.Appx. at 24–27, 2017 WL 442175, at *1–2. Accordingly, the Court will apply that framework here.

3. There Could Be No Objectively Reasonable Reliance on the Facially Unparticularized Warrants

As the Supreme Court has made clear, the objective reasonableness standard in ***398** the context of the good faith exception is "the same" as that applicable to assessments of qualified immunity. *Groh,* 540 U.S. at 565 n.8, 124 S.Ct. 1284 (quoting *Malley v. Briggs,* 475 U.S. 335, 344, 106 S.Ct. 1092, 89 L.Ed.2d 271 (1986)). In turn, "[w]hether an official protected by qualified immunity may be held personally liable for an allegedly unlawful action" generally

depends "on the objective legal reasonableness of the action, assessed in light of the legal rules that were clearly established at the time it was taken." *Messerschmidt v. Millender,* 565 U.S. 535, 546, 132 S.Ct. 1235, 182 L.Ed.2d 47 (2012) (internal quotation marks and alterations omitted) (quoting *Anderson v. Creighton,* 483 U.S. 635, 639, 107 S.Ct. 3034, 97 L.Ed.2d 523 (1987)).

As set forth above, the NYGG Warrant and the Apartment Warrant both on their face plainly violate multiple components of the Fourth Amendment's particularity requirement as construed by the Supreme Court and the Second Circuit. At a minimum, neither identifies in any way the crimes under investigation. And both authorize the seizure of multiple expansive categories of records (e.g., "notes," "memoranda," "correspondence," "communications," "photographs," etc.) without any meaningful linkage to the suspected criminal conduct and limited only, at the outer boundaries, to some relationship to the owner/occupant of the premises being searched. Each of these deficiencies runs afoul of principles that had already been clearly established in binding precedents when the Warrants were issued and Searches conducted. *See, e.g., George,* 975 F.2d at 76 (2d Cir. 1992) (no identification of crimes); *Bianco,* 998 F.2d at 1115–16 ("highly generalized" and "broad" categories of documents not "tied to particular crimes" or subject to "more particular limiting language"); *Buck,* 813 F.2d at 590–93 & n.2 ("catch-all" descriptions of categories of items to be seized without meaningful limiting language); *Rosa,* 626 F.3d at 62; (lack of linkage to suspected criminal activity or other meaningful parameters on search); *see also Zemlyansky,* 945 F.Supp.2d at 472 (collecting pre-2012 cases); *Vilar,* 2007 WL 1075041, at *22 (same). Both the Supreme Court and the Second Circuit had already made abundantly clear, moreover, that such deficiencies could not be cured by the unincorporated, unattached Komar and Garwood Affidavits. *See Groh,* 540 U.S. at 557–58, 124 S.Ct. 1284; *Rosa,* 626 F.3d at 62–64. Finally, and as discussed further below, the record reflects no evidence that the agents' failure to recognize these infirmities may be attributed to exigent or otherwise unusual circumstances that existed when the Affidavits or the Warrants were drafted or the Searches conducted. *Cf. Groh,* 540 U.S. at 565 n.9, 124 S.Ct. 1284 ("[P]etitioner does not contend that any sort of exigency existed when he drafted the affidavit, the warrant application, and the warrant, or when he conducted the search. This is not the situation, therefore, in which we have recognized that 'officers in the dangerous and difficult process of making arrests and executing search warrants' require 'some latitude.' ") (quoting *Maryland v. Garrison,* 480 U.S. 79, 87, 107 S.Ct. 1013, 94 L.Ed.2d 72 (1987)).

To be sure, when an "alleged Fourth Amendment violation involves a search or seizure pursuant to a warrant, the fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner." *Messerschmidt,* 565 U.S. at 546, 132 S.Ct. 1235. But the mere presence of a warrant "does not end the inquiry into objective reasonableness." *Id.* at 547, 132 S.Ct. 1235. When, as here, a warrant plainly ***399** fails to comport with well-settled particularity requirements, officers' reliance upon it—especially in the absence of a credible circumstance-specific explanation—can hardly be deemed objectively reasonable. *See, e.g., George,* 975 F.2d at 78 ("in light of the settled nature of the law concerning the failure for lack of particularity of warrants authorizing the search for 'evidence' limited only by reference to 'a crime,' " the subject warrant was "the type of facially invalid warrant that could not have been relied upon in good faith because one who simply looked at the warrant would suspect it was invalid") (internal quotation marks, alterations, and citation omitted); *Hickey,* 16 F.Supp.2d at 244 (executing officers could not reasonably rely on warrants that were so lacking in particularity as to be "general in nature"); *United States v. One Parcel of Prop. Located at 18 Perkins Road, Woodbridge, Conn.,* 774 F.Supp. 699, 707 (D. Conn. 1991) ("Courts commonly refuse to find good faith reliance when the warrant is too broadly worded or its terms so vague or unspecific that it fails to distinguish adequately between items that are evidence of a crime and innocent possessions.") (internal quotation marks and brackets omitted). [12]

4. Culpability in Execution and Deterrence Considerations Weigh in Favor of Suppression

a. The *Rosa* Factors

The Court next considers the impact of the factors highlighted in *Rosa.* Specifically, it asks whether those factors operate here to render the officers' conduct in applying for or executing the Warrants insufficiently culpable for suppression to carry meaningful deterrence benefits or otherwise support a finding that any such benefits would not be worth the " 'price paid by the justice system.' " *Rosa,* 626 F.3d at 64 (quoting *Herring,* 555 U.S. at 144, 129 S.Ct. 695). In light of its factual findings and for the reasons set forth below, the Court concludes that they do not.

i. Exigency

As alluded to above, exigency, arguably the most critical *Rosa* factor, is entirely absent from this case. *See* *Rosa,* 626 F.3d at 64–66 (repeatedly citing the "time pressures" under which the warrant was obtained and executed and the "necessary speed" with which the officers acted in the "three hours from 2:00 am to 5:00 am"). Indeed, in stark contrast to *Rosa,* there is no dispute here that AUSA Massey and Agent Komar had been leading an investigation into NYGG and Wey for a substantial period of time prior to the Searches and prepared the NYGG Warrant application over the course of "weeks," if not "months." Hearing Tr. 30:23–31:4. Agent Komar conceded that once the NYGG Warrant issued, the FBI had a 10–day window in which to execute it—10 days in which, for example, all members of the NYGG Search team could have reviewed the Komar Affidavit—but it chose, for reasons not clear from the record, to proceed the following day. *Id.* 186:3–25.

In addition, the Searches themselves were not constrained by lack of time or resources. To the contrary, each Search lasted between four and five hours (with every indication that even more time could have been taken, if necessary), each Search was conducted by a team of some seventeen to twenty FBI agents, and, as Government witnesses noted at the Hearing, ***400** neither Search team had to contend with a "substantial" volume of hard-copy materials found onsite. *See supra* Sections I.D.1.–3. Agent Komar testified that the NYGG Search team had more than enough time to review every single hard-copy document found in the NYGG offices onsite. Hearing Tr. 133:14–134:13. Following the physical Searches, moreover, FBI personnel evinced no particular hurry about reviewing the recovered electronic evidence; as discussed, comprehensive pertinence review of that material did not begin for almost a year and half. *See supra* Section I.D.4.

Under these circumstances, the Court finds, as a factual matter, that the actions of the FBI agents in obtaining and then executing what were essentially general warrants, cannot credibly be attributed to some reasonable oversight or accident made under time pressure or otherwise driven by exigency.

To the extent that the Government tried to establish at the Hearing that the Apartment Search, at least, proceeded under time constraints presented by Michaela Wey's frustrations over the Search team's presence in her residence, the Court was unpersuaded. First, Agent McGuire testified that the FBI addressed Michaela Wey's concerns about the imminent return of her children with the "fairly simple solution" of completing its search of the children's rooms and play area first, specifically so that the remainder of the Search could be completed out of the children's presence. Hearing Tr. 255:19–256:4. More fundamentally, given the significant intrusion that inheres in any law enforcement search of the home in particular, it simply cannot be that a resident's impatience with FBI agents in her apartment, in and of itself, affords the Government cover to claim that any constitutional deficiencies reflected in its search were the product of rushed execution.

ii. Komar's Presence During the Searches

Second, while there can be no doubt that Agent Komar led both Search teams and was physically present on the scene for at least substantial portions of both Searches, the Government presented vanishingly little evidence that Komar's involvement *actually impacted* the overwhelming

majority of seizure decisions made by FBI personnel executing the Warrants (which, as discussed further below, often resulted in the seizure of materials well beyond the scope of the Warrant applications). As noted above, Komar personally searched narrowly limited areas of the NYGG offices (the outer reception area) and the Wey Apartment (a guest room and portions of the children's rooms), and he seized only a few items relative to the overall Search take. *See supra* Sections I.D.2.–3. Although Komar testified that he generally recalled answering questions from team members regarding seizure decisions—testimony that the Court found, by and large, too vague and canned to be particularly persuasive—he could cite essentially no examples of instructions *not* to seize any materials based on non-responsiveness to the Warrants or the Warrant applications. And beyond that, the Government introduced zero evidence that Komar imposed any field constraints on the discretion of the agents who seized the overwhelming majority of the materials recovered from both locations. There was no suggestion, as noted above, that Komar directly supervised or double-checked any seizure decisions. Indeed, ASUA Massey testified that, to his understanding, seizure decisions were generally left to individual agents' "discretion," Hearing Tr. 67:18–68:20, and Agent McGuire (the only agent who seized a substantial ***401** portion of materials during either Search to appear as a Government witness at the Hearing) testified that he did not recall consulting any of his colleagues before making seizure decisions and generally made such calls based on his own understanding of the NYGG Warrant, *id.* 243:17–247:23, 298:13–299:1.

Based on the evidence before it, the Court simply cannot conclude that Agent Komar, while undisputedly onsite during both Searches, in fact meaningfully discharged any "respons[ibility] for ensuring that the items seized were within the scope of the approved search." *Rosa,* 626 F.3d at 59. Especially in light of *Groh's* rejection of the proposition that an agent may make up for a warrant's lack of particularity even by actually making certain that the search itself "did not exceed the limits intended by the Magistrate," 540 U.S. at 558–59, 124 S.Ct. 1284, the Court certainly does not read *Rosa* to suggest that an affiant's mere presence during a search may serve as a talismanic cure-all that automatically brings the execution of a grossly unparticularized warrant within the good faith exception. Accordingly, the second *Rosa* factor—Komar's personal involvement in the Searches themselves—has, at best, limited application here.

iii. Non–Reliance on the Defective Warrants

Third, and closely related, the Hearing failed to provide, and the record is otherwise devoid of, any credible evidence tending to show that the searching agents, in practice, cabined their own seizure discretion by "the contemplated limits of the search[es]," asset forth in the Komar and Garwood Affidavits, as opposed to by the four comers of the unparticularized Warrants themselves. *Rosa,* 626 F.3d at 64–66 (emphasizing, with approval, that the searching officers relied on "their knowledge of the investigation and the contemplated limits of the town justice's authorization," rather than "actually rel[ying] on the defective warrant"). As discussed, nothing in the record suggests that any of the more than twenty agents who participated in at least one of the Searches, other than Agents Komar and Garwood themselves, actually reviewed the Komar Affidavit or Garwood Affidavit prior to the Searches. And, critically, nothing suggests that the search team was ever otherwise informed of many of the critical limiting details set forth in those Affidavits, such as which particular Issuers and Nominees were thought to be implicated in Wey's suspected scheme and the nature of their suspected involvement.

The Government maintains that the Operations Order and the pre-operations briefing led by AUSA Massey and Agent Komar provided the executing agents with sufficient information about the ongoing investigation "to be absolutely sure that the search team understood the scope" of, at least, "the NYGG Warrant." Gov't Supp. Opp. at 14. Even bracketing that it is the searching agents' grasp of the scope of the Warrant *applications*—rather than the scope of the Warrants themselves (which was essentially limitless)—that is the relevant consideration here, the Government's contention suffers from at least two critical flaws.

First, the Government provided no credible evidence suggesting that anything beyond high-level generalities was actually conveyed to the executing officers through the Operations Order or briefing. The Operations Order, as

discussed, contained only two short paragraphs setting forth any substantive information at all about the investigation or the objectives of the NYGG Search, and that information amounted to, at best, a 30,000–foot summary—especially when contrasted with the detail set forth in the (unread, it appears) ***402** Komar Affidavit. The Order failed, for example, to identify any of the Issuers implicated in the suspected investigation, to in any way explain the relevance of the individuals and entities listed in Exhibit B, or to otherwise meaningfully link the items to be seized to the suspected crimes. *See* Gov't Ex. 1. For its part, the substantive portion of the pre-operation briefing consisted, according to Agent McGuire (the only beneficiary of the briefing called at the Hearing) of a "big-picture overview" of the investigation and the suspected criminal conduct, which he characterized as consistent with a "fairly typical securities fraud case." Hearing Tr. 239:17–21. Massey and Komar, who led the session, traded in similar generalities during the Hearing, largely failing to provide the Court with any insight as to the specific information conveyed to the agents in attendance. *See, e.g.,* Hearing Tr. 69:6–13 (Massey testifying that he did not "have a recollection of what I actually said" at the briefing); 124:12–15 (Komar testifying that Massey gave "examples of what we believed the scheme was essentially that we were investigating and communicat[ed] what types of documents ... we were going to be looking for"). [13]

Second, even if the general gist of the Wey/NYGG investigation was arguably conveyed by the Operations Order and the case "overview" provided at the briefing, nothing suggests that any such instruction guided the agents' seizure decisions more so than did the Warrants' own sweeping terms. If anything, the Hearing testimony was generally to the contrary. AUSA Massey testified that the searching agents were tasked with exercising their "discretion" in "follow[ing] *what was in the warrant*"—not with executing some more limited vision of that document based on the Affidavits, the Operations Order, or the briefing. Hearing Tr. 68:12–20 (emphasis added). Agent McGuire—it bears repeating, the only search team member other than Komar to appear at the Hearing—testified that he made seizure decisions simply by referencing Exhibit B to the Warrants (the list of relevant individuals and entities that included NYGG and the Weys) and asking whether documents were "responsive to the search warrant" itself. Hearing Tr. 243:17–247:23. When later searching the electronically stored evidence, McGuire further testified, he made decisions about what to electronically "seize"—i.e., to tag as pertinent—based on whether they "covered by the warrant or not." *Id.* 292:9–21. Even Agent Komar himself, who conducted a limited initial review of a portion of the electronically stored evidence, asserted in a sworn declaration in support of the Government's original opposition to Wey's suppression motion that his review sought materials "falling within the parameters of the NYGG Warrant and the [Apartment Warrant]—that is, electronic documents and records of the kinds described in Exhibit ***403** A to the NYGG Warrant and the [Apartment Warrant] which concerned any of the entities or individuals in Exhibit B to those warrants." Komar Dec. ¶ 21. [14]

Consistent with that testimony, Government witnesses at the Hearing explicitly justified arguable examples of overseizure as falling "within the scope of the warrant." *See, e.g., id.* 56:20–57:7. For example and as noted above, AUSA Massey opined that medical prescription information sheets were subject to seizure under the relevant Warrant because they were related to the Weys' "personal expenses." *Id.* Massey similarly found "spreadsheets characterizing family medical issues" to be "within the scope of the warrant." *See* Def. Ex. 4 (e-mail memorandum from Massey). These candid concessions critically undermine, in the Court's view, the Government's post-hoc legal contention that the officers' discretion was meaningfully bounded by independent knowledge of the investigation.

The constitutional problem follows directly. The Warrants simply could not provide the requisite guidance to the searching officers because, as discussed at length above, they by their plain terms authorized the seizure of any record related to NYGG and/or the Weys. Critically, moreover, the record evidence reflects that is precisely how the Warrants were interpreted in practice by the Government agents responsible for their preparation and execution. As noted, AUSA Massey could think of no records beyond the scope of Exhibit A to Warrants (which listed the sorts of materials subject to seizure) other than "evidence ... of child pornography," illegal drug paraphernalia (but only if it did not have a written reference to NYGG on it), and an "al-Qaeda manifesto." Hearing Tr. 40:10–15, 48:2–10, 50:10–20. On the flip side, he agreed that "all the records of [NYGG] ... were in play" and subject to seizure, 14:8–10, 50:10–11, and that any "note," "memoranda," or "videotape"—even if

decades old—was seizable if related to an individual or entity listed on Exhibit B, *id.* 46:23–47:3. Agent McGuire, for his part, thought it "very clear" that the Warrants covered, for example, "any financial records pertaining to the [Weys]," as well as all "financial records related to [NYGG]" and all "e-mails with [NYGG]." *Id.* at 276:12–20, 293:3–18, 304:11–14. On this record, the Court cannot find, as did the *Rosa* Court, that the scope of the Searches and the executing officers' discretion in making seizure decisions was in any way practically constrained by the limitations contemplated by the more specific Komar and Garwood Affidavits. Like any other aspect of the good faith inquiry, it is the Government's burden to establish as much, and the evidence submitted was simply unpersuasive and insufficient.

iv. Overseizure

Finally, there is the matter of overseizure. The *Rosa* Court took care to emphasize that there was "no evidence that the team of officers searched for, or seized, any items that were unrelated to the crimes for which probable cause had been shown." 626 F.3d at 65. Notwithstanding the Government's zealous efforts to persuade the Court otherwise, the same simply cannot be said here.

The agents seized, between the two search locations, a variety of hard-copy materials purely personal in nature, or otherwise plainly outside the scope of the suspected securities and wire fraud ***404** scheme described in the Affidavits.[15] As discussed above, these included medical records, prescription documents, X-rays, health care directives, educational records and scholastic mementos, divorce records, resumes, family photographs, recreational schedules, and other things. *See supra* Sections I.D.2.–3. To be sure, and as the Government emphasizes, several such items do appear to have been seized as part of larger sets of materials that could have been impractical to sort onsite (for example, the trash bag referenced above, which took something of a star turn in the Government's Hearing presentation) and thus were removed wholesale for offsite inspection. Gov't Supp. Opp. at 17. Even crediting such asserted logistical necessity as an explanation for some of these seizures, however, the record reflects that it does not apply to many others. *See, e.g.,* Def. Supp. Br. Ex. A (identifying examples); *see also* Gov't Ex. 14 (Evidence Recovery Log from Apartment Search noting seizure of multiple sets of materials identified onsite as "personal" documents, such as "school" and "immigration" records and "estate planning" documents).

In addition, it appears that following seizure, the Government completed pertinence review of these hard-copy materials by late 2012. To date, however, essentially none of the originals have been returned to NYGG or the Weys, Hearing Tr. 335:4–11, despite the requests of counsel—a potential constitutional violation in and of itself. *See, e.g., United States v. Tamura,* 694 F.2d 591, 596–97 (9th Cir. 1982) ("We likewise doubt whether the Government's refusal to return the seized documents not described in the warrant was proper."); *see also Ganias,* 824 F.3d at 230 (Chin, J., dissenting) (in cases where offsite review was required because "potentially relevant documents [were] interspersed through a large number of boxes or file cabinets," generally "non-responsive documents were to be returned after the relevant items were identified").

Perhaps more troubling than either the initial seizure or the continuing retention, however, are the efforts of the Government and its Hearing witnesses to leverage the inappropriately expansive terms of the Warrants into strained explanations of why these materials were in fact *properly* seized. *See, e.g.,* Hearing Tr. 56:17–57:7, 58:24–59:5, 59:25–60:7, 167:10–18, 304:24–305:3; Opp. at 40. Indeed, in maintaining, as discussed above, that children's school records, medical prescriptions, divorce records, and decade-old clippings from the sports section of the college newspaper among other things fell within the scope of the Warrants because they purportedly bore vague connections to the Weys' personal histories and finances, the Government and its agents leave the Court to find that much—perhaps even most—of the overseizure was not the result of expediency, mistake, or even simple negligence. To the contrary, it seems, this material was reviewed, and a conscious effort was made to deem patently unresponsive materials responsive to the Warrants. Its presence in the Search fruits thus suggests that the execution teams affirmatively wielded the nearly unfettered discretion afforded them by the Warrants' expansive terms to appropriate documents that were perhaps of interest to some broader investigation of the Weys' lives and finances but that bore little or no discernible connection to the securities fraud probable cause showing actually submitted to the

Magistrate Judge. *See, e.g.,* Hearing Tr. 276:14–20 ***405** (Agent McGuire testifying that it was "very important" that the FBI gain a better of understanding through the Searches of the Wey family's "very complex" "financial arrangements"). Put another way, it appears to be, as much as anything else, a product of the intentional execution of what amounted to general warrants.

b. The Government's Continuing Search of the Electronically Stored Evidence

This case presents still another factor, outside of the *Rosa* quartet, for evaluation in determining the Government's level of culpability and, correspondingly, its susceptibility in this context to deterrence. And it is one worth emphasizing: belying any argument that it sought to limit execution of the Warrants according to the parameters of the applications, the Government evinced no hesitation to subject the electronic Search fruits to continuing and, at least to some extent, expanding searches as its investigation and charging theories developed over the months and years following the initial Searches and preceding Wey's indictment.

As discussed above, AUSA Massey and Agent McGuire candidly testified at the Hearing that they had no qualms, for example, about searching the electronically stored evidence —well over a year after the Searches and prior to any sorting for pertinence—for evidence of tax evasion, an "alternative" charging theory not discussed in the Affidavits, apparently not developed until McGuire took over as case agent well after the Searches, and never presented to a judge. Similarly, they considered it within their authority to search the unsorted electronic materials for documents pertaining to a number of individuals and entities not identified or discussed in the Warrants or the applications but whose potential relevance to the ongoing investigation became increasingly apparent sometime after the Searches concluded (Defendant Erbek, for example). *See supra* Section I.D.4.b.

The Government maintains that this approach to reviewing the electronic evidence was entirely appropriate so long as its novel search terms were designed to identify documents that would otherwise fall within the Warrants' (inappropriately expansive) terms. Indeed, when questioned about the continuing searches at oral argument, the Government appeared to take the somewhat surprising position that it would be well within the Government's rights to search retained electronic materials that it had *already deemed unresponsive* to the Warrants using "[a]ny word" the Court could think of as a search term. It would not matter, according to the Government, whether the search bore any connection whatsoever to the actual terms of the Warrants or even how much time had elapsed since the Warrants' issuance. *See, e.g.,* Oral Argument Tr. 12:9–17:11.

As was elicited at the Hearing, moreover, it would seem that such a position was no mere hypothetical. Crediting Agent Miller's version of the pertinent events as explained above, the Court finds that in mid to late 2015 (some three-plus years after the Searches and with a grand jury presentation in the works), the FBI arranged to have Agent Miller run searches across *all* recovered electronic evidence, including that portion earlier deemed unresponsive by Agent McGuire, for documents concerning topics (again, Erbek is an example) not addressed by the Affidavits or Warrants. It evidently saw no need to prepare Agent Miller for this exercise beyond a cursory overview of the case and a review of some "examples," choosing not to arrange briefing or training on the scope of the Affidavits or the Warrants. *See supra* Section I.D.4.b.

***406** Wey urges that this conduct is independently violative of the Fourth Amendment. It may be. Regardless, the Court finds that, if nothing else, it constitutes further evidence of the agents' culpability in making affirmative choices to treat the Warrants as though they were the functional equivalent of general warrants. Such conduct can and should be deterred.

First, the record does not support the factual premise that forms the core of the Government's argument as to the propriety of these later searches: that the only documents that could be deemed pertinent—and thus electronically "seized"—during this process were those that were independently subject to seizure based on the Warrant themselves. Agent McGuire, who, as discussed, conducted searches using an expanded list of search terms in mid–2013, testified that he generally did not even review all documents returned by a term-based search before deeming them wholesale pertinent. Rather, after running such a search, he would review a sample of the returns, make a preliminary determination as to whether the search term appeared to yield at least some returns arguably within the Warrants'

scope, and then proceed to "seize" the entire set with no further document-by-document review. Hearing Tr. 289:1–20; 292:9–294:3. With respect to certain extra-Warrant search terms (such as "Erbek"), McGuire further testified that their presence in a document could be enough, in and of itself, to merit a pertinence tag based on his evolving understanding that, for example, documents pertaining to Erbek tended to concern financial matters. *Id.* 351:1–352:1. As for Agent Miller's 2015 searches, the Government simply offered no evidence through any witness with direct knowledge of the process that only documents previously identified as pertinent were tagged by Agent Miler. *See id.* 339:9–341:7 (McGuire conceding that he did not participate in the actual searches and never viewed electronic records thereof); *id.* 374:2–375:23 (Miller testifying that McGuire provided her with, at the most, two or three documents as "examples" to help guide her searches and that she then tagged as pertinent possibly as many as fifty or more documents in the FBI databases).

Furthermore, the Government cites, and the Court is aware of, no authority suggesting that simply because it has retained all originally searchable electronic materials, the Government is permitted to return to the proverbial well months or years after the relevant Warrant has expired to make another sweep for relevant evidence, armed with newly refined search criteria and novel case theories.

Perhaps most plainly problematic on this score are Agent Miller's 2015 searches which, as noted, covered all documents in the FBI databases, including those materials *already sorted out as impertinent* two years earlier. Clearly, as the defense urged at oral argument, additional physical searches in 2013 or 2015 of hard-copy documents judged irrelevant and left behind during the NYGG Search or the Apartment Search would have been presumptively impermissible—new search terms or not—in the absence of a fresh warrant. *Cf.* *Ganias,* 824 F.3d at 212–213 (recognizing that, though perhaps "imperfect," the analogy between searches of physical files and electronic files "has some force, particularly as seen from the perspective of the affected computer user," and "ha[s] some relevance" to the Fourth Amendment inquiry"). Indeed, the proper analogy to help appreciate the nature of the agents' conduct here is not the Government seizing, for example, a hard-copy notebook deemed responsive to a warrant, retaining it, and later returning to that notebook for follow-up searches as its investigation developed. Instead, Agent Miller's searches are akin ***407** to the Government seizing some hard-copy notebooks while leaving others it deemed unresponsive behind, and then returning to the premises two years later to seize the left-behind notebooks based on investigative developments but without seeking a new warrant.

The stark contrast between the Government's conduct on this front and its conduct in *Ganias*—a recent Second Circuit decision focused on the retention and search of computer data—underscores this point. In *Ganias,* agents from the United States Army Criminal Investigation Division obtained, pursuant to a warrant, forensic mirrors of all data stored on several computer hard drives in an accountant's office as part of an investigation that targeted two of the accountant's clients—but not the accountant himself. The Government searched the data and identified and segregated relevant files within a few months, but then retained all of the recovered data (not just that deemed relevant) for several more years. Approximately three years after the execution of the original warrant, the Government independently developed probable cause to believe that the accountant was personally involved in a tax evasion scheme. Understanding that it could not unilaterally re-search the mirrored data in its possession that it had previously sorted out as non-responsive to the original warrant (such as the accountant's personal financial records and records of clients not targeted by the original investigation), the Government *applied for a new search warrant* and made clear in its application that it wished to run new searches over electronic materials that had been in its custody, and assumed irrelevant, for several years. After securing and executing a fresh warrant to search that data, the Government indicted the accountant. The Circuit, sitting *en banc*, upheld the later search under the good faith exception in large measure because the Government *had acted reasonably in applying for the second warrant and alerting the magistrate to the circumstances. See* *Ganias,* 824 F.3d at 200–07, 224–26.

For the Government to skirt that new-warrant obstacle here by—appearances would suggest—intentionally taking advantage of its sweeping electronic take to look for evidence in an essentially analogous manner is inconsistent, in the Court's view, with a claim to good faith in executing the Warrants.

The Second Circuit's recent discussion of electronic searches in *Ulbricht* is not to the contrary. There, the Defendant argued in pertinent part that a warrant authorizing the search of his laptop computer was insufficiently particularized because it did not "specify the search terms and protocols" to be used in reviewing the contents of the laptop "*ex ante.*" 858 F.3d at 101–04. The Court of Appeals disagreed, reasoning that "it will often be impossible to identify in advance the words or phrases that will separate relevant files or documents before the search takes place, because officers cannot readily anticipate how a suspect will store information related to the charged crimes"—a concern that was viewed as particularly reasonable in the context of the investigation at issue, which targeted an individual suspected of running an online marketplace for illegal goods and services that "us[ed] sophisticated technology to mask its users' identities." *Id.* at 102. Here, Wey does not argue, and the Court does not conclude, that the Warrants were insufficiently particularized due to any failure of their electronic search protocols to incorporate search term lists *ex ante.* The Court fully recognizes, moreover—as the *Ulbricht* Court took care to emphasize—that privacy invasions are inevitable in searches of electronic data and that the Government may ***408** "come across personal documents ... unrelated to [the defendant's] crimes" in the course of executing such searches without running afoul of the Fourth Amendment. *Id.* at 103. But nothing in *Ulbricht,* or in any other authority of which the Court is aware, permits the Government to sit on eighteen terabytes of data for years after the expiration of the authorizing warrant and intentionally mine it with searches targeting individuals and charging theories absent from the warrant application but identified as relevant by post-search developments in the Government's investigation. It should also be noted that the warrant in question in *Ulbricht* provided robust limitations on what electronic documents could ultimately be seized, regardless of the search terms used to identify them. *See id.* at 99–104 (explaining that the warrant and the explicitly incorporated underlying affidavit, among other things, identified the relevant crimes and specifically "connect[ed] the information sought to the crimes charged"). The utter lack of similar limitations in the Warrants at issue here—especially when combined with the agents' unrestrained interpretation of their seizure authority under those Warrants—makes the Government's use of a continually expanding search term list to identify documents of interest all the more troubling as a practical matter.

* * *

As the Court of Appeals has observed, "[g]ood faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly,* 76 F.3d 1271, 1280 (2d Cir. 1996).

Government agents leading a long-running, well-resourced investigation took weeks or months to draft proposed Warrants that were plainly lacking the basic features called for by the Fourth Amendment's particularity requirement and whose scope, partially as a result, grossly exceeded the probable cause showing ultimately made to the Magistrate Judge. Upon issuance of those Warrants, the agents deployed the trappings of good faith—an Operations Order, a briefing—while dispensing with more robust safeguards such as a requirement that the search personnel read the Affidavit, and then proceeded to conduct sweeping physical and electronic searches lacking in any discernible parameter beyond the inappropriately broad terms of the Warrants themselves. Interpreting and executing their authority expansively—in keeping, the evidence suggests, with the intention of the drafters—the agents treated the Warrants both during and after the physical Searches as, for all intents and purposes, general warrants.

The Court does not conclude that the agents acted with malice. But it does find that their conduct cannot be credibly explained by exigent circumstance, by simple mistake, or by mere negligence. The agents—who are charged with reasonable knowledge of what the law prohibits—appear to have disregarded well-established constitutional principles that provide a bulwark against the execution of general warrants. That reflects, at the least, gross negligence or recklessness as to the potential for violation of the Fourth Amendment. It cannot be that a facade of particularity and reasonableness built on superficial checkmarks in the *Rosa* boxes brings that conduct within the good faith exception. Echoing Judge Oetken in *Zemlyansky,* "[t]his conduct is

deferrable, and the Constitution requires its deterrence." 945 F.Supp.2d at 476.

For these reasons, the Court cannot, on the record before it, find that the Government has carried its burden on the good faith question. The Court is mindful that "the Supreme Court [has] strongly signaled ***409** that most searches conducted pursuant to a warrant would likely fall within [the] protection" of the exception. *Clark,* 638 F.3d at 100 (citing *Leon,* 468 U.S. at 921–922, 104 S.Ct. 3405). Nevertheless, it remains "clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued." *Leon*, 468 U.S. at 922–93, 104 S.Ct. 3405 (footnote omitted); *see also* *Ganias,* 824 F.3d at 221 (reaffirming that reliance on a later invalidated warrant "must be *objectively reasonable*" to trigger the good faith exception) (emphasis in original). Finding such circumstances here and finding the conduct of the Government agents in obtaining and executing the Warrants to be both culpable and deferrable, the Court concludes that the good faith exception has no application to the Searches at issue. Accordingly, suppression is warranted.

D. Remedy

Having determined that the Warrants do not comport with the Fourth Amendment and that the Searches cannot be salvaged by the good faith exception, what remains is the question of the appropriate remedy.

As a preliminary matter, the Court recognizes the Second Circuit's directive that, to the extent possible, constitutionally infirm warrants should generally be assessed for the prospect of severability, and infirm searches for the possibility that any of the challenged evidence was in plain view when seized. *See, e.g.,* *Galpin,* 720 F.3d at 448. Here, the Government has largely waived any substantive argument as to severability, even despite an express invitation to do so at oral argument. *See* Oral Argument Tr. at 77:20–78:10. In any event, the Court easily concludes that the Warrants are not severable. The primary deficiencies described above—the lack of reference to any crime under investigation, the absence of linkage between seizable items and suspected criminal conduct, the "limitation" only by relation to the Weys or to NYGG—apply to substantially every provision of Exhibit A to both the Warrants, and, accordingly, they "taint each of the ... [W]arrants *in toto.*" *Hickey,* 16 F.Supp.2d at 244. As *Galpin* itself instructs, severance is usually "not an available remedy" if "no part of the warrant is sufficiently particularized ... or where the sufficiently particularized portions make up only an insignificant or tangential part of the warrant." 720 F.3d at 448.

As for the plain view doctrine, it is the Government's burden to demonstrate, if it so chooses, that specific seized items fall within that exception to the Fourth Amendment's requirements, and the Government here has not developed any evidentiary record that would allow the Court to reach such a conclusion. Indeed, as discussed above, the Government declined to call as Hearing witnesses the agents who actually seized the overwhelming majority of the items taken during both Searches. Accordingly, the Court cannot apply the exception to salvage any particular portion of the evidence seized during the Searches. *See, e.g.,* *United States v. Kiyuyung,* 171 F.3d 78, 83–85 (2d Cir. 1999) (rejecting plain-view argument because Government failed to develop sufficient evidentiary record).

Unable, then, to further tailor the remedy according to the severability or plain view doctrines, the Court concludes that suppression of all evidence seized during the courses of both Searches is the only appropriate recourse under the circumstances. Of some note, the Government—again given the express opportunity—declined to submit any concrete alternative remedy for the Court's consideration. *See* Oral Argument Tr. 77:4–78:10 (submitting ***410** only, in sum and substance, that "wholesale suppression ... would be too severe" and that the Court should limit any suppression "to where the Court believes the government sort of went too far or acted unreasonably"). Even in the absence of meaningful input from the Government, however, the Court recognizes the gravity of its decision and does not reach it lightly. "[W]holesale suppression," of the sort urged by Wey, is generally considered an extraordinary remedy, appropriate only when (1) government agents "effect a widespread seizure of items that were not within the scope of the warrant," and (2) "do not act in good faith." *Shi Yan Liu,* 239 F.3d at 140 (internal quotation marks and citations omitted). "[T]o satisfy the first prong ... the search conducted by government agents must *actually resemble* a general search." *Id.* at 141.

"The rationale for blanket suppression is that a search that greatly exceeds the bounds of a warrant and is not conducted in good faith is essentially indistinguishable from a general search." *Id.* at 141; *see also* *Cardwell,* 680 F.2d at 78 ("If no portion of the warrant is sufficiently particularized to pass constitutional muster, then total suppression is required. Otherwise the abuses of a general search would not be prevented.") (internal citation omitted); *United States v. Rettig,* 589 F.2d 418, 424 (9th Cir. 1978) (ordering blanket suppression where, "[a]s interpreted and executed by the agents, this warrant became an instrument for conducting a general search" and, "[u]nder the circumstances, it [was] not possible for the court to identify after the fact the discrete items of evidence which would have been discovered had the agents kept their search within the bounds permitted by the warrant"); *cf.* *United States v. Medlin,* 842 F.2d 1194, 1199 (10th Cir. 1988) ("When law enforcement officers grossly exceed the scope of a search warrant in seizing property, the particularity requirement is undermined and a valid warrant is transformed into a general warrant thereby requiring suppression of all evidence seized under that warrant.").

For all of the reasons discussed at length above, however, that scenario—unusual though it may be—is the one facing the Court. The Government took weeks or months to apply for Warrants facially lacking in particularity and so sweepingly broad in the scope of their proposed authorization as to exceed the probable cause showing submitted to the Magistrate Judge. As issued, those Warrants, by their terms, authorized essentially limitless search and seizure —targeting all documents in both the NYGG offices and the Wey Apartment, regardless of their potential connection to any criminal conduct and bounded only by the illusory "limitation" that they relate to NYGG or the Weys. The searching agents, interpreting that authority expansively and unconstrained (the Court has found) by the superficial extra-Warrant safeguards the Government trumpets as evidence of good faith, proceeded to execute the Warrants as though they were the functional equivalents of general warrants, in both their indiscriminate physical searches and seizures and, later, their expanded mining of the retained electronic take for evidence related to new persons and new crimes. This conduct reflects, at least, grossly negligent or reckless disregard of the strictures of the Fourth Amendment, and that is sufficient to infer a lack of good faith. In the Court's view, these are precisely the sort of circumstances, rare or not, that call for blanket suppression.

III. Conclusion

For the reasons set forth above, Wey's motion to suppress evidence is GRANTED in its entirety. Because the Court reaches this conclusion based on the Warrants' ***411** lack of particularity and overbreadth, it does not reach Wey's alternative arguments that the Affidavits submitted in support of the Government's warrant applications were misleading or that the Government's long-standing retention of the evidence recovered during the Searches constitutes a Fourth Amendment violation in and of itself.

In light of the suppression remedy that it hereby orders, the Court also views it as unnecessary to address Wey's application to preclude the Government from further reviewing any potentially privileged documents seized during the Searches and to compel the Government to disclose information about the review process. If the parties think otherwise, they shall set forth their respective positions in letter-briefs, not to exceed three pages in length, within fourteen days of this Order.

Wey's separate motion to seal certain evidentiary exhibits submitted in support of his post-Hearing supplemental brief, *see* Def. Supp. Br. Exs. A–C, is GRANTED. The relevant materials reflect sensitive medical, financial, educational, and other personal information pertaining to non-parties, and the Court finds that the privacy interests of those non-parties outweigh any public interest in disclosure, whether derived from the First Amendment or the common-law right of access, and that the sealing application is narrowly tailored to serve those interests. *See* *Lugosch v. Pyramid Co. of Onondaga,* 435 F.3d 110, 124 (2d Cir. 2006).

Finally, it is ORDERED that, within fourteen days of this Order, the parties shall meet and confer and jointly submit a letter proposing a schedule to govern all remaining pretrial proceedings, including the submission of motions *in limine* and other pretrial materials.

This resolves Dkt. No. 44.

SO ORDERED.

All Citations

256 F.Supp.3d 355

Footnotes

1 The Court notes that Nasdaq's decision was subsequently set aside on review by the Securities Exchange Commission ("SEC"). *See In re Application of CleanTech Innovations, Inc.,* Exchange Act Release No. 69968, 2013 WL 3477086 (Jul. 11, 2013).

2 Following the Hearing and at the Court's direction, the Government submitted for the Court's reference a binder containing all documentary and electronic exhibits entered into evidence by the parties. The index to that binder is being filed concurrently with this Opinion and Order as Court Exhibit 1.

3 In roughly the same timeframe and further reflecting the shifting focuses of the Government's investigation and its evolving theories of its case, AUSA Massey became aware through conversations with FBI analysts that some of the electronic data recovered during the Searches—including data that the Government had already shared with the SEC to aid its parallel of investigation of Wey—included documents of "a purely personal nature," such as "spreadsheets reflecting family medical issues." Def. Ex. 4 (May 3, 2013 e-mail memorandum to file by Massey); Hearing Tr. 77:8–78:4. In a May 2013 memorandum to file, Massey rationalized the seizure of such documents as "within the scope the warrant because Wey's tax returns are relevant documents because we believe he committed tax fraud, and he claimed large medical deductions most years." Def. Ex. 4; Hearing Tr. 79:5–20. Once again, neither tax fraud nor any other scheme involving medical deductions was presented to Magistrate Judge Dolinger or communicated to the Search teams as a current subject of Government interest at the time of the Searches. *See, e.g.,* Hearing Tr. 78:17–79:16, 80:7–14.

4 As a threshold matter, a defendant "seeking to suppress the fruits of a search by reason of a violation of the Fourth Amendment" generally "must show that he had a 'legitimate expectation of privacy' in the place searched." *United States v. Hamilton,* 538 F.3d 162, 167 (2d Cir. 2008) (quoting *Rakas v. Illinois,* 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978)). "Where the premises searched is a business, defendants seeking suppression must establish both that they are associated with the business and that they have a legitimate expectation of privacy in the part of the business that was searched." *United States v. Kazarian*, 10–cr–895, 2012 WL 1810214, *18 (S.D.N.Y. May 18, 2012) *(citing O'Connor v. Ortega*, 480 U.S. 709, 718, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987)). Here, the parties do not appear to dispute that Wey has standing to challenge the Search of his residence or the Search of the offices of NYGG, a private firm of which Wey was founder and chief executive officer.

5 As the Government correctly observes, the Second Circuit's *Galpin* decision, cited above, post-dates the Searches at issue. *See* Government's Memorandum of Law in Opposition to Defendant Benjamin Wey's Motions to Suppress Evidence, Prevent a Privilege Review, Dismiss the Indictment, Take His Co–Defendant's Deposition Abroad, and Strike References to Aliases, Dkt. No. 53 ("Opp."), at 30. The Court does not view that fact as material to its analysis of the Warrants. It may be true that prior to *Galpin,* the Circuit had not necessarily articulated one "settled formula for determining whether a warrant lacks particularity." *Zemlyansky,* 945 F.Supp.2d at 453. Still, the requirements outlined in *Galpin* are hardly novel, and each had been clearly idenfitied on an individualized basis well prior to the advent of the comprehensive

Galpin framework—and, more importantly, well prior to the Searches. Indeed, the *Galpin* Court itself cited at least one earlier Circuit decision in support of each requirement it enumerated and in no way purported to break any ground in marshalling that law. 720 F.3d at 445–446. Still further, well before *Galpin,* courts in this District surveying the particularity case law consistently recognized at least two discrete "factors" that "tend to define a warrant's insufficient particularity." *See, e.g., United States v. Vilar*, 05–cr–621, 2007 WL 1075041, at *21–22 (S.D.N.Y. Apr. 4, 2007) (collecting cases). Those factors substantially track the two item-related requirements explicitly set forth in *Galpin*: (i) the failure to "tell[ ] the searching officers for what crime the search is being undertaken" and (ii) the inclusion of "general catch-all paragraph[s] or provision[s], often ... authorizing the seizure of 'any and all records' of a particular type." *Vilar,* 2007 WL 1075041, at *21–22 (internal quotation marks and citations omitted) (collecting cases); *see also Zemlyansky,* 945 F.Supp.2d at 453–54 (same). Accordingly, the Court is satisfied that the intervention of the *Galpin* decision is of no particular moment on this point one way or the other.

6 Nor, on a similar note, does the Warrants' single passing reference to seizing "property purchased with the proceeds of fraud," NYGG Warrant Ex. A. ¶ 10, substitute for the requisite identification of the crime under investigation. *See, e.g., United States v. Vilar,* 2007 WL 1075041, at *22 ("oblique reference" in warrant rider to " 'participants in fraud schemes' " could not cure warrant's failure to "indicate what specific acts of wrongdoing are being investigated"); *see also Galpin,* 720 F.3d at 445 n.5 (because the "purpose" of the requirement that the crime be identified is "to minimize the discretion of the executing officer, other Circuits have held that even warrants that identify catchall statutory provisions, like the mail fraud or conspiracy statutes, may fail to comply with this aspect of the particularization requirement") (collecting cases).

7 Other courts in this Circuit have concluded that similarly expansive categories of documents rendered warrants constitutionally deficient. *See, e.g., United States v. Bianco,* 998 F.2d 1112, 1115–1116 (2d Cir. 1993) (warrant for home authorizing seizure of "[n]otes, ledgers, envelopes, papers, and records containing initials, names, addresses, dollar amounts, codes, figures, and the like" was insufficiently particularized especially when such items were not "tied to particular crimes"), *abrogated on other grounds by Groh,* 540 U.S. at 557, 124 S.Ct. 1284; *Buck,* 813 F.2d at 591 (warrant consisting entirely of "general boilerplate terms, without either explicit or implicit limitation on the scope of the search" was insufficiently particularized); *Zemlyansky,* 945 F.Supp.2d at 457–59 (no particularity where warrant authorized seizure of, among other things, "checks, cash, and other financial instruments," "bank account information," "calendars and patient appointment records," and "records related to patient care"); *Hernandez,* 2010 WL 26544, *10 (warrant to search business offices likely lacked particularity because it "could have encompassed most all of the business records on the premises"); *Vilar,* 2007 WL 1075041, at *22–23 (warrant provision authorizing seizure of all "corporate records" concerning the occupant of the premises and its affiliates reflected "patent lack of particularity," notwithstanding inclusion of illustrative list of items); *United States v. Hickey,* 16 F.Supp.2d 223, 237–241 (E.D.N.Y. 1998) (warrant authorizing seizure of "all business records" of four companies, "including but not limited to" approximately fifty individually listed generic items, was deficient); *United States v. Gigante,* 979 F.Supp. 959, 966 (S.D.N.Y. 1997) (warrant provision permitting seizure of "financial, banking, safe deposit, investment, asset, tax, bookkeeping, and accounting records," along with "underlying, supporting, and related documentation," of "or referring or relating to" several named individuals lacked particularity).

8 USA Massy conceded at the Hearing that he had read portions of the Government's briefing on Wey's suppression motion and was aware that it was pressing an argument based on the all-records exception. Hearing Tr. 32:22–33:4.

9 "[W]hen multiple officers are involved in an illegal search, 'it is necessary to consider the objective reasonableness, not only of the officers who eventually executed a warrant, but also of the officers who originally obtained it or who provided information material to the probable-cause determination.' " *Zemlyansky,* 945 F.Supp.2d at 476 (internal brackets omitted) (quoting *Leon,* 468 U.S. at 923 n.24, 104 S.Ct. 3405).

10 Invoking this reasoning, Wey advances the threshold argument that the Warrants are so facially deficient that the good faith exception is, essentially, unavailable to the Government. Supp. Br. at 3–5. Because, as discussed further below, the Court concludes that the good faith exception has no application to this case under even the arguably more generous interpretation of the doctrine signaled by more recent Supreme Court and Second Circuit decisions, it need not, and does not, address that argument.

11 *Zemlyansky,* 945 F.Supp.2d at 468.

12 Because the Court reaches this conclusion with respect to the Warrants' lack of particularity, it does not separately consider—to the extent that it would implicate an independent analysis—whether an objectively reasonable officer could have relied on the Warrants notwithstanding their overbreadth.

13 All of this assumes that even a thorough and detailed briefing on the contemplated limits of the Magistrate Judge's authorization could potentially bring the otherwise constitutionally infirm search within the good faith exception—a proposition about which at least one court in this District has expressed considerable doubt. *See* *Zemlyansky,* 945 F.Supp.2d at 473–74 (recognizing both that a "briefing session generates substantial room for slippage between the magistrate's authorization and the searching officers' understanding of their authority" and that the "historic notice function served by a lawful warrant," as emphasized in *Groh,* would "fall by the wayside if officers could claim good faith each time" they had simply "been briefed about the affidavit" before the search); *see also* *Vilar,* 2007 WL 1075041, at *8, 22 n.13 (notwithstanding pre-search briefing, there was "no certainty that all members of the search team were aware of the limits, if any, to be read into the Warrant from the supporting documents").

14 At the Hearing (which, of course, the Court explicitly convened to address the good faith question), Komar changed his tune, testifying that he relied primarily on his "knowledge of the case" rather than on "search materials"—an assertion the Court found less than persuasive. Hearing Tr. 153:13.

15 That is to say nothing of the more than 100,000 electronic documents ultimately seized by the Government, examples of which—to the Court's understanding—have largely not been put before it.

THE YALE LAW JOURNAL FORUM
OCTOBER 25, 2017

Why Rely on the Fourth Amendment To Do the Work of the First?

Alex Abdo

ABSTRACT. Modern surveillance threatens not only individual privacy but also the freedom to dissent. Yet for a variety of reasons, American courts almost always evaluate the lawfulness of government surveillance solely through the lens of the Fourth Amendment rather than the First Amendment. This Essay explains why we should not expect the Fourth Amendment to adequately protect First Amendment interests, and it briefly sets out how the First Amendment might once again become a bulwark against overreaching government surveillance.

Government surveillance implicates the freedom of speech as well as the right to privacy, and yet our courts usually evaluate the lawfulness of government surveillance solely through the lens of the Fourth Amendment rather than the First. Is that approach defensible?

This term in *Carpenter v. United States*, for example, the Supreme Court will consider whether the warrantless and long-term collection of an individual's "cell site location information," revealing the movements and locations of the user, violates the Fourth Amendment.[1] But the case has clear implications for First Amendment freedoms, too—particularly the ability to express dissent. Dissent's fragile lifecycle—from formulation to ferment—requires privacy and often confidential association to flourish. Warrantless location tracking threatens these conditions, exposing to the government both the participants that initiate and the private places that incubate dissent. And yet the legal fight in

1. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (mem.) (June 5, 2017) (No. 16-402).

Carpenter and many other surveillance cases is taking place almost entirely on Fourth Amendment grounds.

This trend is problematic because the Fourth Amendment is not up to the task of safeguarding dissent from the threat of new technology. As explored below, the Fourth Amendment differs from the First substantially in both its coverage and the strength of its protections. First, Fourth Amendment doctrine addresses invasions of privacy, not speech, and has been held to ignore a whole class of surveillance—the collection of third-party records—with significant implications for expression. Second, unlike the First Amendment, the Fourth Amendment is often blind to the cumulative effect of invasions of privacy that are small in isolation but substantial in combination. Third, and relatedly, the Fourth Amendment tends to focus narrowly on individual harms, not collective or societal ones. Fourth, even when it does apply, the Fourth Amendment offers much weaker protection than does the First, which requires a heightened government interest and means narrowly tailored to that interest. Finally, Fourth Amendment doctrine has been developed largely in the context of criminal prosecutions, in which both the claimants and the relief available tend to generate judicial antipathy.

In other words, we should not expect the Fourth Amendment to pull double constitutional duty, and yet courts routinely act as though it can. The result is that First Amendment freedoms are often at the mercy of a Fourth Amendment doctrine not designed to protect them. The time may have come to fully disentangle the two legal regimes to more fully recognize, as one court has said, that "the First Amendment requires a different analysis, applying different legal standards," than the Fourth.[2]

This Essay sketches out that argument. Part I describes the state of surveillance in the United States and its effect on dissent. Part II argues that we should not expect the Fourth Amendment to protect dissent and other First Amendment freedoms against the threat of modern surveillance. And Part III briefly describes how a First Amendment surveillance doctrine might differ from the current Fourth Amendment framework.

2. Tabbaa v. Chertoff, 509 F.3d 89, 102 n.4 (2d Cir. 2007) ("[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.").

I. SURVEILLANCE AND DISSENT

A. The State of Modern Surveillance

Government surveillance has always threatened the freedom of speech and dissent. As the Supreme Court has said: "Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech."[3]

This risk is compounded by modern surveillance capabilities, which have reached a tipping point. Their recent evolution has been not incremental, but abrupt. The crucial advance of modern surveillance has been the development of inexpensive automation. Where before the government had to rely on human agents or informants to spy, today it spies through a proliferating network of unsleeping sensors. And where before agents had to manually review what they collected, today they use computers to make sense of their harvest.[4] The government's appetite for digitally collected data has grown in conjunction with its capabilities for collection and analysis. And, when law enforcement agencies cannot sate that appetite directly, they feast, instead, on data accumulated by private companies.[5]

The result of these advances is that, for the first time in human history, the government can now engage in nearly pervasive surveillance of the public. We have seen a glimpse of that reality already, through Edward Snowden's disclosures to the press of the breathtaking scope of surveillance by the National Security Agency[6] and recent reports on law enforcement's expanding use of new and invasive technologies like cell-site simulators,[7] automated license plate

3. United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 320 (1972).

4. *See infra* notes 6-8 and accompanying text.

5. *See* American Civil Liberties Union, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements* 28-29 (July 2013), http://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf [http://perma.cc/K9CD-K9NF].

6. *Edward Snowden: Leaks that Exposed US Spy Programme*, BBC (Jan. 17, 2014), http://www.bbc.com/news/world-us-canada-23123964 [http://perma.cc/F5VY-EJX6].

7. Cell-site simulators are devices that imitate cell towers to gather information on potentially thousands of nearby cellphones in order to locate a specific cellphone. *See* Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014), http://www.wsj.com/news/article_email/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533-lMyQjAxMTI0NTEwNDAxMTQwWj [http://perma.cc/8R5W-DMY8]; Nicky Woolf, *Stingray Documents Offer Rare Insight into Police and FBI Surveillance*, GUARDIAN (Aug. 26, 2016), http://www.theguardian.com/us-news/2016/aug/26/stingray-oakland-police-fbi-surveillance [http://perma.cc/SBA9-8CXR] ("[A]t least 66 state and federal agencies are now known to use the devices, including the IRS, as well as dozens of state and local police departments."); Kim Zetter, *California Police Used Stingrays in Planes to*

readers,[8] pervasive aerial surveillance systems,[9] and facial-recognition databases.[10]

The trend in technology is to reduce virtually everything we do to digital data. Our cellphones are livestreams of our locations; our internet-usage histories are unintended journals of our thoughts; our e-mails are often-permanent records of once-ephemeral conversations. Newer technologies digitize even more of our lives: smart watches, smart TVs, smart refrigerators, smart cars, and a host of other internet-connected devices have made *The Wizard of Oz*'s technicolor transition seem impossibly quaint.

Whether by warrant, subpoena, or some other demand, the government can access more data about us than ever before.

B. The Cost to Dissent

Many commentators have explained that this new surveillance state of affairs comes at considerable cost to the freedom to dissent.[11]

Spy on Phones, WIRED (Jan. 27, 2016), http://www.wired.com/2016/01/california-police-used-stingrays-in-planes-to-spy-on-phones [http://perma.cc/69ST-P74S].

8. Automated license plate readers are cameras affixed to police cars or to roadside infrastructure that automatically scan every license plate they see and note the exact time and location of the scan. *See* American Civil Liberties Union, *supra* note 5, at 2 (reporting that automatic license plate readers "have been proliferating around the country at worrying speed"); *id.* at 20 (showing license plate information retention periods of various jurisdictions); *id.* at 25 ("The Wall Street Journal reported in 2012 that, over the past five years, the Department of Homeland Security distributed over $50 million in grants to fund the acquisition of license plate readers.").

9. One such surveillance system is capable of tracking the movements (although not identifying features) of every car and person in a thirty-square-mile area. *See* Monte Reel, *Secret Cameras Record Baltimore's Every Move from Above*, BLOOMBERG BUSINESSWEEK (Aug. 23, 2016), http://www.bloomberg.com/features/2016-baltimore-secret-surveillance [http://perma.cc/JJW3-M7MS]; *see also* Andrea Peterson, *FBI Spy Planes Used Thermal Imaging Tech in Flights over Baltimore after Freddie Gray Unrest*, WASH. POST (Oct. 30, 2015), http://www.washingtonpost.com/news/the-switch/wp/2015/10/30/fbi-spy-planes-used-thermal-imaging-tech-in-flights-over-baltimore-after-freddie-gray-unrest [http://perma.cc/N2YZ-U73S] (discussing the use of thermal imaging cameras from surveillance aircraft to monitor protests).

10. The FBI and state and local agencies now routinely use facial-recognition technology as a "virtual, perpetual line-up" of the estimated 117 million Americans whose faces are in facial-recognition databases. Clare Garvie et al., *The Perpetual Line-Up: Unregulated Police Face Recognition in America*, GEO L. CTR. ON PRIVACY & TECH. (Oct. 18, 2016), http://www.perpetuallineup.org [http://perma.cc/T3S7-W2NA].

11. BERNARD E. HARCOURT, EXPOSED (2015) (asserting that today's digital landscape and data collection apparatus is building an "expository state" that is breaking down boundaries between individuals and the state and encumbering our freedom); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1950 (2013).

Dissent requires breathing space: to formulate dissenting ideas, to test and debate those ideas with close associates, to expand the association into a movement, and finally to air grievances publicly, to convince fellow citizens, and to effect political change.

Expansive modern surveillance threatens this fragile process at each stage of development. The threats are most visible at the final stage, when dissidents take their message to the public. Modern surveillance empowers the government to identify and respond to that public outreach earlier and more quickly than ever before.

As the government's surveillance capabilities grow, the threat to dissent reaches earlier into its lifecycle. John Milton described the prior restraint of publication as the abortion of one's "intellectual[] off-spring."[12] Pervasive surveillance can have the same abortive effect. When people are watched or fear that they might be watched, they change their behavior. This is why we close our curtains, password-protect our emails, and clear our internet browsing history. But because we cannot guard against all forms of modern surveillance (most digital "curtains" require technical savvy to use), some amount of self-censorship is inevitable.[13]

The most insidious threat that expansive surveillance poses reaches even earlier into the lifecycle of dissent. For a thought to be birthed in a Miltonian sense, it must first be conceived, and here pervasive surveillance has a contraceptive effect. Those watched change not only their behavior; they change their thinking, too, so that they do not even conceive the thoughts that would become their "intellectual offspring." This is what Neil Richards calls the "normalizing gaze of surveillance,"[14] and it is perhaps analogous to the "observer

12. JOHN MILTON, *Areopagitica: A Speech of Mr. John Milton for the Liberty of Unlicenc'd Printing, to the Parliament of England*, *reprinted in* AREOPAGITICA AND OTHER POLITICAL WRITINGS OF JOHN MILTON 3, 13 (Liberty Fund ed., 1999) (1644) ("Till then Books were ever as freely admitted into the world as any other birth; the issue of the brain was no more stifl[e]d than the issue of the womb: no envious *Juno* sat cross-leg[ge]d over the nativity of any man's intellectual[] off-spring . . . .").

13. *See, e.g.*, *Americans' Privacy Strategy Post-Snowden*, PEW RES. CTR. 4 (Mar. 16, 2015), http://www.pewinternet.org/files/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf [http://perma.cc/D54F-G343] (finding that that 22% percent of American adults—about 54 million people—have changed their online behavior "a great deal" or "somewhat" after learning of the scope of U.S. government surveillance, with those most informed changing their behavior most); *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN AM. CTR. 6 (Nov. 12, 2013), http://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf [http://perma.cc/WXP6-HNPL] (finding that 28% of American writers had curtailed their use of social media and, more troublingly, that 24% had "deliberately avoided certain topics in phone or email conversations" and that 16% had avoided "writing or speaking about a particular topic").

14. Richards, *supra* note 11.

effect" in physics. Unobserved, a citizen's thoughts—like particles—follow their own path. But the more closely watched they become, the more their possible paths are determined by the very act of observation.[15]

II. THE FOURTH AMENDMENT'S INADEQUATE PROTECTION OF FIRST AMENDMENT INTERESTS

Though expansive surveillance threatens free speech and dissent, courts typically evaluate the constitutionality of surveillance solely with reference to Fourth Amendment doctrine.

This is not categorically the case. In the late 1950s and early 1960s, the Supreme Court issued a string of seminal decisions rejecting subpoenas or other compulsory disclosures that would have exposed the membership of organizations central to the civil rights movement. The decisions invoked the First Amendment, finding the chilling effect of disclosure obvious and unconstitutional.[16] Since that time, many lower courts have questioned and sometimes invalidated subpoenas on similar grounds where they would expose and chill protected associations.[17]

---

15. *See, e.g.*, Jonathon W. Penney, *Chilling Effects: Online Surveillance and Wikipedia Use*, 31 BERKELEY TECH. L.J. 117, 161 (2016) (finding, in a sophisticated study of self-censorship following the Snowden disclosures, a "large, statistically significant, and immediate drop in total views" of certain politically controversial Wikipedia articles, as well as a "broad and statistically significant shift in the overall trend in the data" that "suggests any chilling effects observed may be substantial and long-term"); *Americans' Privacy Strategy Post-Snowden*, *supra* note 13, at 4 (finding that that about 17% of American adults who are aware of government surveillance programs had changed their use of internet search engines); *Chilling Effects*, *supra* note 13, at 6 (finding that 16% of the American authors polled had "refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious" and that another 12% had "seriously considered" doing the same).

16. *See* Shelton v. Tucker, 364 U.S. 479, 485-86 (1960) ("[T]o compel a teacher to disclose his every associational tie is to impair that teacher's right of free association, a right closely allied to freedom of speech and a right which, like free speech, lies at the foundation of a free society."); NAACP v. Alabama, 357 U.S. 449, 462-63 (1958) ("[W]e think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association and dissuade others from joining it because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."); *see also* Bates v. City of Little Rock, 361 U.S. 516 (1960) (holding the same, in Arkansas).

17. *See, e.g.*, FEC v. Larouche Campaign, 817 F.2d 233, 234-45 (2d Cir. 1987) (quashing a subpoena for campaign records that would "compromise the privacy of individual political associations"); Local 1814 v. Waterfront Comm'n of N.Y. Harbor, 667 F.2d 267, 270-71 (2d Cir. 1981) (approving of a subpoena for union members' names, after substantial narrowing to

Nevertheless, judicial application of the First Amendment to state surveillance demands has generally been narrow. The courts have analyzed more traditional surveillance challenges—those involving physical or electronic searches and seizures, rather than compelled disclosure—primarily in Fourth Amendment terms.

In *Zurcher v. Stanford Daily*, for example, the Supreme Court recognized the free speech implications of a warrant authorizing the seizure of photographs directly from a newspaper's offices, but it held that those concerns were addressed by the application of the Fourth Amendment's requirements with "scrupulous exactitude."[18] Congress responded by enacting the Privacy Protection Act of 1980, which insulates journalists from certain searches and seizures, but the statute's protections are narrow, and they are, of course, statutory rather than constitutional.[19]

A few years later, the Supreme Court distilled its jurisprudence concerning the seizure of books and films, holding that while the First Amendment requires scrupulous application of certain procedural protections, the seizures "should be evaluated under the same standard of probable cause used to review warrant applications generally."[20] About the same time, the Sixth Circuit broadly stated that "physical surveillance consistent with Fourth Amendment protections in connection with a good faith law enforcement investigation does not violate First Amendment rights, even though it may be directed at communicative or associative activities."[21]

---

accommodate First Amendment concerns); *see also In re* Grand Jury Subpoena to First Nat'l Bank, 701 F.2d 115 (10th Cir. 1983) (remanding for consideration of a First Amendment challenge to a subpoena for bank records of tax-protest groups).

18. 436 U.S. 547, 564 (1978) (quoting Stanford v. Texas, 379 U. S. 476, 485 (1965)).

19. *See* 42 U.S.C. §§ 2000aa, 2000aa-5 to 2000aa-7. The Act is limited in important respects. For instance, it does not apply if there is cause to believe that the journalist in question has committed an offense involving the "receipt, possession, or communication of information relating to the national defense, classified information, or restricted data." *Id.* § 2000aa(a)(1), (b)(1).

20. New York v. P.J. Video, Inc., 475 U.S. 868, 875 (1986); *see also id.* at 873 (collecting cases).

21. Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983) (citations omitted); *see also* United States v. Mohamud, 843 F.3d 420, 444 n.28 (9th Cir. 2016) ("Finally, the district court correctly rejected Mohamud's First Amendment challenge, as motions to suppress based on First Amendment violations are analyzed under the Fourth Amendment."); Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint at 37, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *rev'd*, 785 F.3d 787 (2d Cir. 2015) (No. 13 Civ. 3994 (WHP)), 2013 WL 5221584 ("The law is clear that governmental investigations conducted in observance of Fourth Amendment requirements, without purpose to deter or penalize protected expression or association, do not violate the First Amendment.").

Even in these contexts, the Supreme Court has recognized the overlapping concerns of the First and Fourth Amendments.[22] But when it comes to actually analyzing the constitutionality of more traditional surveillance, courts tend to apply a traditional Fourth Amendment framework, asking whether the surveillance constitutes a search or seizure within the meaning of the Fourth Amendment and, if so, whether that search or seizure is reasonable.[23]

The result is that the First Amendment freedoms of speech and of the press are often at the mercy of Fourth Amendment doctrine. It is critical to ask, then, whether current Fourth Amendment doctrine adequately protects those First Amendment rights. It does not.

First, the Fourth Amendment protects against intrusions into privacy, not free speech. This is obvious, of course, given the substance of the Fourth Amendment, but it contradicts a seemingly necessary predicate of judicial decisions analyzing First Amendment harms in exclusively Fourth Amendment terms. If the coverage of the two differs, why should we expect defense of one to replace defense of the other? Why, in other words, should an amendment historically focused on the sanctity of the home and other personal effects displace application of an amendment directed at expression?

One glaring example of this mismatch in coverage is the third-party doctrine, through which courts have interpreted the Fourth Amendment to be blind to the seizure of data held by third parties. There is no obvious reason why the First Amendment should be similarly indifferent, and historically, it has not been. The seminal Supreme Court cases quashing subpoenas directed at identifying civil rights activists were, after all, First Amendment cases. But there are signs that the third-party doctrine is now distorting First Amendment doctrine, too. A district court considering a challenge to the NSA's bulk collection of call records held both that the Fourth Amendment does not apply because of the third-party doctrine *and* that the government's argument that the First Amendment should not apply either was "well-supported."[24] The court ultimately dodged the question, but it appeared persuaded that the First

22. *See, e.g.*, United States v. U.S. Dist. Court *(Keith)*. 407 U.S. 297, 313 (1972) ("National security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime."); *id.* at 314 ("The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.").

23. *But see* Tabbaa v. Chertoff, 509 F.3d 89, 102 n.4 (2d Cir. 2007) ("[D]istinguishing between incidental and substantial burdens under the First Amendment requires a different analysis, applying different legal standards, than distinguishing what is and is not routine in the Fourth Amendment border context.").

24. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

Amendment does not have force independent of the Fourth, thus suggesting that third-party possession eliminates First *and* Fourth Amendment protections.[25]

The Supreme Court may revisit the third-party doctrine this term in *Carpenter*, but the general point remains that the First and Fourth Amendments differ in their coverage.

Second, courts have sometimes taken a divide-and-conquer approach to privacy that is foreign to the First Amendment. Fourth Amendment doctrine tends to focus narrowly on individual harms, whereas First Amendment doctrine accounts for collective or societal ones. The Supreme Court has said many times that Fourth Amendment rights are "personal rights which, like some other constitutional rights, may not be vicariously asserted."[26] On this theory, courts have resisted aggregating "reasonable" invasions of the privacy of many individuals to find the invasions "unreasonable" in their totality.[27] For example, the Foreign Intelligence Surveillance Court has held that an individual challenge to the NSA's bulk collection of call records is not strengthened by the fact that the NSA collected everyone else's call records as well. In that court's words, "where one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[28]

In contrast, courts applying the First Amendment give significant weight to the collective chilling effect on third parties not before the court. In *Local 1814 v. Waterfront Commission of N.Y. Harbor*, for instance, the Second Circuit slashed the number of longshoremen's names that a state regulatory agency could subpoena in an investigation into union coercion out of concern that a broader

25. *Id.*

26. Rakas v. Illinois, 439 U.S. 128, 133-34 (1978) (quoting Brown v. United States, 411 U.S. 223, 230 (1973)).

27. *See, e.g.*, United States v. Dionisio, 410 U.S. 1, 13 (1973) ("It does not follow that each witness may resist a subpoena on the ground that too many witnesses have been called."); *In re* Grand Jury Proceedings: Subpoenas Duces Tecum, 827 F.2d 301, 305 (8th Cir. 1987) ("Western Union's overbreadth argument is based on its fear that the subpoena may make available to the grand jury records involving hundreds of innocent people. But the fourth amendment does not necessarily prohibit the grand jury from engaging in a 'dragnet' operation."); Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint at 37-40, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 1:13-cv-03994).

28. *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [redacted], BR 13-109, at 9 (FISA Ct. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf [http://perma.cc/ZTF2-DCM8].

subpoena for more names "may have the practical effect of discouraging" union membership.[29]

Third, and relatedly, courts have taken a similar divide-and-conquer approach to privacy even with respect to multiple privacy invasions of a single individual. In several cases around the country, courts have held that because individuals do not have an expectation of privacy in the address of a single website they have visited online, they do not have any expectation of privacy in a list of *all* websites they have visited.[30] Proponents of that logic say that "zero plus zero equals zero."[31]

The First Amendment, by contrast, is more attentive to the cumulative effect of even individually insubstantial invasions. In *Clark v. Library of Congress*, the D.C. Circuit held that a government employee could pursue a First Amendment claim based on the understandable chill of his expressive activities caused by a "full field investigation" into his association with the Young Socialist Alliance.[32] The investigation consisted of interviewing his coworkers, neighbors, and teachers and of obtaining his school, credit, and other records.[33] A more limited investigation, involving perhaps only a single interview of a coworker, would likely have produced a different outcome. The constitutional harm, then, flowed from the investigation's cumulative effect.

Fourth, the two Amendments also differ in the strength of their legal protections. Significant burdens on free speech must be narrowly tailored to serve heightened state interests.[34] Searches and seizures under the Fourth Amend-

---

29. 667 F.2d 267, 270 (2d Cir. 1981); *see also* Broadrick v. Oklahoma, 413 U.S. 601 (1973) ("Litigants, therefore, are permitted to challenge a statute not because their own rights of free expression are violated, but because of a judicial prediction or assumption that the statute's very existence may cause others not before the court to refrain from constitutionally protected speech or expression.").

30. United States v. Ulbricht, 858 F.3d 71, 97-98 (2d Cir. 2017) (holding that one does not have an expectation of privacy in IP address routing information and collecting cases stating the same); United States v. Forrester, 512 F.3d 500 (9th Cir. 2008) (stating that there is no expectation of privacy in "e-mail to/from addresses and IP addresses"); United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *13-14 (D. Ariz. May 8, 2013) (reiterating that there is no expectation of privacy in 1.8 million IP addresses of websites visited).

31. There are many reasons to criticize the approach, and the Supreme Court has already signaled it may reverse the trend itself. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring); *id.* at 429-31 (Alito, J., concurring).

32. 750 F.2d 89, 92-95 (D.C. Cir. 1984).

33. *Id.* at 91.

34. Az. Free Enter. Club's Freedom Club PAC v. Bennett, 564 U.S. 721, 734 (2011); *Clark*, 750 F.2d 89.

ment, by contrast, need only be reasonable.[35] The Supreme Court has said that, to be reasonable, searches and seizures must generally be supported by a warrant based on probable cause.[36] But the interest that a search or seizure serves need not be heightened, and the search or seizure need not serve that interest in as narrow a means as possible. The reasonableness and particularity requirements of the Fourth Amendment require some tailoring of the government's searches and seizures, but the Supreme Court has held that they do not require the government to choose the least-intrusive means available to achieve its interests.[37]

Finally, Fourth Amendment doctrine has been developed largely in the context of criminal prosecutions, in which both the claimants (criminal defendants) and the relief available for violations (suppression of evidence) tend to generate judicial antipathy. Judicial anguish at the prospect of awarding criminal defendants the perceived windfall of suppression is often palpable. In a recent and oft-cited decision, the Supreme Court explained that suppression "exacts a heavy toll on both the judicial system and society at large," because "its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment."[38]

In contrast, courts often pride themselves on preserving and expanding the promises of the First Amendment. In 1964, the Supreme Court said that the First Amendment reflects "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[39] That principle has been a rallying cry of free speech ever since, invoked in nearly every major free speech opinion, and defended against efforts to regulate even the most hateful speech.[40] Though it may be impossible to prove, the differing judicial attitudes toward the First and Fourth Amendments may have promoted the growth of the one while stunting the growth of the other.

---

35. Brigham City, Utah v. Stuart, 547 U.S. 398, 403 (2006) ("the ultimate touchstone of the Fourth Amendment is 'reasonableness'").

36. Katz v. United States, 389 U.S. 347, 357 (1967) ("searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment").

37. *See* Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 629 n.9 (1989) (collecting cases holding that searches and seizures need only be reasonable, not the least-intrusive means available).

38. Davis v. United States, 564 U.S. 229, 237 (2011).

39. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

40. *See, e.g.*, Snyder v. Phelps, 562 U.S. 443, 452 (2011).

III. A FIRST AMENDMENT FRAMEWORK FOR SURVEILLANCE

If the Fourth Amendment is, for these reasons, an inadequate guarantor of First Amendment rights against overreaching surveillance, what is the alternative? The obvious candidate is the First Amendment itself. Courts could simply apply the First Amendment independently of the Fourth to surveillance that substantially burdens free speech and dissent.

There would be at least three obvious differences in that regime.

First, courts would undertake a First Amendment analysis in circumstances where the Fourth Amendment might not apply at all. For instance, courts that currently find no constitutional restraint on the government's collection of the list of websites someone has visited might recognize that such surveillance burdens free inquiry and dissent. This would not require much legal innovation. The Supreme Court has already recognized the First Amendment harms of the compelled disclosure of organizational membership lists.[41] All that remains is to extend that logic to other forms of surveillance.

Second, where the First Amendment applies, it would require the government to demonstrate a heightened interest to justify its surveillance. The Fourth Amendment generally imposes no such requirement, at least in practice: courts generally do not require the government to defend its interest in executing a warrant, except by establishing probable cause to believe the search or seizure would turn up evidence of a crime. The First Amendment framework would be more fine-grained and might, for example, forbid particularly invasive surveillance predicated on minor offenses or on token showings of cause. For example, whereas the Fourth Amendment might permit officers to track the cellphones of protesters to gather evidence of jaywalking, the First Amendment might prohibit that surveillance as too invasive to be used to investigate an offense so minor.

Finally, where the First Amendment applies, it would require narrow tailoring of the surveillance to the government's interests. Under current Fourth Amendment doctrine, the government need not select the least-invasive surveillance that would accomplish its goals; the First Amendment would require just that. To take one example, courts often permit government investigators to collect extraordinary volumes of a suspect's digital data, on the view that the investigators are best positioned to review the data to determine what is relevant to the investigation and what is not.[42] Where that overbroad collection

---

41. *See supra* notes 16-17 and accompanying text.

42. *See, e.g.*, United States v. Mann, 592 F.3d 779 (7th Cir. 2010) (approving investigator's search of several hard drives for incriminating images and rejecting Ninth Circuit's proposed guidelines addressing the over-collection of digital data).

would burden free speech and dissent, the First Amendment might require narrow tailoring of the collection.

Consider, again, the *Carpenter* case. The government argues that individuals have no expectation of privacy in their "cell site location information," because they voluntarily share that information with their cell phone providers. The result, according to the argument, is that the Fourth Amendment simply does not apply to the government's monitoring of the movements of its citizens using cellular location data. That principle would apply whether the government collected two days' or two years' worth of location data; whether the collection related to an investigation into recreational marijuana use or murder; and whether the government had used the least invasive or most invasive means of pursuing its investigation.

A First Amendment analysis would proceed differently. It would first ask whether the unchecked tracking of the suspect, particularly for long periods of time, burdened the freedoms of speech and association. The analysis would account not only for the chilling effect on the actual surveillance target, but also for the systemic chilling effect imposed by the availability and use of that power. If a court determined that the proposed location tracking would substantially burden First Amendment freedoms, it would ask whether, in the case before it, the tracking nonetheless served heightened government interests and was narrowly tailored to those interests. Even if held to be reasonable under the Fourth Amendment, pervasive and judicially unsupervised tracking of individuals suspected of minor crimes might not pass First Amendment muster. Judicially overseen tracking of individuals suspected of serious felonies for a short period might. In the former case, the government's interests are more minor and its means less measured. In the latter, its interests are stronger and its tactics tailored.

One objection to this approach might be to its administrability. The Fourth Amendment generally provides a predictable roadmap to police officers. The First Amendment framework set out here may appear more freeform. In practice, however, I suspect courts would apply it, much like Fourth Amendment analysis, in a categorical fashion. That is, courts would consider the free speech implications of categories of surveillance, much as courts now consider the privacy implications of categories of government investigation.

The requirement of narrow tailoring under the First Amendment framework might not, however, be as easily generalizable. The Fourth Amendment's focus on reasonableness gives law enforcement great leeway in using surveillance tools that are generally considered constitutional. A requirement that law enforcement narrowly tailor its use of certain surveillance tools might introduce some uncertainty into the constitutionality of using those same tools, as it would require a more searching inquiry. Again, I suspect courts would fashion

rules to provide for predictability. For instance, the federal wiretapping law requires police officers to attest in their surveillance applications that other investigative procedures have failed or would fail.[43] A similar test of narrow tailoring could be imposed under the First Amendment framework for especially intrusive practices.

* * *

Modern surveillance threatens First Amendment freedoms in obvious ways. The time may have come to dispense with the legal fiction that the Fourth Amendment adequately safeguards those freedoms.

Alex Abdo is a senior staff attorney at the Knight First Amendment Institute at Columbia University. Prior to joining the Institute, he was a senior staff attorney at the American Civil Liberties Union's Speech, Privacy, and Technology Project. *He is grateful for thoughtful feedback on drafts of this essay from Jameel Jaffer, Lincoln Caplan, Patrick Toomey, Brett Max Kaufman, and the staff of the* Yale Law Journal Forum*, including Lauren Hobby, Meenakshi Krishnan, Arjun Ramamurti, Erin van Wesenbeeck, and Kyle Victor.*

Preferred Citation: Alex Abdo, *Why Rely on the Fourth Amendment To Do the Work of the First?*, 127 YALE L.J. F. 444 (2017), http://www.yalelawjournal.org/forum/why-rely-on-the-fourth-amendment-to-do-the-work-of-the-first.

43. 18 U.S.C. § 2518(1)(c) (2012).

NOTE

Game of Phones, Data Isn't Coming: Modern Mobile Operating System Encryption and Its Chilling Effect on Law Enforcement

*Kristen M. Jacobsen**

ABSTRACT

The encrypted smartphone presents a novel legal issue that is hard to crack. Smartphone data is essential to investigating and prosecuting a range of crimes, such as murder, human trafficking, child pornography, and terrorism. However, Apple and Google's recently reengineered mobile operating systems threaten to lock out law enforcement completely. These operating systems use full-disk encryption technology, which converts everything on a hard drive into an unreadable format until the passcode is entered. Additionally, other security features on the smartphone could result in the data being completely destroyed if the passcode is incorrectly entered a certain number of times. Locked smartphones are thus quickly becoming expensive paperweights filing the evidence rooms of state and federal law enforcement.

This Note provides relevant background information on Apple and Google's use of full-disk encryption technology on their respective mobile operating systems. Based on the necessity of smartphone data in the twenty-first century, this Note explains that the inaccessibility of such crucial data will likely frustrate investigations and prosecutions because law enforcement cannot access it elsewhere. This Note concludes that to prevent "Going Dark,"

* J.D., expected May 2017, The George Washington University Law School; B.A., English, 2014, University of Denver. I would like to thank my parents, Jim Jacobsen and Denise Martin, for their unending support and the staff of *The George Washington Law Review* for their thoughtful comments throughout this process.

Congress must immediately enact an amendment to the Communications Assistance for Law Enforcement Act that subjects the manufacturer and mobile operating system provider to a civil penalty for each instance that law enforcement cannot decrypt a smartphone it has the legal authority to search.

TABLE OF CONTENTS

INTRODUCTION

On December 2, 2015, Syed Farook and Tashfeen Malik murdered fourteen people and wounded twenty-one others in San Bernardino, California, during a mass shooting and attempted bombing at a holiday party.[1] This was the first Al Qaeda- or Islamic State of Iraq and Syria ("ISIS")-inspired attack on U.S. soil where a skilled shooter team used both guns and explosives.[2] Investigators found Farook's locked iPhone 5c[3] and obtained legal authority to search its data.[4] However, the iPhone's hard drive was full-disk encrypted.[5] Law enforcement investigators did not have the technological capability to safely access the iPhone's data without the passcode,[6] and both

1 Michael S. Schmidt & Richard Pérez-Peña, *F.B.I. Treating San Bernardino Attack as Terrorism Case*, N.Y. TIMES (Dec. 4, 2015), http://www.nytimes.com/2015/12/05/us/tashfeen-malik-islamic-state.html.

2 Tim Lister et al., *ISIS Goes Global: 143 Attacks in 29 Countries Have Killed 2,043*, CNN (Jan. 16, 2017, 3:02 PM), http://www.cnn.com/2015/12/17/world/mapping-isis-attacks-around-the-world/.

3 Katie Benner & Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, N.Y. TIMES (Mar. 28, 2016), http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html. The iPhone was running Apple's iOS 9 operating system. *Id.*

4 Eric Lichtblau & Katie Benner, *Apple Fights Order to Unlock San Bernardino Gunman's iPhone*, N.Y. TIMES (Feb. 17, 2016), http://www.nytimes.com/2016/02/18/technology/apple-timothy-cook-fbi-san-bernardino.html. The FBI believed that the iPhone contained information regarding communications with ISIS extremists overseas. *See* Cecilia Kang & Eric Lichtblau, *F.B.I. Error Locked San Bernardino Attacker's iPhone*, N.Y. TIMES (Mar. 1, 2016), http://www.nytimes.com/2016/03/02/technology/apple-and-fbi-face-off-before-house-judiciary-committee.html.

5 Full-disk encryption technology prevents anyone from being able to unlock a device without the end user's unique, personal passcode. U.S. DEP'T OF COMMERCE, GUIDE TO STORAGE ENCRYPTION TECHNOLOGIES FOR END USER DEVICES: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY § 3.1.1 (2007). Since September 2014, both Apple and Google's respective mobile operating systems include full-disk encryption technology by default. *See, e.g.*, Craig Timberg, *Newest Androids Will Join iPhones in Offering Default Encryption, Blocking Police*, WASH. POST (Sept. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/09/18/newest-androids-will-join-iphones-in-offering-default-encryption-blocking-police/.

6 The iPhone's contents would be permanently deleted after ten failed attempts at input-

gunmen had died in a shootout with police following the attack.[7] The U.S. Department of Justice ("DOJ") thus turned to Apple. Apple publicly refused to help the government unlock the iPhone,[8] which incited a legal standoff between the DOJ and "the world's most valuable public company."[9] This led to "heated rhetoric from both sides in dueling court filings" and "spurred debates—[with the issue] finding its way onto late night talk shows, and dividing the public."[10] Ultimately, the government ended its legal effort to compel Apple's assistance when an anonymous hacker[11] was able to unlock the iPhone.[12] But immediately following the government's success, Apple released a statement saying that the company "will continue to increase the security of [its] products"[13] and will pursue legal measures to force the government to disclose the exploited security vulnerability so that it may reverse-engineer the problem.[14] Indeed, since the case was filed, Apple has begun developing new security measures that are designed

---

ting the passcode. Eric Lichtblau, *Judge Tells Apple to Help Unlock iPhone Used by San Bernardino Gunman*, N.Y. TIMES (Feb. 16, 2016), http://www.nytimes.com/2016/02/17/us/judge-tells-apple-to-help-unlock-san-bernardino-gunmans-iphone.html.

7 Schmidt & Pérez-Peña, *supra* note 1.

8 Tim Cook, CEO of Apple, wrote a letter to the company's customers:

> The United States government has demanded that Apple take an unprecedented step which threatens the security of our customers. We oppose this order, which has implications far beyond the legal case at hand. . . . [T]he U.S. government has asked us for something we simply do not have, and something we consider too dangerous to create. . . . We feel we must speak up in the face of what we see as an overreach by the U.S government.

Tim Cook, *A Message to Our Customers*, APPLE (Feb. 16, 2016), http://www.apple.com/customer-letter/ [https://perma.cc/38X4-WNDG]; *see also* Katie Benner & Nicole Perlroth, *How Tim Cook, in iPhone Battle, Became a Bulwark for Digital Privacy*, N.Y. TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/technology/how-tim-cook-became-a-bulwark-for-digital-privacy.html.

9 Benner & Lichtblau, *supra* note 3.

10 *Id.*

11 At the time of this Note's publication, the identity of the hacker is still unknown. *See id.*

12 *See* Government's Status Report, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Mar. 28, 2016); Benner & Lichtblau, *supra* note 3.

13 Alina Selyukh, *The FBI Has Successfully Unlocked The iPhone Without Apple's Help*, NPR (Mar. 28, 2016, 6:20 PM), http://www.npr.org/sections/thetwo-way/2016/03/28/472192080/the-fbi-has-successfully-unlocked-the-iphone-without-apples-help (quoting Apple's statement).

14 *See id.*; Chris Strohm et al., *Thank You for Hacking iPhone, Now Tell Apple How You Did It*, BLOOMBERG TECH. (Mar. 22, 2016, 9:04 PM), http://www.bloomberg.com/news/articles/2016-03-23/thank-you-for-hacking-iphone-now-tell-apple-how-you-did-it; *see also* Complaint at 1–4, Associated Press v. FBI, No. 16-cv-1850 (D.D.C. Sept. 16, 2016) (multiple news organizations sue the FBI under the Freedom of Information Act for disclosure of the hacker's identity and the "so-called iPhone access tool").

to prevent the government from unlocking an iPhone using similar methods.[15]

The effects of full-disk encryption extend beyond the San Bernardino iPhone. Crimes across 3000 local jurisdictions are often impossible to crack when law enforcement cannot access crucial smartphone data.[16] For example, in April 2015, eight-months pregnant Brittney Mills was shot to death on her doorstep by a man investigators believed she knew—and whose identity they suspect is currently locked in her iPhone 5.[17] In June of the same year, Ray C. Owens, a father of six, was found shot to death and robbed with two locked phones next to his body: an iPhone 6 and a Samsung Galaxy 6S Edge running Android.[18] And in July, Sharon Vugusta found her brother, U.S. Marine George Mitego, with a fatal gunshot wound to his head.[19] The coroner ruled Mr. Mitego's death a suicide, but his family believes that evidence of a murder may be trapped in his locked iPhone.[20] Currently, it appears that the Federal Bureau of Investigation ("FBI"), the government agency in possession of the decryption technology provided by the anonymous hacker, will not help unlock smartphones in the majority of local cases frustrated by full-disk encryption.[21] Any informa-

---

15 Matt Apuzzo & Katie Benner, *Apple Is Said to Be Trying to Make It Harder to Hack iPhones*, N.Y. TIMES (Feb. 24, 2016), http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html?_r=0; *see also* Katie Benner et al., *Apple's New Challenge: Learning How the U.S. Cracked Its iPhone*, N.Y. TIMES (Mar. 29, 2016), http://www.nytimes.com/2016/03/30/technology/apples-new-challenge-learning-how-the-us-cracked-its-iphone.html.

16 *See* Michael Learmonth, *FBI Keeps iPhone Hack Secret As Hundreds Of Locked Apple Devices Sit In Local Evidence Rooms*, INT'L BUS. TIMES (Mar. 30, 2016, 1:01 PM), http://www.ibtimes.com/fbi-keeps-iphone-hack-secret-hundreds-locked-apple-devices-sit-local-evidence-rooms-2345548. For a chart detailing the types of data that can only be accessed through the physical smartphone, see *infra* Appendix.

17 *See* Renita D. Young, *Brittney Mills' Locked iPhone Hampers Search for Her Killer*, TIMES PICAYUNE (Aug. 3, 2015, 12:30 PM), http://www.nola.com/crime/baton-rouge/index.ssf/2015/07/brittney_mills_locked_iphone.html; Letter from Hillar C. Moore, III, Dist. Attorney, 19th Judicial Dist. E. Baton Rouge Par., to U.S. Senate Comm. on the Judiciary (July 2015).

18 *See* Cyrus R. Vance Jr. et al., Opinion, *When Phone Encryption Blocks Justice*, N.Y. TIMES (Aug. 11, 2015), http://www.nytimes.com/2015/08/12/opinion/apple-google-when-phone-encryption-blocks-justice.html.

19 *See* Andy Pierrotti, *Going Dark: How iPhone Encryption Hurts Law Enforcement*, KVUE (Sept. 25, 2015, 7:15 AM), http://www.kvue.com/story/news/investigations/defenders/2015/09/24/going-dark-how-iphone-encryption-hurts-law-enforcement/72743852/.

20 *See id.*

21 *See* Learmonth, *supra* note 16. *But see* Doreen McCallister, *FBI To Help Arkansas Prosecutor Unlock iPhone Linked To Murder Case*, NPR (Mar. 31, 2016, 5:40 AM), http://www.npr.org/sections/thetwo-way/2016/03/31/472497468/fbi-to-help-arkansas-prosecutor-unlock-iphone-linked-to-murder-case.

tion shared increases the likelihood that Apple will isolate and close any vulnerability on future mobile operating systems.[22]

Unfortunately for law enforcement, defendants are dialed in to the possibilities this new encryption technology presents. The ISIS terrorist group—which claimed responsibility for the November 2015 attacks in Paris and the March 2016 attack in Brussels—instructs its followers on how to use encryption technology to evade law enforcement.[23] But the problem extends beyond international terrorist organizations. A Manhattan felon on a recorded jailhouse call said: "Apple and Google came out with these softwares that can no longer be encrypted [sic: *de*crypted] by the police. . . . If our phones is [sic] running on the iO[S]8 software, they can't open my phone. That might be another gift from God."[24] John J. Escalante, former Chief of Detectives for Chicago's police department, predicts that "Apple will become the phone of choice for the pedophile."[25]

Despite calls for federal legislation,[26] the Obama administration ultimately declined to seek a legislative solution.[27] The Trump administration has not yet stated whether it will champion legislation that bans or limits encryption on smartphones; however, Trump's cam-

---

22 *See* Learmonth, *supra* note 16.

23 *See, e.g.*, Rukmini Callimachi, *How ISIS Built the Machinery of Terror Under Europe's Gaze*, N.Y. TIMES (Mar. 29, 2016), http://www.nytimes.com/2016/03/29/world/europe/isis-attacks-paris-brussels.html; Pamela Engel, *A Pro-ISIS Account Is Giving Its Belgian Followers Specific Instructions on How to Evade Authorities*, BUS. INSIDER (Mar. 22, 2016, 4:29 PM), http://www.businessinsider.com/isis-belgian-supporters-encryption-2016-3.

24 *Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. 17 (2015) [hereinafter *Encryption and Technology Issues Hearing*] (statement of Cyrus R. Vance, Jr., District Attorney, New York County District Attorney's Office).

25 *See* Craig Timberg & Greg Miller, *FBI Blasts Apple, Google for Locking Police Out of Phones*, WASH. POST (Sept. 25, 2014), https://www.washingtonpost.com/business/technology/2014/09/25/68c4e08e-4344-11e4-9a15-137aa0153527_story.html. "Many perpetrators, particularly those who commit sexual offenses, take photos and videos of their acts, and store them on . . . smartphones." *Encryption and Technology Issues Hearing*, *supra* note 24, at 2.

26 *See, e.g.*, *Encryption and Technology Issues Hearing*, supra note 24; *Addressing Remaining Gaps in Federal, State, and Local Information Sharing: Hearing Before the Subcomm. on Counterterrorism & Intelligence of the H. Comm. on Homeland Sec.*, 114th Cong. 14 (2015) [hereinafter *Addressing Remaining Gaps in Federal, State, and Local Information Sharing Hearing*] (statement of Chief Richard Beary, President, International Association of Chiefs of Police); Congressman Peter T. King, *Remembering the Lessons of 9/11: Preserving Tools and Authorities in the Fight Against Terrorism*, 41 J. LEGIS. 173, 183 (2014–2015); Letter from Hillar C. Moore, III, *supra* note 17.

27 *Sen. Ron Johnson Holds a Hearing on Threats to the Homeland: Hearing Before S. Comm. on Homeland Sec. & Governmental Affairs*, 114th Cong. (2015) [hereinafter *Hearing on Threats to the Homeland*] (statement of James B. Comey, Director, Federal Bureau of Investigation); *see also* Apuzzo & Benner, *supra* note 15.

paign talk indicates that his administration is inclined to do so.[28] In February 2016, at a rally in South Carolina, and later that same day on Twitter, then-Republican presidential candidate Trump urged a boycott of all Apple products because of the company's refusal to help the FBI unlock the San Bernardino iPhone.[29] But assuming Trump follows the action plan of his predecessor, the Trump administration will attempt to achieve a solution via negotiation and forgo any legislative action.[30] Yet it is highly doubtful that tech companies will cooperate.[31] Technology companies—the most vocal of which is Apple—have publicly stated that they will not make their smartphones amenable to search warrants.[32]

Recent legislative proposals further threaten law enforcement's ability to access critical smartphone data. There are currently three pending bills in the U.S. Congress that would each forbid federal government agencies from mandating or requesting an access point into commercial products.[33] On February 11, 2016, a bipartisan group of legislators in Congress introduced the Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016 ("ENCRYPT Act").[34] The Act would prevent states and localities from passing laws banning encryption on smartphones sold in the United States.[35]

---

28 Kif Leswing, *'Boycott Apple'—3 Ways a Trump Presidency Could Affect Apple*, BUS. INSIDER (Nov. 9, 2016, 10:31 AM), http://www.businessinsider.com/how-trump-presidency-will-affect-apple-2016-11.

29 *Id.*; *see also* Pamela Engel, *TRUMP: 'Boycott All Apple Products,'* BUS. INSIDER (Feb. 19, 2016, 3:37 PM), http://www.businessinsider.com/donald-trump-boycott-apple-2016-2.

30 *See Hearing on Threats to the Homeland*, *supra* note 27; Apuzzo & Benner, *supra* note 15.

31 *See* Ellen Nakashima & Andrea Peterson, *Obama Administration Opts Not to Force Firms to Decrypt Data—For Now*, WASH. POST (Oct. 8, 2015), https://www.washingtonpost.com/world/national-security/obama-administration-opts-not-to-force-firms-to-decrypt-data—for-now/2015/10/08/1d6a6012-6dca-11e5-aa5b-f78a98956699_story.html.

32 According to Apple's website, "Apple has never worked with any government agency from any country to create a 'backdoor' in any of our products or services. . . . And we never will." Privacy, *Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ [https://perma.cc/KRV2-EAHX] (last visited Feb. 6, 2017); *see also supra* note 8.

33 *See* Secure Data Act of 2015, S. 135, 114th Cong. (2015); End Warrantless Surveillance of Americans Act, H.R. 2233, 114th Cong. (2015); Secure Data Act of 2015, H.R. 726, 114th Cong. (2015).

34 Ensuring National Constitutional Rights for Your Private Telecommunications (ENCRYPT) Act of 2016, H.R. 4528, 114th Cong. (2016).

35 *See id.*

This Note calls for Congress to immediately amend the Communications Assistance for Law Enforcement Act ("CALEA")[36] in order to account for the serious law enforcement threat that full-disk encryption poses.[37] Part I begins by providing relevant information on Apple and Google's full-disk encryption technology on their respective mobile operating systems. After establishing the technological basics, Part II explains the importance of smartphone data in twenty-first century investigations and prosecutions. Part II also discusses how full-disk encryption threatens law enforcement by making smartphone data inaccessible. After explaining why current proposals fail in Part III, Part IV introduces the CALEA and discusses its current inapplicability to smartphones. Part V calls for an amendment to the CALEA that makes the Act applicable to smartphones and imposes a civil penalty on both the manufacturer and mobile operating system provider for each instance law enforcement cannot decrypt a smartphone that it has the legal authority to search. Finally, Part VI defends the proposed amendment against potential counterarguments.

I. Full-Disk Encryption Technology on Apple and Google's Mobile Operating Systems

Full-disk encryption automatically converts "everything on a hard drive, including the operating system, into an unreadable form until the proper key (i.e., passcode) is entered."[38] In September 2014, Apple and Google announced that they had reengineered their mobile

36 Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1010 (2012).

37 This Note is limited to "full-disk" encryption. As such, the problem of "end-to-end" encryption is beyond the scope of this Note. This Note also does not address whether the First Amendment prohibits the government from requiring private companies to make smartphones amendable to search warrants. *Compare* Neil Richards, *Apple's "Code = Speech" Mistake*, MIT Tech. Rev. (Mar. 1, 2016) https://www.technologyreview.com/s/600916/apples-code-speech-mistake/ (requiring companies to make smartphones amenable to governmental search warrants does not violate the First Amendment), *with* Hayley Tsukayama, *We Asked a First Amendment Lawyer if Apple's 'Code Is Speech' Argument Holds Water. Here's What He Said.*, Wash. Post (Feb. 26, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/26/we-asked-a-first-amendment-lawyer-if-apples-code-is-speech-argument-holds-water-heres-what-he-said/ (arguing that a government request to build software that circumvents smartphone's security features "would essentially force Apple to say, in code, something" and thus violate the First Amendment).

38 Sarah Wilson, *Compelling Passwords from Third Parties: Why the Fourth and Fifth Amendments Do Not Adequately Protect Individuals when Third Parties Are Forced to Hand Over Passwords*, 30 Berkeley Tech. L.J. 1, 8 (2015).

operating systems[39] to include full-disk encryption technology by default.[40] Apple and Google also deliberately removed "backdoor"[41] access to passcodes, making it no longer feasible for the companies to comply with government warrants requesting data on locked smartphones.[42] Consequently, up to ninety-nine percent of all smartphones worldwide are rendered inaccessible to authorized government searches.[43] Due to the nuances inherent in the different systems, this Section begins by looking at the two most popular mobile operating system providers separately.

A. Apple

Apple manufactures smartphones, named iPhones, which run an operating system named iOS.[44] Numerical names designate different versions of the operating system (e.g., iOS 8).[45] Apple adopted full-disk encryption by default in September 2014 with iOS 8.[46] For all iPhones running iOS 8 and higher, Apple states that the company

---

39 A mobile operating system "manages the hardware and software components of smartphones." FRANCIS M. ALLEGRA & DANIEL B. GARRIE, PLUGGED IN: GUIDEBOOK TO SOFTWARE AND THE LAW § 5:3 (2015).

40 *See* Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, WALL ST. J. (Sept. 22, 2014, 7:42 PM), http://www.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341.

41 A "backdoor" is the term describing a mechanism or access point in a communications device or network that allows "the creator of software or hardware [to] access [the] data without the permission or knowledge of the user." Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 460 (2012).

42 According to Apple's website:

> On devices running iOS 8 and later versions, your personal data is placed under the protection of your passcode. For all devices running iOS 8 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess.

Privacy, *Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ [https://perma.cc/TU8X-T8BW] (last visited Feb. 6, 2017).

Niki Christoff, a Google spokeswoman, stated:

> For over three years Android has offered encryption, and keys are not stored off of the device, so they cannot be shared with law enforcement . . . . As part of our next Android release [Android Lollipop OS], encryption will be enabled by default out of the box, so you won't even have to think about turning it on.

Timberg, *supra* note 5.

43 This information is correct as of Q3 2016. *Smartphone OS Market Share*, 2016 Q3, INT'L DATA CORP., http://www.idc.com/prodserv/smartphone-os-market-share.jsp [https://perma.cc/F8QN-NF9S] (last visited Feb. 6, 2017).

44 *See iPhone*, APPLE, http://www.apple.com/iphone/ (last visited Feb. 6, 2017); *iOS 10*, APPLE, http://www.apple.com/ios/ios-10/ (last visited Feb. 6, 2017).

45 *iOS 10*, *supra* note 44.

46 *See* Barrett & Yadron, *supra* note 40.

"will not perform iOS data extractions [in response to government search warrants] as data extraction tools are no longer effective."[47] The majority of iPhones in circulation now function on software with full-disk encryption. As of January 4, 2017, approximately ninety-four percent of all iOS devices currently in use run iOS 9 and higher.[48]

B. Google

Google's mobile operating system is named Android.[49] Android operating systems are named after a dessert or candy (e.g., Éclair) and have a unique numerical identifier (e.g., 2.1).[50] Unlike iPhones, several manufacturers (called original equipment manufacturers ("OEMs")) produce Android-powered smartphones.[51]

Android users have had the ability to activate full-disk encryption on certain smartphones since the release of Honeycomb 3.0 in January 2011.[52] Shortly after Apple announced iOS 8 in 2014, Google said that it would make full-disk encryption mandatory for new Android-powered smartphones running Lollipop 5.0.[53] However, two months later, Google changed its position from requiring to "very strongly recommend[ing]" OEMs make full-disk encryption a default feature.[54] Despite this, the Google-manufactured Nexus smartphones running Lollipop 5.0 had full-disk encryption by default in 2014.[55]

---

47 *Legal Process Guidelines: U.S. Law Enforcement*, APPLE (Sept. 29, 2015), http://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf [https://perma.cc/RW8N-Z3W3].

48 Support, *Apple Developer*, APPLE, https://developer.apple.com/support/app-store/ (last visited Feb. 6, 2017).

49 J. Gregory Sidak, *Do Free Mobile Apps Harm Consumers?*, 52 SAN DIEGO L. REV. 619, 621 (2015).

50 *See* John D. Sutter, *Why Does Google Name Its Android Products After Desserts?*, CNN (Feb. 4, 2011, 11:07 AM), http://www.cnn.com/2011/TECH/innovation/02/04/google.honeycomb.android.names/.

51 OEMs of Android-powered smartphones include Google, Motorola, Samsung, HTC, LG, Sony, Asus, and Acer. *See* Brad Reed, *Here Are the Android OEMs That Do the Best Job of Getting You the Latest Software*, BGR (May 2, 2014, 4:42 PM), http://bgr.com/2014/05/02/android-software-updates-samsung-htc-motorola/.

52 *See* Jerry Hildenbrand, *How to Enable Encryption in Android*, ANDROID CENTRAL (Feb. 26, 2016, 2:31 PM), http://www.androidcentral.com/how-enable-encryption-andorid [https://perma.cc/J4FU-3JGP].

53 *See* Timberg, *supra* note 5; *A Sweet Lollipop, with a Kevlar Wrapping: New Security Features in Android 5.0*, ANDROID OFFICIAL BLOG (Oct. 28, 2014), https://android.googleblog.com/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html.

54 ANDROID, COMPATIBILITY DEFINITION: ANDROID 5.1 § 9.9 (last updated July 10, 2015), https://static.googleusercontent.com/media/source.android.com/en//compatibility/5.1/android-5.1-cdd.pdf.

55 *See* David Ruddock, *Android 6.0 Will Finally Require Manufacturers To Enable Full-Disk Encryption By Default On New Devices*, ANDROID POLICE (Oct. 19, 2015), http://

Google released Marshmallow 6.0 in October 2015.[56] That month, Google published an updated version of the Android Compatibility Definition Document ("CDD")[57] for Marshmallow 6.0 that requires OEMs to make full-disk encryption a default feature on all new Android-powered phones.[58] The percentage of Android-powered smartphones that have full-disk encryption by default is rapidly increasing. As of February 6, 2017, approximately sixty-five percent of Android-powered devices run Lollipop 5.0 or higher.[59]

II. How Full-Disk Encryption Threatens Law Enforcement

This Part starts by explaining the necessity of smartphone data in twenty-first century investigations and prosecutions, giving real life examples that demonstrate its importance. It then discusses how the inaccessibility of smartphone data inhibits law enforcement efforts, as the data is often available only on the physical phone. Finally, this Part ends by explaining how current legal and technological tools cannot access smartphone data protected by full-disk encryption.

A. Smartphones Frequently Contain Evidence Crucial to Criminal Investigations and Prosecutions

As of October 2015, sixty-eight percent of American adults have a smartphone.[60] The Supreme Court has recognized that the term "'cell phone' is itself misleading shorthand; many of these devices are in fact minicomputers" that "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[61] And these multiple func-

www.androidpolice.com/2015/10/19/android-6-0-will-finally-require-manufacturers-to-enable-full-disk-encryption-by-default-on-new-devices/.

56 *See* Sarah Mitroff, *Here Are the Android 6.0 Marshmallow Features that Matter*, CNET (Oct. 5, 2015, 8:00 AM), http://www.cnet.com/products/google-android-6-0-marshmallow/.

57 The CDD sets guidelines for OEMs. *See* Ruddock, *supra* note 55.

58 The new rule of mandatory full-disk encryption exempts smartphones launched with older versions of Android that upgraded to Marshmallow 6.0 later and smartphones that do not meet the minimum crypto-performance requirements. Android, Compatibility Definition: Android 7.1 at 80–81 (last updated Dec. 20, 2016), http://static.googleusercontent.com/media/source.android.com/en//compatibility/android-cdd.pdf.

59 According to Google, approximately 10.1% run Lollipop 5.0, 23.3% run Lollipop 5.1, 29.6% run Marshmallow 6.0, 0.5% run Nougat 7.0, and 0.2% run Nougat 7.1. *Dashboards*, Android, https://developer.android.com/about/dashboards/index.html (last visited Feb. 6, 2017).

60 Monica Anderson, *Technology Device Ownership: 2015*, Pew Res. Ctr. (Oct. 29, 2015), http://www.pewinternet.org/2015/10/29/technology-device-ownership-2015/.

61 Riley v. California, 134 S. Ct. 2473, 2489 (2014); *see, e.g.*, United States v. Zavala, 541 F.3d 562, 577 (5th Cir. 2008) ("A cell phone is similar to a personal computer that is carried on one's person . . . .").

tionalities are widely used.[62] Thus, to law enforcement agencies, smartphones are crucial repositories of potentially dispositive information.[63]

Law enforcement's inability to access smartphone data "means that lives may well be at risk or lost and those guilty parties may remain free."[64] Investigations and prosecutions of a wide range of cases rely on evidence found on smartphones. One such example is the Los Angeles Police Department's recent investigation into the death of a two-year-old girl.[65] Officers were able to ascertain that she died from blunt force trauma; however, they were unable to identify any eyewitnesses to the lethal event.[66] Investigators were ultimately able to charge the girl's parents based on text message exchanges stored on their smartphones.[67] These text messages revealed that the mother was responsible for the young girl's death, the father was aware of the lethal assault and failed to prevent it, and both parents failed to seek appropriate medical attention while the child convulsed in her crib.[68] The timely discovery of highly probative text message evidence convinced both parents to plead guilty.[69]

Additionally, smartphone data has exonerated innocent individuals in a variety of cases. In Kansas, cellphone data—a recovered deleted video—proved the innocence of several teens accused of rape.[70] Similarly, in Manhattan, a detective found several iPhones at the

---

62 *See Mobile Technology Fact Sheet*, PEW RES. CTR. (Dec. 27, 2013), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/9/ [https://web.archive.org/web/20160603030022/http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/9/] (stating that as of May 2013, eighty-one percent of adult cell owners use their phones to send or receive text messages, sixty-three percent use their phones to go online, fifty-two percent use their phones to send or receive email, fifty percent use their phones to download apps, and forty-nine percent use their phones to get directions, recommendations, or other location-based information).

63 *See Encryption and Technology Issues Hearing*, *supra* note 24, at 14–17.

64 *Addressing Remaining Gaps in Federal, State, and Local Information Sharing Hearing*, *supra* note 26, at 15. As of April 2016, the Manhattan District Attorney's Office possesses 175 iPhones that it cannot unlock. Katie Benner & Matt Apuzzo, *Narrow Focus May Aid F.B.I. in Apple Case*, N.Y. TIMES (Feb. 22, 2016), http://www.nytimes.com/2016/02/23/technology/apple-unlock-iphone-san-bernardino.html?_r=0.

65 *See* James B. Comey, Dir., Fed. Bureau of Investigation, Speech at the Brookings Institution, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) (transcript at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course).

66 *Id.*

67 *Id.*

68 *Id.*

69 *See id.*

70 *Id.*

scene of a homicide.[71] Investigators obtained a search warrant and unlock order and, with Apple's cooperation, extracted critical evidence from the smartphones.[72] The iPhone data showed inaccuracies in the investigators' initial timeline and that a suspect was not involved in the homicide.[73] Investigators linked a phone number in one of the iPhones to another individual, who later confessed and pled guilty.[74]

B. A Significant Amount of Data Is Only Contained on the Physical Smartphone

A number of commentators believe that law enforcement's ability to pursue other, more traditional avenues of investigation diminishes the need for smartphone data contained on the physical device.[75] However, a report conducted by the New York County (Manhattan) District Attorney's Office shows that certain crucial data only exists on the physical smartphone.[76] The table in the Appendix shows that iMessage[77] content and details (e.g., dates, times, phone numbers involved), SMS/MMS[78] content, historical cell site data, historical GPS data, contacts, photos/videos, internet search history, internet bookmarks, and third-party app data can only be accessed on the physical phone.[79] Phone companies can likely only provide SMS/MMS and phone call details.[80]

Many critics argue that smartphone operating system providers and manufacturers do not need to make their devices amenable to

---

71 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, SMARTPHONE ENCRYPTION AND PUBLIC SAFETY 11 (Nov. 2015).

72 *Id.* In the past, mobile operating system providers assisted law enforcement agencies in accessing smartphone data. *See infra* notes 148–49 and accompanying text.

73 *Id.*

74 *Id.*

75 *See, e.g.*, MATTHEW G. OLSEN ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U., DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 9–15 (2016).

76 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 6–8.

77 iMessage is a service akin to text messaging; it allows iPhone users to "send messages back and forth with anyone on iPad, iPhone, iPod touch, or a Mac running [the operating system] Mountain Lion or later." Bodyxs, Comment to *imessage*, APPLE (Oct. 17, 2014, 7:53 PM), https://discussions.apple.com/thread/6599367?start=0&tstart=0. iMessages may contain text and attachments such as photos, videos, locations, links, and contacts. *See* SUPPORT, *Learn how to use Messages*, APPLE, https://support.apple.com/explore/messages (last visited Feb. 6, 2017).

78 iPhones and Android-powered smartphones can send Short Messages Service ("SMS") messages and Multimedia Messaging Service ("MMS") messages. SMS messages are "text messages of up to 160 characters in length." MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 24 n.9. MMS messages "include messages with multimedia content, like photos [or video]." *Id.*

79 *See infra* Appendix.

80 *See infra* Appendix.

searches because law enforcement can already lawfully search suspects' cloud accounts.[81] But data stored in the cloud does not necessarily reflect all of the data stored within a smartphone device.[82]

Smartphone users do not have to set up a cloud account or back up their data to it.[83] Accordingly, even "minimally sophisticated wrongdoers" can simply choose not to back up their smartphone data to a cloud storage service and successfully obfuscate crimes facilitated through their phones.[84] Indeed, in the San Bernardino case, Farook had disabled iCloud backups for certain apps and data on his phone,[85] and the last backup was made about six weeks before the attacks.[86] But the problem is not limited to the wrongdoer who uses his smartphone in perpetration of crime. A future victim may hinder investigation of the crime(s) committed against him by not regularly backing up all data to a cloud server.

Beyond hiding information from potential law enforcement access, there is a myriad of reasons why a user may not set up a cloud account or back up all his data to it. Cloud providers only offer a small amount of storage space for free; additional space must be purchased.[87] The cost of extra storage space may deter users from backing

81 *See, e.g.*, OLSEN ET AL., *supra* note 75, at 9, 11.

82 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 8.

83 *Id.*

84 *Encryption and Technology Issues Hearing*, *supra* note 24, at 6.

85 Backups for "Mail," "Photos," and "Notes" were all turned off on his iPhone. Supplemental Declaration of Christopher Pluhar in Support of Government's Reply in Support of Motion to Compel and Opposition to Apple Inc.'s Motion to Vacate Order at 4, *In re* The Search of an Apple iPhone During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (SP) (C.D. Cal. Mar. 10, 2016) [hereinafter Supplemental Declaration of Christopher Pluhar].

86 *Id.* at 3–4.

87 iPhone users can back up information to iCloud. *iCloud*, APPLE, http://www.apple.com/icloud/ (last visited Feb. 6, 2017). The first five gigabytes ("GB") of storage on an iCloud account are free. *Id.* Users can upgrade their iCloud storage to 50 GB for $0.99 per month, to 200 GB for $2.99 per month, to 1 terabyte ("TB") for $9.99 per month, and to 2 TB for $19.99 per month. *Id.* iPhones come with either 16, 32, 64, 128, or 256 GBs of storage space on the device itself. *Compare iPhone models*, APPLE, http://www.apple.com/iphone/compare/ (last visited Feb. 6, 2017). Google has several locations for cloud storage. iPhones and Android-powered smartphones can both back up data to Google's cloud. Google offers an initial 15 GB of cloud storage space at no cost that is shared across three of its services: Google Drive, Gmail, and Google+ Photos. *Pricing Guide*, GOOGLE DRIVE, https://www.google.com/drive/pricing/ (last visited Feb. 6, 2017). After that, a Google cloud user can upgrade to 100 GB for $1.99 per month, to 1 TB for $9.99 per month, to 10 TB for $99.99 per month, to 20 TB for $199.99 per month, and to 30 TB for $299.99 per month. *Id.* Many Android smartphones have a minimum of 16 GB of storage space, *see Phones*, ANDROID, https://www.android.com/phones/ (last visited Feb. 6, 2017), and one can hold up to 640 GB, *see V SQUARED Specs*, SAYGUS, https://www.saygus.com/v2-2/ (last visited Feb. 6, 2017).

up significant portions of their data. Users can also elect to remove certain types of content from the backup process.[88] Many opt to upload a limited number of specific files for a variety of reasons, including conserving storage space and protecting sensitive information from hacker attacks.[89] Additionally, some cloud accounts require the user to access a Wi-Fi connection before backing up data to the cloud.[90] Cloud accounts thus typically contain little or no data of interest to law enforcement—in fact, the "most common use for cloud storage is music."[91]

Without access to a smartphone's data, law enforcement has "no reasonable way" of determining which mobile cloud service(s) a person uses for storage.[92] Even assuming that access to a cloud account produces the same information obtained from a physical phone, law enforcement still must identify the relevant mobile cloud service provider(s) before they can access data stored on the account. Apple, Google, Dropbox, and Microsoft all offer mobile cloud storage.[93] Because locating the user's mobile cloud server(s) is time-intensive, law enforcement may not be able to locate a user's account(s) before the user or an accomplice permanently deletes all evidence.[94]

Additionally, it is more difficult for a prosecutor to establish ownership of a cloud account. A phone may be discovered on a defendant's person or within an area of his control (e.g., house, car), which raises an inference of ownership and would likely only require the testimony of one witness (e.g., the officer who recovered the device).[95] By contrast, to prove ownership of a cloud account, "[a] prosecutor

88 *See* SUPPORT, *iCloud: Change iCloud Feature Settings*, APPLE (Dec. 13, 2016), https://support.apple.com/kb/ph2613?locale=EN_US; *cf.* Drive Help, *Back Up Photos & Videos Automatically in Google Drive: Android*, GOOGLE, https://support.google.com/drive/answer/6093613?hl=en&ref_topic=7000756&co=GENIE&co=GENIE.Platform%3DAndroid&oco=1 (last visited Feb. 6, 2017) (describing how users may enable or disable automatic backup).

89 There have been several recent, highly-publicized hacks of cloud accounts. For example, "Celebgate" involved a man hacking 50 iCloud and 72 Gmail accounts of celebrities and leaking personal information contained therein, including nude photographs. *See* Jon Blistein, *Hacker Pleads Guilty to Stealing Celebrity Nude Photos*, ROLLINGSTONE (Mar. 15, 2016), http://www.rollingstone.com/movies/news/hacker-pleads-guilty-to-stealing-celebrity-nude-photos-20160315.

90 *See iCloud*, *supra* note 87.

91 *Apple's iCloud Is Most-Used Cloud Service in the US, Beating Dropbox & Amazon*, APPLEINSIDER (Mar. 21, 2013, 8:55 AM), http://appleinsider.com/articles/13/03/21/apples-icloud-is-most-used-cloud-service-in-the-us-beating-dropbox-amazon; *see* Supplemental Declaration of Christopher Pluhar, *supra* note 85, at 4.

92 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 8.

93 *Id.*

94 *See Encryption and Technology Issues Hearing*, *supra* note 24, at 7.

95 *Id.*

may need to present testimony or records from [the mobile cloud provider] relating to the subscriber information, IP login history, and/or content of the account, testimony or records from internet service providers regarding the subscriber information of certain IP addresses, and/or testimony of forensic analysts."[96] Mere potential access to a cloud account is thus insufficient.

C. Current Legal and Technological Tools Cannot Crack Full-Disk Encryption

Defendants often do not consent to smartphone searches or choose to disclose their passcodes.[97] Sometimes a passcode cannot be obtained because the user's identity is unknown (e.g., a phone found at a crime scene) or the user is unavailable because he has been abducted or killed (e.g., a phone of a kidnapping or murder victim).[98] Law enforcement thus has to turn to alternative methods of gaining access into the phone, including using brute force and asking the service providers themselves—none of which is particularly helpful.

1. Law Enforcement Likely Cannot Force Defendants to Unlock Their Smartphones

Under the Fifth Amendment, "[n]o person shall be . . . compelled in any criminal case to be a witness against himself."[99] There are three elements an individual must establish in order to invoke this privilege: (1) compulsion; (2) a testimonial communication; and (3) incrimination.[100]

Caselaw indicates that the government violates a defendant's Fifth Amendment right against self-incrimination when it compels the defendant to *tell* his numerical or alphanumerical passcode.[101] Al-

96 *Id.*

97 There are a number of reported cases in which suspects refused to surrender their passwords, *see, e.g.*, United States v. Diermyer, No. 3:10-cr-071-HRH-JDR, 2010 WL 4683550, at *2 (D. Alaska Nov. 12, 2010); Griffin-El v. Beard, No. 06-2719, 2009 WL 2929802, at *2 (E.D. Pa. Sept. 8, 2009); United States v. Horton, No. 4:08CR3005, 2009 WL 1872612, at *7 (D. Neb. June 30, 2009), or conveniently "forgot" them, *see* Matt Apuzzo et al., *Apple's Line in the Sand Was Over a Year in the Making*, N.Y. TIMES (Feb. 18, 2016), http://www.nytimes.com/2016/02/19/technology/a-yearlong-road-to-a-standoff-with-the-fbi.html.

98 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 4.

99 U.S. CONST. amend. V. The Fifth Amendment's privilege from compulsory self-incrimination has been "incorporated" by the Fourteenth Amendment so that the privilege applies to state criminal proceedings as well as federal. *See* Griffin v. California, 380 U.S. 609, 615 (1965); Malloy v. Hogan, 378 U.S. 1, 6 (1964).

100 *In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335, 1341 (11th Cir. 2012).

101 *See, e.g.*, *id.* at 1346 (compelling an individual's passcode constitutes a violation of his Fifth Amendment self-incrimination privilege); SEC v. Huang, No. 15-269, 2015 WL 5611644, at

though the Supreme Court has not yet ruled on this precise issue, dicta in *Doe v. United States*[102] strongly suggests that the Court would find that requiring a defendant to disclose his passcode would violate the Fifth Amendment right against compulsory self-incrimination.[103] Indeed, lower courts are mostly in agreement that disclosing a passcode is "incriminating" within Supreme Court jurisprudence.[104]

Although the government cannot compel an individual to disclose his passcode, it may be able to require a defendant to unlock his phone using his fingerprint if the smartphone has a biometric fingerprint scanner.[105] At first blush, the solution seems promising. However, because "biometric authentication cannot be set up without first creating a passcode" (thus directly linking authentication to a passcode), commentators contend that a fingerprint scan still constitutes a Fifth Amendment violation.[106] Additionally, not all smartphones have fingerprint authentication technology.[107] Even for smartphones that

---

*2–3 (E.D. Pa. Sept. 23, 2015) (same); United States v. Kirschner, 823 F. Supp. 2d 665, 668–69 (E.D. Mich. 2010) (same); United States v. Rogozin, No. 09-CR-379(S)(M), 2010 WL 4628520, at *6 (W.D.N.Y. Nov. 16, 2010) (same); Virginia v. Baust, No. CR14-1439, 2014 WL 6709960, at *3 (Va. Cir. Ct. 2014) (same).

102 487 U.S. 201 (1988).

103 The Court declared that "be[ing] forced to surrender a key to a strongbox containing incriminating documents" is non-testimonial, while "be[ing] compelled to reveal the combination to [a] wall safe" is. *Id.* at 210 n.9 (quoting *id.* at 219 (Stevens, J., dissenting)). In sum, a defendant cannot be forced to disclose the contents of his mind. *Id.*

104 *See* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. HEIGHTENED SCRUTINY 11, 24 (2012) ("Courts generally agree that divulging a password constitutes a testimonial act.").

105 *See Baust*, 2014 WL 6709960, at *3 (holding that a "[d]efendant cannot be compelled to produce his passcode to access his smartphone but he can be compelled to produce his fingerprint to do the same," because his "fingerprint, like a key . . . does not require the witness to divulge anything through his mental processes").

106 Erin M. Sales, Note, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free from Self-Incrimination*, 69 U. MIAMI L. REV. 193, 227 (2014). A defendant forced to unlock his smartphone using his fingerprint was arguably compelled to indirectly disclose knowledge of the passcode because the fingerprint is connected to the passcode:

> Thus, unlike the cases where the Supreme Court has held that compelling the suspect to be the source of physical evidence did not violate the self-incrimination privilege, a court may consider biometric authentication differently. In those cases, the physical evidence was not linked to any knowledge. The blood analysis in *Schmerber*, the blouse modeling in *Holt*, the speech in *Wade*, and the handwriting exemplar in *Gilbert*, all occurred without the defendant creating a passcode committed to his and only his memory.

Id. at 228 (footnotes omitted).

107 On certain iPhones, the user can enable Touch ID, a fingerprint sensing system that requires the user's fingerprint to unlock the device. *See* APPLE INC., IOS SECURITY 7 (Sept. 2014) [hereinafter IOS SECURITY GUIDE]. Some Android devices have fingerprint scanners, which allow the user to unlock the device with their fingerprint. *See* Google Store, *Android 6.0 Marsh-*

have such technology, the user is not required to enable it.[108] In other words, the user could choose to only have a numerical or alphanumerical passcode.[109] Thus, a defendant looking to keep the contents of his smartphone from law enforcement will simply not enable the biometric authentication function.

The "forgone conclusion" exception, which applies if the government learns "little or nothing" from the information conveyed by the defendant's act of production,[110] may allow the government to require the defendant to unlock his smartphone *using* his passcode[111] or to provide its decrypted contents.[112] In either circumstance, only the data on the smartphone, not the passcode itself, would be revealed.[113] It is "difficult" for the government to "clear the 'foregone conclusion' hurdle."[114] The Eleventh Circuit is currently the only federal appeals court to have ruled on the standard the government must meet to satisfy the foregone conclusion exception.[115] In *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*,[116] law enforcement believed the defendant was using a specific Youtube.com account to share sexually explicit material of underage girls.[117] Investigators were able to seize several of the defendant's laptops and external hard drives, however, forensic examiners were unable to access parts of the encrypted drives.[118] A grand jury subpoena required the defendant to produce the "unencrypted contents" of the digital media.[119] A forensic

---

mallow. S'more to Love, GOOGLE, https://store.google.com/magazine/android_6_platform_story (last visited Jan. 18, 2017). However, due to the variety of OEMs making Android devices, not all Android devices can be unlocked using the user's fingerprint. MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 3.

108 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 2–3.

109 *See id.* at 3.

110 Fisher v. United States, 425 U.S. 391, 411 (1976) ("The existence and location of the papers are a foregone conclusion and the taxpayer adds little or nothing to the sum total of the Government's information by conceding that he in fact has the papers.").

111 *See* Commonwealth v. Gelfgatt, 11 N.E.3d 605, 614 (Mass. 2014); Orin Kerr, *Apple's Dangerous Game*, WASH. POST: THE VOLOKH CONSPIRACY (Sept. 19, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/09/19/apples-dangerous-game/.

112 *See, e.g.*, United States v. Fricosu, 841 F. Supp. 2d 1232, 1235, 1238 (D. Colo. 2012) (directing the defendant to provide a decrypted copy of her computer's hard drive where its contents were accessible only by entry of a passcode); *In re* Grand Jury Subpoena to Boucher, No. 2:06-mj-91, 2009 WL 424718, at *1, *4 (D. Vt. Feb. 19, 2009) (same).

113 *See supra* notes 111–112.

114 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 5.

115 *See generally In re* Grand Jury Subpoena Duces Tecum, 670 F.3d 1335 (11th Cir. 2012).

116 670 F.3d 1335 (11th Cir. 2012).

117 *Id.* at 1339.

118 *Id.*

119 *Id.*

examiner for the government testified that they believed data existed on the encrypted parts of the hard drive because the still-encrypted parts contained nonsensical characters and numbers.[120] The examiner believed that these characters and numbers suggested the presence of an encrypted form of data.[121]

The Eleventh Circuit rejected the government's contention that the existence of evidence on the hard drive was a foregone conclusion.[122] The court noted that while the government showed that "the drives *could* contain files," the government did not meet its burden to show that "the drives *actually* contain any files."[123] It does not appear that the requisite probable cause standard for a search warrant would satisfy the foregone conclusion exception. The "substance" of probable cause only requires a "reasonable ground" for belief that a phone contains evidence of a crime;[124] the standard "does not demand any showing that such a belief be correct or [even] more likely true than false."[125] Additionally, the "foregone conclusion" exception does not apply to situations where the defendant denies ownership or control of the smartphone.[126]

2. *Law Enforcement Cannot Use Brute Force to Unlock Smartphones*

Smartphones protected by full-disk encryption can theoretically be unlocked using "brute force," which is a trial and error method that involves running through all possible passcode combinations (e.g., "1,1,1,1," "1,1,1,2," "1,1,1,3").[127] However, brute force extraction of data from smartphones is highly unavailing for two reasons.

First, brute force extractions are so time-intensive that they are frequently considered an unviable extraction alternative.[128] This is be-

120 *Id.* at 1340.

121 *Id.*

122 *See id.* at 1346.

123 *Id.* at 1347–48 ("*Fisher* and *Hubbell* . . . require that the Government show its knowledge *that the files exist*."); *see also* SEC v. Huang, No. 15-269, 2015 WL 5611644, at *4 (E.D. Pa. Sept. 23, 2015) ("Here, the SEC has no evidence any documents it seeks are actually located on the work-issued smartphones, or that they exist at all. Thus, the foregone conclusion doctrine is not applicable.").

124 Brinegar v. United States, 338 U.S. 160, 175 (1949).

125 Texas v. Brown, 460 U.S. 730, 742 (1983).

126 *See* Fisher v. United States, 425 U.S. 391, 410, 412 (1976).

127 Martin Kaste, *Your Smartphone Is a Crucial Police Tool, If They Can Crack It*, NPR: ALL TECH CONSIDERED (Mar. 25, 2014, 2:54 PM), http://www.npr.org/sections/alltechconsidered/2014/03/25/291925559/your-smartphone-is-a-crucial-police-tool-if-they-can-crack-it; MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 4.

128 *See, e.g.*, *Encryption and Technology Issues Hearing*, *supra* note 24, at 4; Lily Hay New-

cause iOS and Android discourage passcode attacks with escalating time delays that trigger after an invalid passcode is entered at the lock screen.[129] Time delays dramatically limit the efficacy of brute force attempts; according to Apple, "it would take more than 5½ years to try all combinations of a six-character alphanumeric passcode with lowercase letters and numbers."[130] Four-digit numerical passcodes may require less time, but they still could take up to 10,000 guesses.[131] In regards to iPhones, passcodes (otherwise known as Personal Identification Numbers ("PINs")) must be entered by hand on the physical device, one at a time.[132]

Second, brute force could result in a complete data wipe once a maximum number of incorrect passcodes is entered. For iOS, "[u]sers can choose to have the device automatically wiped if the passcode is entered incorrectly after 10 consecutive attempts."[133] Similarly, for Android, the data may become permanently inaccessible if a user enters an incorrect passcode a certain number of times in a row.[134]

3. The Recent Unlocking of the San Bernardino iPhone Does Not Create a Viable Method to Access a Smartphone's Contents

Although an anonymous hacker was able to access data on the San Bernardino iPhone for the FBI, this one-time unlocking is not a permanent or viable solution. As mentioned above, the FBI is un-

---

man, *Federal Judge Says Law Enforcement Can't Make You Hand Over Your Smartphone Passcode*, SLATE: FUTURE TENSE (Sept. 25, 2015, 2:41 PM), http://www.slate.com/blogs/future_tense/2015/09/25/court_rules_that_defendants_don_t_have_to_provide_smartphone_passcodes.html.

129 *See* APPLE, iOS SECURITY, iOS 9.0 OR LATER 12 (Sept. 2015).

130 *Id.* For iPhones, iOS 9 and higher now ask for a six-digit passcode by default. Jason Cipriani, *Secure Your iOS Device With a Six-Digit Passcode on iOS 9*, CNET (Sept. 11, 2015, 10:58 AM), http://www.cnet.com/how-to/secure-your-ios-device-with-a-six-digit-passcode-on-ios-9/. However, users can manually switch to a four-digit numeric code, a custom numeric code, or a custom alphanumeric code. *See* iOS SECURITY, iOS 9.0 OR LATER, *supra* note 129, at 12. For Android-powered smartphones operating on Froyo 2.2 and higher, the phone offers the ability to lock the device using a numeric or alphanumeric passcode. *See* Phil Nickinson, *Password Protect Your Phone*, ANDROID CENTRAL (Aug. 6, 2010, 11:16 AM), http://www.androidcentral.com/password-protect-your-phone.

131 Martin Kaste, *The Security Cracks In Your Smartphone*, NPR: ALL TECH CONSIDERED (Mar. 25, 2014, 2:49 PM), http://www.npr.org/sections/alltechconsidered/2014/03/25/291942703/the-security-cracks-in-your-smartphone.

132 Chris Smith, *Does Apple Even Have the Ability to Hack the iPhone Like the FBI Wants?*, BGR (Feb. 17, 2016, 12:33 PM), http://bgr.com/2016/02/17/apple-iphone-security-backdoors/.

133 iOS SECURITY GUIDE, *supra* note 107, at 11; *see also* iOS SECURITY, iOS 9.0 OR LATER, *supra* note 129, at 12.

134 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 3.

likely to share the method in every single case that involves smartphone encryption.[135] Because Apple is proactively trying to isolate and mitigate this security vulnerability,[136] the FBI has chosen to selectively use its newly-found "key" in order to protect its secrecy.[137] This fear is not unfounded; in the past, Apple has developed new security measures to close weaknesses exposed by hackers.[138] Moreover, many technology experts have speculated on the method used by the anonymous hacker—increasing the likelihood that Apple will uncover the vulnerability.[139] Apple may even pursue legal measures to force the government to disclose the vulnerability.[140] Regardless of whether Apple uncovers the actual method used, Apple engineers are continually strengthening the security of iPhones and their corresponding encryption technology.[141] For example, on March 21, 2016, Apple released iOS 9.3 which corrected an encryption flaw in iMessage.[142]

Even assuming the FBI does share its "key" before Apple can close the vulnerability, technology experts note that it may not work on every iPhone.[143] Additionally, iOS and Android are distinct mobile operating systems (with, by extension, distinct vulnerabilities) and a hack that works for one will likely not work for the other.[144]

Finally, the government's continued, ad hoc reliance on anonymous, third-party hackers disservices the public. A hacking service that only one—or at most, a few—can perform creates a hacker-controlled monopoly. A hacker who can successfully extract data from a full-disk encrypted smartphone can demand a very high price for his services.[145] Assuming future mobile operating systems have unique se-

---

135 *See* Learmonth, *supra* note 16.

136 *See supra* notes 13–15 and accompanying text.

137 *See* Learmonth, *supra* note 16.

138 *See* Apuzzo & Benner, *supra* note 15 ("Apple regularly publishes security updates and gives credit to researchers who hunt for bugs in the company's software.").

139 *See* Benner et al., *supra* note 15; Alina Selyukh, *The Apple-FBI Whodunit: Who Is Helping The Feds Crack The Locked iPhone?*, NPR: ALL TECH CONSIDERED (Mar. 23, 2016, 5:58 PM), http://www.npr.org/sections/alltechconsidered/2016/03/23/470573608/the-apple-fbi-whodunit-whos-helping-the-feds-crack-the-locked-iphone.

140 *See* Selyukh, *supra* note 13; Strohm et al., *supra* note 14.

141 *See* Apuzzo & Benner, *supra* note 15.

142 *See* Tim Moynihan, *Apple iOS 9.3 Is Available Today. Here's Why You Want It*, WIRED (Mar. 21, 2016, 1:56 PM), http://www.wired.com/2016/03/ios-9-3-is-available/.

143 *See* Richard Winton & James Queally, *Will the FBI Share Its iPhone-Cracking Method with Police? Probably Not*, L.A. TIMES (Mar. 29, 2016, 4:59 PM) http://www.latimes.com/local/lanow/la-me-ln-police-phone-access-san-bernardino-20160329-story.html.

144 *See id.*

145 Rewards can total in the millions for hackers able to demonstrate critical security vulnerabilities: Google has paid outside hackers more than $6 million for finding security flaws. *See*

curity flaws that allow a hacker to access the smartphone's contents, the government will continually have to use taxpayer dollars to pay substantial bounties for each updated system.[146] Alternatively, hackers could stop performing data extractions altogether for future mobile operating systems.[147]

4. Apple and Google Refuse to Comply with Government Search Warrants

In cases where a passcode is withheld or unable to be obtained, a prosecutor can apply to a court for a search warrant.[148] Law enforcement agencies used to be able to obtain search warrants and orders (often referred to as "unlock orders") that required tech companies to assist in data extraction procedures.[149] After obtaining an unlock order,

> [t]he prosecutor . . . then sends . . . a copy of the warrant, the unlock order, the device, and a blank external hard drive. [The mobile operating system provider] uses a proprietary method to extract data from the device, and sends a copy of the data to law enforcement on the external hard drive.[150]

However, in several recent cases, Apple has challenged the legal validity of unlock orders.[151] Many technology companies, including

---

Nicole Perlroth & Katie Benner, *Apple Policy on Bugs May Explain Why Hackers Would Help F.B.I.*, N.Y. TIMES (Mar. 22, 2016), http://www.nytimes.com/2016/03/23/technology/apple-policy-on-bugs-may-explain-why-hackers-might-help-fbi.html.

146 Cellebrite, an Israeli data forensics firm, is rumored to be the anonymous hacker that unlocked the iPhone 5c in the San Bernardino case. *See, e.g.*, Mikey Campbell, *Cellebrite Again Rumored to Have Accessed San Bernardino iPhone 5c for FBI*, APPLEINSIDER (Apr. 1, 2016, 3:54 PM), http://appleinsider.com/articles/16/04/01/-cellebrite-again-rumored-to-have-accessed-san-bernardino-iphone-5c-for-fbi. Cellebrite signed a $218,000 contract with the FBI the same day DOJ announced it unlocked the iPhone. *Id.* Over the last seven years, the FBI purchased forensic tools from Cellebrite averaging $10,883 each. *Id.* The $218,000 is the largest to date. *Id.*

147 *See* Paresh Dave, *Why Few Hackers Are Lining Up to Help FBI Crack iPhone Encryption*, L.A. TIMES (Mar. 23, 2016, 6:17 PM), http://www.latimes.com/business/technology/la-fi-tn-apple-hackers-20160323-snap-htmlstory.html (noting that the stigma of assisting the FBI with an investigation could deter potential hackers).

148 The Supreme Court held that warrants based on probable cause are required for searches of smartphone data, absent an exception. Riley v. California, 134 S. Ct. 2473, 2485 (2014).

149 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 4.

150 *Id.*

151 *See* Apple Inc.'s Motion to Vacate Order Compelling Apple Inc. to Assist in Search, and Opposition to Government's Motion to Compel Assistance, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. CM 16-10 (SP), 2016 WL 618401 (C.D. Cal. Feb. 25, 2016) [hereinafter Apple Inc.'s Motion to Vacate Order]; Apple Inc.'s Supplemental Response to Court's October 9, 2015 Order and Opinion, *In re* Apple, Inc., No. 15 MISC 1902 (JO) (E.D.N.Y. Oct. 23, 2015).

Google, have filed amicus briefs in support of Apple.[152] Unlock orders, thus, are no longer an effective way of compelling tech companies to extract data from full-disk encrypted smartphones.[153]

III. Critique of Other Proposals

There have been attempts to remedy this problem before. A judicial approach through the use of the All Writs Act and several legislative approaches, both on the federal and state levels, have been put forth. Taking each proposal in turn, this Part demonstrates why they are not sufficient.

A. The All Writs Act

In two highly publicized cases, the DOJ tried to use the All Writs Act to get a court order requiring Apple to help the government access data on locked, encrypted iPhones.[154] The All Writs Act says that courts have broad statutory authority to issue orders necessary to effectively carry out the duties of an independent judiciary.[155] Thus, courts may issue orders when three requirements are satisfied: (1) the issuance of the writ is "in aid of" the issuing court's jurisdiction; (2) the type of writ requested is "necessary or appropriate" to provide such aid to the issuing court's jurisdiction; and (3) the issuance of the writ is "agreeable to the usages and principles of law."[156] Apple's public statements and court filings demonstrate its opposition to writ-based unlock orders.[157] The government's use of the All Writs Act is problematic for three primary reasons.

---

152 *See, e.g.*, Brief for Amazon.com et al. as Amici Curiae Supporting Apple, Inc., *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED CM 16-10 (SP) (Mar. 4, 2016); Brief for Airbnb, Inc. et al. as Amici Curiae Supporting Apple, Inc., *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED CM 16-10 (SP) (Mar. 3, 2016).

153 *See infra* Section III.A.

154 *See In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED 15-0451M, 2016 WL 618401, at *1 (C.D. Cal. Feb. 16, 2016); *In re* Apple, Inc., 149 F. Supp. 3d 341, 344 (E.D.N.Y. 2016).

155 The All Writs Act states: "The Supreme Court and all courts established by Act of Congress may issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a) (2012).

156 *In re Apple, Inc.*, 149 F. Supp. 3d at 350; *see, e.g.*, United States v. Williams, 400 F.3d 277, 280–81 (5th Cir. 2005) (quoting *In re* United States, 397 F.3d 274, 282 (5th Cir. 2005)).

157 *See The Encryption Tightrope: Balancing Americans' Security and Privacy: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 100 (2016) (statement of Bruce Sewell, Senior Vice President & General Counsel, Apple, Inc.); Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 14–15; Customer Letter, *supra* note 8.

First, numerous critics argue that the All Writs Act cannot be extended to compel private companies, like Apple and Google, to assist the government in unlocking encrypted smartphones.[158] Currently the only legal precedent on the issue of whether a court has the power to issue such an order is in Apple's favor.[159] In *In re Apple, Inc.*,[160] Judge Orenstein based his denial to extend the All Writs Act partly on the fact that Congress has yet to pass a law explicitly requiring tech companies to provide assistance to law enforcement.[161] Both the DOJ and Apple agreed that the CALEA[162] currently does not compel a private company to help law enforcement agencies unlock encrypted smartphones.[163] Judge Orenstein held that this omission reflects a legislative choice to exempt tech companies from complying with unlock orders for encrypted smartphones.[164] He also found that, alternatively, Apple was an "information service provider" and thus expressly exempted under the CALEA from providing the governmental assistance sought.[165]

Second, some critics argue that the government's use of the All Writs Act adds to the loss of confidence in oversight of the American national security establishment.[166] Numerous technology companies, including Apple and Google, redesigned their products to include encryption in direct response to Edward Snowden's infamous disclosure regarding the U.S. government's mass surveillance.[167] The DOJ's current reliance on the All Writs Act reignites fears tied to governmental circumvention of democratic and legal processes for investigatory purposes—"invoking 'terrorism' and moving *ex parte* behind closed courtroom doors, the government sought to cut off debate and circumvent thoughtful analysis."[168] Indeed, opponents view the government's application of the All Writs Act as an "unlimited" and

158 *See, e.g.*, Brief for Airbnb, Inc. et al., *supra* note 152; Brief for Amazon.com et al., *supra* note 152; Brief for AT&T Mobility LLC as Amici Curiae Supporting Apple, Inc. at 4–6, *In re* Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, Cal. License Plate 35KGD203, No. ED CM 16-10 (SP) (C.D. Cal. Mar. 3, 2016).

159 *See In re* Apple, Inc., 149 F. Supp. 3d at 344, 351.

160 149 F. Supp. 3d 341 (E.D.N.Y. 2016).

161 *See id.* at 355–59.

162 For a discussion on the CALEA, see *infra* Part IV.

163 *In re Apple, Inc*., 149 F. Supp. 3d at 355.

164 *See id.* at 355–59.

165 *See id.* at 356–57.

166 *See, e.g.*, Yochai Benkler, *We Cannot Trust Our Government, So We Must Trust the Technology*, GUARDIAN (Feb. 22, 2016, 8:00 AM), http://www.theguardian.com/us-news/2016/feb/22/snowden-government-trust-encryption-apple-fbi.

167 *See* Apuzzo & Benner, *supra* note 15.

168 Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 2, 5.

"sweeping use of the judicial process."[169] Critics believe that the All Writs Act does not sufficiently hold the government accountable and guard privacy interests. They warn that this precedent could be extended to access data from other products and unwilling private companies (e.g., microphones on televisions, computers, and even children's toys).[170]

Third, reliance on the All Writs Act would produce inconsistent results. Even if a subsequent court were to grant the government's order, the All Writs Act is discretionary and judges are not required to grant orders even if all three statutory requirements are met.[171] Moreover, historically, legislatures have prescribed mandatory law enforcement assistance requirements that involve technological changes on the part of private companies.[172] The "information environment of legislative rulemaking is superior to that of judicial rulemaking in the context of developing technologies."[173] Unlike Congress,[174] "[j]udges decide cases based primarily on a brief factual record, narrowly argued legal briefs, and a short oral argument. They must decide their cases in a timely fashion, and can put only so much effort into any one case."[175] Legislation, as opposed to a judicially-issued writ, is the only feasible solution to this problem.

---

169 *Id.* at 1; *see* Benkler, *supra* note 166.

170 *See, e.g.*, Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 25–26; OLSEN ET AL., *supra* note 75, at 13–15.

171 *See, e.g.*, 28 U.S.C. § 1651(a) (2012) ("The Supreme Court and all courts . . . *may* issue all writs . . . ." (emphasis added)); Morrow v. District of Columbia, 417 F.2d 728, 736 (D.C. Cir. 1969); Paramount Film Distrib. Corp. v. Civic Ctr. Theatre, Inc., 333 F.2d 358, 360 (10th Cir. 1964).

172 *See, e.g.*, 18 U.S.C. § 2703(f)(1) (2012) (requiring providers "of wire or electronic communication services" to assist law enforcement by preserving specified evidence); 47 U.S.C. § 1007(a) (2012) (providing authority for court-issued orders to communications carriers requiring carriers to assist law enforcement).

173 Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 881 (2004).

174 On February 29, 2016, Senator Mark Warner introduced in the Senate a bipartisan bill to establish in the legislative branch the National Commission on Security and Technology Challenges. The purpose of the Commission is:

> To bring together leading experts and practitioners from the technology sector, cryptography, law enforcement, intelligence, the privacy and civil liberties community . . . and the national security community to examine the intersection of security and digital security and communications technology . . . and determine the implications for national security, public safety, data security, privacy, innovation, and American competitiveness in the global marketplace.

Digital Security Commission Act of 2016, S. 2604, 114th Cong. § 3(b)(1) (2016).

175 *See* Kerr, *supra* note 173, at 875 (footnote omitted).

B. The Manhattan District Attorney's Office's White Report

In November 2015, the Manhattan District Attorney's Office released a report calling for a legislative solution to full-disk encryption on smartphones.[176] The report called for state and federal legislation that would require "that any smartphone manufactured, leased, or sold in the U.S. must be able to be unlocked" pursuant to a lawful search warrant and unlock order.[177]

Critics argue that the proposed legislation takes an "absolutist" approach and, as such, does not adequately take into consideration Apple and Google's interests.[178] But what if full-disk encryption is not as "impossible" to crack as the government asserts? What if it does not frustrate as many investigations and prosecutions as previously suggested? Regardless, under the proposed legislation, Apple and Google will still have to produce smartphones with "weakened" encryption.[179] As discussed above, the government has already successfully unlocked an iPhone 5c running iOS 9 with the assistance of a third party hacker,[180] and Zerodium, a firm that sells security vulnerabilities to the U.S. government and private corporations, reported that a team of hackers had successfully exploited a flaw in iOS 9.[181] Apple and Google do have an interest in the quality of their products and their company brands. These brands are, in fact, built on privacy and security.[182] It may negatively impact the companies' brands if the public perceives the companies as "weakening" security and assisting the government to extract "private" data.[183] This is a distinct possibility given that both companies (particularly Apple) have heavily marketed their opposition to any government-imposed changes in their mobile operating systems.[184]

---

176 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 13.

177 *Id.*

178 Benner & Perlroth, *supra* note 8.

179 *See id.*

180 *See* Benner & Lichtblau, *supra* note 3.

181 *See* Perlroth & Benner, *supra* note 145.

182 *See* Katie Benner & Paul Mozur, *Apple Sees Value in Its Stand to Protect Security*, N.Y. TIMES (Feb. 20, 2016), http://www.nytimes.com/2016/02/21/technology/apple-sees-value-in-privacy-vow.html.

183 *Cf.* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html (discussing the loss to American tech companies in foreign markets after Snowden's revelations).

184 *See, e.g.*, Benner & Mozur, *supra* note 182; Benner & Perlroth, *supra* note 8; Customer Letter, *supra* note 8.

The proposal could also be seen as deputizing private corporations without providing just compensation. This is because the proposed legislation does not contemplate a reimbursement scheme.[185] According to Apple, it would take a team of six to ten Apple engineers and employees between two to four weeks to develop a decryptable mobile operating system.[186] The proposed legislation would force Apple to bear the entire cost of development.

C. Legislative Solutions at the State Level

Currently two states—New York and California—have introduced bills that would require smartphones sold in the state to be amenable to search warrants. New York Assemblyman Matthew Titone (D-Staten Island) introduced legislation, bill A8093, that would require any smartphone manufactured, sold, or leased in New York to be "capable of being decrypted and unlocked by its manufacturer or its operating system provider."[187] Any smartphone that cannot be decrypted and unlocked will subject its seller or lessor to a $2500 fine. California Assemblyman Jim Cooper (D-Elk Grove) introduced legislation, bill AB 1681,[188] that would subject a manufacturer or operating system provider to "a civil penalty of $2500 for each instance in which the smartphone is unable to be decrypted," if decryption is ordered by a state court.[189] Neither bill proposes a compensation scheme to reimburse companies for the costs of reengineering smartphones to be amenable to search warrants and unlocking them pursuant to a court order.[190] Additionally, neither bill states what the funds from the civil penalty will be used for.[191]

---

185 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 13.

186 *See* Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 13.

187 A8093A, 2016 Leg., 239th Sess. (N.Y. 2016). Assemblyman Titone introduced the bill on June 8, 2015, *see id.*, and it was referred to committee in January 2016 following publicity around DA Vance's white report. *See* Tom Risen, *New York Bill Aims to Ban Encrypted Phones*, U.S. NEWS (Jan. 15, 2016, 5:46 PM), http://www.usnews.com/news/articles/2016-01-15/new-york-bill-aims-to-ban-encrypted-phones.

188 AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016). Assemblyman Copper introduced the bill on January 20, 2016, and the bill was amended in assembly on March 28, 2016, after this Note had been substantially drafted. *See id.* The bill as first introduced was nearly identical to the pending New York bill, however, the stated rationale was to fight human trafficking rather than terrorism. *See* Cyrus Farivar, *Yet Another Bill Seeks to Weaken Encryption-by-Default on Smartphones*, ARS TECHNICA (Jan. 21, 2016, 5:00 AM), http://arstechnica.com/tech-policy/2016/01/yet-another-bill-seeks-to-weaken-encryption-by-default-on-smartphones/; *see also* N.Y. A8093A § 1.

189 Cal. AB-1681.

190 *See* Cal. AB-1681; N.Y. A8093A.

191 *See* Cal. AB-1681; N.Y. A8093A.

Opponents criticize New York and California's pending bills in part because they are state legislation.[192] If the New York and California bills passed, a tech company (like Apple or Google) that sells encrypted-by-default smartphones would have four options. One, a tech company could stop including full-disk encryption on its smartphones. For companies like Apple and Google, this would contradict almost two years of outspoken statements on encryption technology and its corresponding privacy and security benefits.[193] Indeed, Apple has a built a "global marketing strategy" around privacy and security (particularly against government intrusion).[194] Two, a tech company could cease selling smartphones in two of the richest states in the United States.[195] It would be ironic if California-based Apple and Google could not sell smartphones in the Silicon Valley state. Three, a tech company could create decryptable smartphones for those states to abide by their anti-encryption laws. This third option would most likely result in New York or California residents purchasing full-disk encrypted smartphones from neighboring states.[196] Differences in products across states create incentives for secondary market sales.[197] Additionally, the California bill only imposes a fine for each instance that a smartphone cannot be decrypted pursuant to a "state court order."[198] The bill would do nothing to further federal investigations and prosecutions in the state. Thus, the state legislation ultimately would not further law enforcement investigations because criminals and future victims could still obtain a full-disk encrypted smartphone with a quick trip across the state border. Moreover, the pending bills would

192 *See* Brian Barrett, *New Bill Aims to Stop State-Level Decryption Before It Starts*, WIRED (Feb. 10, 2016, 3:27 PM), http://www.wired.com/2016/02/encrypt-act-2016/.

193 *See* Benner & Perlroth, *supra* note 8; Customer Letter, *supra* note 8.

194 Apuzzo & Benner, *supra* note 15; *see also* Benner & Mozur, *supra* note 182.

195 *See* U.S. CENSUS BUREAU, MEDIAN HOUSEHOLD INCOME (IN 2013 INFLATION-ADJUSTED DOLLARS) BY STATE RANKED FROM HIGHEST TO LOWEST USING 3-YEAR AVERAGE: 2011-2013; Megan Willett, *The Wealthiest People in America Live in These States*, BUS. INSIDER (Mar. 24, 2015, 2:05 PM), http://www.businessinsider.com/us-states-with-the-wealthiest-residents-2015-3.

196 *See* Barrett, *supra* note 192.

197 For example, immediately after New York City and State cigarette tax increased in April 2002, there was a "'flood' of cigarette smuggling into NYC and a rise in illegal sales of untaxed cigarettes." Donna Shelley et al., *The $5 Man: The Underground Economic Response to a Large Cigarette Tax Increase in New York City*, 97 AM. J. PUB. HEALTH 1483, 1483 (2007). A New York City Department of Health and Mental Hygiene's Community Health Survey reported that eighty-nine percent of cigarettes in New York City were purchased through alternative sales channels (i.e., not through New York City retailers). *Id.*

198 AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016).

negatively impact the economy in those states by driving away business from New York and California smartphone retailers.[199]

And finally, four, in regard to the California bill, tech companies would likely continue to sell encrypted smartphones in the state. The state legislation would not have "the clout to affect multinational corporations like Apple and Google."[200] Over the course of one year, the Manhattan District Attorney's Office reported that it had 175 smartphones that it could not decrypt.[201] Covering a population of approximately 1.644 million,[202] that is roughly one inaccessible smartphone per every 9394 individuals. Presuming that this ratio is constant, there will be approximately 4167 smartphones that California law enforcement cannot decrypt every year.[203] This would result in the imposition of a $10.417 million civil penalty each year to be shared amongst the manufacturers and mobile operating system providers of those inaccessible smartphones. However, this penalty would be unlikely to compel tech companies to reengineer their smartphones to be decryptable pursuant to a court order. In just the third quarter of fiscal year 2015, Apple had a quarterly net profit of $10.7 billion,[204] while Google had a quarterly net profit of $3.979 billion.[205] Even if each respective company were to pay the entire estimated yearly penalty, it would only constitute 0.097% of Apple's quarterly net profit and 0.261% of Google's.[206] Moreover, the civil penalty would likely not be shouldered by one company (or even two). The California bill fines the "manufacturer or operating system provider,"[207] and there are presently at least ten distinct companies that manufacture

199 *See* Barrett, *supra* note 192.

200 Ellen Nakashima, *Officials Seizing the Moment of Paris Attacks to Rekindle Encryption Debate*, WASH. POST (Nov. 18, 2015), https://www.washingtonpost.com/world/national-security/officials-seizing-the-moment-of-paris-attacks-to-rekindle-encryption-debate/2015/11/18/cdb89400-8d5c-11e5-acff-673ae92ddd2b_story.html.

201 *See* Benner & Apuzzo, *supra* note 64.

202 This information is current as of July 1, 2015. U.S. CENSUS BUREAU, QUICKFACTS: NEW YORK COUNTY (MANHATTAN BOROUGH), NEW YORK, http://www.census.gov/quickfacts/table/PST045215/36061,36 [https://perma.cc/GE79-ZFRE] (last visited Feb. 6, 2017).

203 As of July 1, 2015, California has a population of approximately 39,144,818. U.S. CENSUS BUREAU, QUICKFACTS: CALIFORNIA, http://www.census.gov/quickfacts/table/PST045215/06,00 [https://perma.cc/PSQ3-W7SZ] (last visited Feb. 6, 2017).

204 Press Release, *Apple Reports Third Quarter Results*, APPLE (July 21, 2015), http://www.apple.com/pr/library/2015/07/21Apple-Reports-Record-Third-Quarter-Results.html?sr=hotnews.rss [https://perma.cc/H77Z-Z3LK].

205 Jared Dipane, *Google Announces Q3 2015 Results: $18.7 Billion in Revenue, $3.97 Billion Net Income*, ANDROID CENTRAL (Oct. 22, 2015, 4:19 PM), http://www.androidcentral.com/google-announces-q3-2015-results-187-billion-revenue-397-billion-net-income.

206 *See supra* notes 203–05 and accompanying text.

207 AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016).

smartphones or engineer mobile operating systems in the United States.[208] In sum, this solitary bill would not motivate companies to reengineer their encryption technology; the bill's effectiveness depends on other states adopting congruent legislation. Because there are no other pending state bills similar to California's, the absence of extrajurisdictional penalties diminishes the proposed scheme's effectiveness.

Critics of the pending bills argue that state legislation concerning smartphone encryption would be illegal under the Dormant Commerce Clause.[209] The Dormant Commerce Clause is a constitutional doctrine that forbids states from enacting legislation that imposes undue burdens on interstate commerce.[210] Opponents argue that the pending bills would place undue burdens on interstate commerce for many of the reasons discussed above (e.g., forcing companies to create substantially different mobile operating systems for each state).[211]

On February 11, 2016, due to concerns associated with the impracticality of state-by-state encryption laws, a bipartisan group of legislators in the U.S. Congress introduced the ENCRYPT Act of 2016. The Act would prevent states and localities from passing laws banning encryption on smartphones sold in the United States.[212] The Act is specifically aimed at the pending legislation in New York and California.[213]

Additionally, nothing in the New York bill prevents Apple and Google from making the fully encryption-enabled version of its mobile operating system available to anyone who, after purchasing the smartphone, can get the encryption technology through a software update. Under the pending bill, the seller or lessor is only subject to the $2500 civil penalty if the retailer knew "at the time of the sale or lease that the smartphone was not capable of being decrypted and unlocked

208 *See* Victor H., *Top 10 Smartphone Makers in Q1 2015: Sony and Microsoft Drop Out of the Picture, Chinese Phone Makers Take Over*, PHONE ARENA (May 25, 2015, 4:46 AM), http://www.phonearena.com/news/Top-10-smartphone-makers-in-Q1-2015-Sony-and-Microsoft-drop-out-of-the-picture-Chinese-phone-makers-take-over_id69643.

209 *See* Farivar, *supra* note 188.

210 The Dormant Commerce Clause is inferred from the Commerce Clause in Article I of the United States Constitution. *See, e.g.*, McBurney v. Young, 133 S. Ct. 1709, 1719 (2013); United States v. Lopez, 514 U.S. 549, 579 (1995). The Commerce Clause expressly grants Congress the power to regulate commerce "among the several states." U.S. CONST. art. I, § 8, cl. 3. This grant of power implies a negative converse.

211 *See* Barrett, *supra* note 192.

212 Ensuring National Constitutional Rights for Your Private Telecommunications Act of 2016, H.R. 4528, 114th Cong. § 2 (2016).

213 *See id.*

by its manufacturer or its operating system provider."[214] Thus, criminals and future victims could frustrate New York investigations and prosecutions with a trivial software update.

Further, the New York bill exclusively punishes retailers.[215] Manufacturers and mobile operating system providers are not subject to any civil penalty.[216] It is inherently unfair to punish the retailer for an encryption technology that it had no hand in creating.[217] The New York bill works indirectly to achieve its goal: it imposes a civil penalty on retailers to discourage the sale of full-disk encrypted smartphones in order to ultimately force manufacturers and mobile operating system providers to reengineer their products.

The California bill is silent on how the government would determine whether to fine the "manufacturer or [the] operating system provider."[218] Sometimes the manufacturer and the mobile operating system provider are the same company, like for Apple's iPhones.[219] However, for the majority of smartphones running Android, the manufacturer and mobile operating system provider are two separate companies.[220] The bill's silence could easily lead to arbitrary and inconsistent results. For example, the state government could fine Google for one instance of an inaccessible LG G5 (a smartphone made by LG Electronics ("LG") that runs Android) and then LG for the next five.

IV. Background on the CALEA

Having now explored various judicial and legislative solutions, this Part discusses a pertinent federal legislative Act that will form the basis of this Note's proposal.

Beginning in the 1990s, emerging digital and wireless technologies have increasingly frustrated law enforcement efforts to facilitate court-authorized surveillance.[221] In response, Congress, concerned about the efficacy of modern law enforcement, prompted the Govern-

214 A8093A, 2016 Leg., 239th Sess. (N.Y. 2016).

215 *See id.*

216 *See id.*

217 In fact, the California bill, when it was first introduced, subjected only the seller or lessor to the civil penalty. However, the state legislature explicitly amended the bill to state that the "inability of a smartphone manufacturer or its operating system provider to decrypt the contents of the smartphone . . . shall not result in liability to the seller or lessor." AB-1681, 2016 Leg., 2015–2016 Sess. (Cal. 2016).

218 *Id.*

219 *See supra* note 44 and accompanying text.

220 *See supra* note 51 and accompanying text.

221 *See* King, *supra* note 26, at 178.

ment Accountability Office to examine the growing application of digital technology in public telephone systems.[222] Their investigation found that digitalization could potentially inhibit the FBI's ability to effectively wiretap and surveil suspects.[223] Unfortunately, this concern manifested as more than just a hypothetical impediment: a 1992 FBI survey indicated that advanced telecommunications technologies prevented law enforcement from carrying out court-authorized electronic surveillance in ninety-one instances.[224] Congress felt compelled to rectify this burgeoning problem and ultimately enacted in 1994 the Communications Assistance for Law Enforcement Act.[225] This Act ensures that court-authorized surveillance investigations could survive contemporary technological advancements.[226]

A. Requirements

"The primary purpose of the CALEA is to clarify a telecommunications carrier's duty to assist law enforcement agencies with the lawful interception of communications and the acquisition of call-identifying information in an ever-changing telecommunications environment."[227] The CALEA requires that telecommunications carriers meet the assistance capability requirements in section 1002.[228] Generally, section 1002 requires that telecommunication carriers ensure their equipment, facilities, and services are capable of enabling the government, pursuant to a court order, to effectively intercept communications within the carrier's service area, to or from its equipment, concurrently with the transmission.[229] The carriers must assist law enforcement, even "to the exclusion of any other communications."[230] Telecommunications carriers must also allow law enforcement access

222 *See* U.S. Gov't Accountability Office, FBI: Advanced Communications Technologies Pose Wiretapping Challenges (July 1992).

223 *See id.* at 2 ("[S]ince 1986, the FBI has become increasingly aware of the potential loss of wiretapping capability due to the rapid deployment of new technologies, such as cellular and integrated voice and data services, and the emergence of new technologies such as Personal Communication Services, satellites, and Personal Communication Numbers.").

224 *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearing Before the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil & Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 36 (1994) (statement of Louis J. Freeh, Director, FBI).

225 Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2012).

226 *See* Implementation of the Communications Assistance for Law Enforcement Act, 60 Fed. Reg. 53643 (Oct. 16, 1995).

227 *Id.*

228 *See* 47 U.S.C. § 1002.

229 *See id.* § 1002(a)(1).

230 *Id.*

to "call-identifying information that is reasonably available to the carrier . . . before, during, or immediately after the transmission."[231]

B. Reimbursement

At the outset, the CALEA dedicated $500 million to reimburse telecommunications carriers for upgrades and modifications that were made during fiscal years 1995 through 1998.[232] The affected industries raised concerns that the $500 million would be insufficient to compensate telecommunications carriers for their start-up costs.[233] For this reason, if compliance is not reasonably achievable, and the Attorney General does not agree to reimburse, the telecommunications carrier will be deemed in compliance without having to perform the modifications required under section 1003.[234] The carrier will continue to be deemed in compliance unless it notably modifies the relevant equipment, facility, or service.[235] After the initial four-year period,[236] the government will no longer reimburse telecommunications carriers, and the affected companies will bear "reasonable costs of compliance," to be determined by the FCC.[237]

C. Enforcement

A court may impose a civil penalty against a telecommunications carrier of up to $10,000 per day for its failure to comply with the CALEA.[238] A court can impose a civil penalty only if: (1) it finds that law enforcement has no other reasonably available alternatives (such as another carrier) to implement interception; and (2) compliance with the CALEA would have been "reasonably achievable" on the

---

231 *Id.* § 1002(a)(2).

232 *Id.* § 1009. The Act provides that the Attorney General may reimburse telecommunications carriers for "all reasonable costs directly associated" with modifications to equipment, facilities, and services installed on or before January 1, 1995. *Id.* § 1008(a). The Federal Communications Commission ("FCC") determines, on petition, whether a telecommunications carrier will be compensated/receive funds for such changes after January 1, 1995. *Id.* § 1008(b)(1).

233 *See* 140 CONG. REC. H27,707 (daily ed. Oct. 4, 1994) (statement of Rep. Hyde).

234 The telecommunications carrier may petition the FCC to determine whether compliance would impose significant difficulty or expense. *See* 47 U.S.C. § 1008(b)(1). The FCC bases its decision on ten enumerated factors, including public safety and national security, and one catchall factor. *Id.* § 1008(b)(1)(A)–(K).

235 *See id.* § 1008(d).

236 The FCC may extend the transition period up to two additional years. 140 CONG. REC. H27,707 (daily ed. Oct. 4, 1994) (statement of Rep. Hyde).

237 *See id.*

238 18 U.S.C. § 2522(c)(1).

part of the offending carrier.[239] A court can mandate that the offending carrier perform the required upgrades and modifications to bring it into compliance with the CALEA, so long as the directed upgrades and modifications do not result in unreasonable costs that will not be reimbursed by the Attorney General.[240]

D. Inapplicability to Smartphone Data

Since the introduction of the first widely adopted smartphone in 2007,[241] it has been quickly noted that the CALEA does not apply to data on these smartphone devices.[242] This has sparked a "great deal of debate" about expanding the Act.[243] In 2009, the FBI voiced concerns about the CALEA's inability to reach smartphone data.[244] In the following years, the agency spoke before Congress on the "Going Dark" problem[245] and drafted amendments to the CALEA that would encompass smartphone data.[246] The Justice Department approved the draft legislation, but the White House never sent the proposed CALEA amendments to Congress.[247]

V. Congress Must Amend the CALEA to Address Full-Disk Encryption on Smartphones

As Justice Alito observed, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public

---

239 47 U.S.C. § 1007(a).

240 *See id.* § 1007(c).

241 King, *supra* note 26, at 178.

242 *Id.*

243 *Id.*; *see In re* Apple, Inc., 149 F. Supp. 3d 341, 355 (E.D.N.Y. 2016) (noting that both the government and Apple agree that the CALEA does not compel a private company, such as Apple, to help the government access an encrypted phone's data).

244 King, *supra* note 26, at 178.

245 Unfortunately, the law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. We call it "Going Dark," and what it means is this: Those charged with protecting our people are not always able to access the evidence we need to prosecute crime and prevent terrorism even with lawful authority. We have the legal authority to intercept and access communications and information pursuant to court order, but we often lack the technical ability to do so.

James Comey, Dir., Fed. Bureau of Investigation, Speech at the Brookings Institution, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) (transcript available at https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course).

246 *See* King, *supra* note 26, at 178.

247 *Id.* at 179.

safety in a comprehensive way."[248] By enacting legislation, "the United States could make clear that the era of 'secret cooperation' [between the government and U.S. tech companies] is over."[249]

This Note proposes an amendment to the CALEA that gives manufacturers and mobile operating system providers a choice to either make smartphones amenable to search warrants or pay a civil penalty each time a smartphone cannot be decrypted pursuant to a court order. Under the proposed amendment, manufacturers and mobile operating system providers would be liable for $127,500[250] for each instance that law enforcement cannot unlock or otherwise access the data on a smartphone it has the legal authority to search.[251] This civil penalty scheme is similar to that being considered by the California legislature in the bill described in Section IV.B.[252] However, this Note's proposed amendment effectively responds to the criticisms and failings raised by other proposals (including the pending California bill).[253]

Under this Note's proposed amendment, the law enforcement agency must obtain a search warrant and unlock order from the court with proper jurisdiction. In order for the court to issue an unlock order, it must first find that the moving law enforcement agency exhausted its technological capabilities. This will help safeguard against a deputization of Apple and Google as the IT department of the state and U.S. governments,[254] and prevent (quite literally) unwarranted intrusions into citizens' privacy.

---

248 United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment) (citation omitted); *see, e.g.*, Kerr, *supra* note 173.

249 Reema Shah, Comment, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L.J. 543, 558 (2015).

250 This number constitutes the medium payment made to hackers by the U.S. government. *See* Jayesh Limaye, *$250,000 Paid To Reveal iOS Exploit*, TECHTREE (July 3, 2012, 8:51 PM), http://www.techtree.com/content/news/879/250000-paid-to-reveal-ios-exploit.html. However, this number serves more as a placeholder and is by no means the exact number that should be adopted. This Note argues that open debate in Congress would lead to the optimal civil penalty. *See supra* notes 173–75 and accompanying text.

251 In cases where the same company is both the manufacturer and the mobile operating system provider, the company will have to pay a total of $255,000. There are two distinct wrongs given the two different capacities that the manufacturer and mobile operating system provider serve.

252 *See* AB-1681, 2016 Leg., 2015–2016 Sess. § 2(b) (Cal. 2016) ("A manufacturer or operating system provider of a smartphone sold or leased in California on or after January 1, 2017, shall be subject to a civil penalty . . . for each instance in which the manufacturer or operating system provider of the smartphone is unable to decrypt the contents of the smartphone pursuant to a state court order.").

253 *See supra* Part IV.

254 *See supra* notes 184–86 and accompanying text.

Companies that make their smartphones amenable to search warrants (by either giving law enforcement a method to access the data or accessing the data for law enforcement) will avoid civil penalties and be reimbursed for the costs of their compliance with the proposed statutory scheme. Similar to CALEA sections 1008 and 1009, the amendment authorizes $500 million[255] to reimburse manufacturers and operating system providers for the costs associated with reengineering their smartphones.[256] The funds will be available until exhausted or four fiscal years have passed since the amendment's enactment.[257] To quell potential concerns about insufficient compensation, the amendment contains a provision similar to section 1008(b)(1) and (d) of the CALEA: if a manufacturer or mobile operating system provider cannot "reasonably achieve" compliance, and the Attorney General does not agree to reimburse, the company will be deemed compliant and thus exempt from the civil penalty.[258] After the initial four-year period, the government will no longer reimburse manufacturers and mobile operating system providers, and the affected companies will bear "reasonable costs of compliance."[259] This part of the reimbursement scheme is limited to four years in order to encourage companies to immediately make smartphones amenable to search warrants. Additionally, under the proposed amendment, the government will compensate the manufacturer or mobile operating system provider for each smartphone that needs to be unlocked using a proprietary method that only the company possesses. Reimbursement for data extractions of specific smartphones will continue indefinitely.

Under this Note's proposed legislation, manufacturers and mobile operating system providers do not have to make smartphones amenable to search warrants. If a company elected not to make its smartphones amendable to a search warrant, investigators could bring a civil suit against it. For federal investigations and prosecutions, a U.S. Attorney may bring civil suit in federal court for any inaccessible, legally searchable smartphone in his district. Similarly, for state investigations and prosecutions, the Attorney General of that state or the

255 This is the same amount that the CALEA allotted to reimburse telecommunications carriers. *See* 47 U.S.C. § 1009 (2012). However, this Note recognizes that open debate is necessary to achieve the correct reimbursement amount to be set aside for manufacturers and mobile operating system providers wanting to make their products amenable to search warrants. *See supra* notes 173–75 and accompanying text.

256 *See supra* note 232 and accompanying text.

257 *See supra* note 236 and accompanying text.

258 *See supra* notes 234–37 and accompanying text.

259 *See supra* notes 236–37 and accompanying text.

District Attorney of that jurisdiction may bring civil suit in federal court for any inaccessible, legally searchable smartphone. The court would then have the ability to impose the $127,500 civil penalty only if law enforcement has no "reasonable alternative" to access the phone's data. A reasonable alternative is limited to one of the following: (1) the user consents; (2) law enforcement obtains a court order requiring the user to unlock his smartphone or provide its contents; or (3) law enforcement has in its possession the technological capability to safely unlock the smartphone at issue. Regarding the third reasonable alternative, law enforcement must actually possess the technology—the fact that law enforcement can pay a third-party hacker will not exempt the companies from the civil penalty. The amendment will prohibit the manufacturer and mobile operating system provider from passing on any portion of the costs associated with compliance or the civil penalty.

Rather than go into the state or U.S. Treasury (as most civil penalties do),[260] the civil penalties here will be paid directly to the respective state or federal investigative agency that obtained the search warrant and unlock order. With the money going to these agencies, the fine will more directly further investigative and prosecutorial efforts. The civil penalties can be used to create specialized investigative teams, training programs to respond to changing technology, or to recoup the costs of paying a third-party hacker. For example, state governments and the DOJ could create both entry-level and advanced onsite training courses for law enforcement that are aimed at improving the investigation of electronic crimes and the collecting and examining of technology-based evidence.[261] Jurisdictions can partner with the private high-tech industry to develop a joint task force or can create an onsite high-tech task force that is trained to investigate electronic crimes and examine technology-based evidence.

This Note's proposed amendment puts the decision in the hands of the affected private companies. The statute imposes a civil penalty to force tech companies to engage in a more balanced weighing of the

260 Kathleen Pender, *When Government Fines Companies, Who Gets Cash?*, SFGATE (May 6, 2010, 4:00 AM), http://www.sfgate.com/business/networth/article/When-government-fines-companies-who-gets-cash-3189724.php.

261 The FBI "lost a chance to capture data" from the iPhone in the San Bernardino case when FBI personnel mistakenly believed that resetting the iCloud passcode would grant access to the data on the iPhone. Kang & Lichtblau, *supra* note 4. Instead, "the change had the opposite effect—locking [the FBI] out and eliminating other means of getting in." *Id.* Perhaps this mistake (and subsequent litigation) could have been avoided if federal investigative agencies had specialized training programs focused exclusively on investigating and using technology.

costs and benefits. Companies currently have no incentive to make smartphones amenable to search warrants. As mentioned, Apple and Google publicly advocated against altering current full-disk encryption technology on their mobile operating systems.[262] They have created a brand based on privacy and security, particularly against government intrusion.[263]

This Note's proposed amendment takes a balanced approach to remedying the encryption problem. The civil penalty is attached to only those smartphones that the government has the legal authority to search but cannot decrypt. The civil penalty should be substantial enough to "highly encourage" manufacturers and mobile operating system providers to elect to make their smartphones amenable to search warrants; however, the penalty should not be so substantial as to unequivocally prevent companies from selling full-disk encrypted smartphones.

The amendment can adapt to the nebulous intersection of tech and law enforcement; for example, the government may only infrequently encounter inaccessible smartphones. If this highly unlikely supposition becomes a reality,[264] then forcing private companies to reengineer their mobile operating systems for every smartphone sold in the United States would be an excessive response. If most defendants voluntarily disclose their passcodes or are made to provide their smartphone's data or physically unlock it using their passcode or fingerprint, then there is no harm to law enforcement investigations and thus no civil penalty imposed on tech companies. If law enforcement possesses the technology, then companies will not have to pay the civil penalty.[265] This Note's proposed amendment limits the imposition of a civil penalty (or private companies' assistance) to those few cases that are truly detrimental to the public interest. The investigative agency will receive $127,500 to offset the costs of paying a hacker or pursue other investigatory avenues in cases where the smartphone is indisputably inaccessible.

---

262 *See, e.g.*, Brief for Amazon.com et al. as Amici Curiae, *supra* note 152; Benner & Perlroth, *supra* note 8; Customer Letter, *supra* note 8.

263 *See supra* notes 182–84 and accompanying text.

264 *See supra* Part II.

265 For instance, the FBI currently has the technology to unlock some iPhones running iOS 9 and older versions. *See* Benner & Lichtblau, *supra* note 3. An anonymous third-party hacker gave the FBI a previously unknown tool that could access the data on at least one iPhone, *see id.*, which may potentially be used to unlock others, *see* McCallister, *supra* note 21.

On the other hand, if—as current evidence suggests[266]—smartphone encryption is consistently an impediment to law enforcement investigations, then companies will be persuaded by the frequently-imposed civil penalty to make smartphones amenable to search warrants.

VI. Responses to Counterarguments

This Part addresses and refutes the three biggest counterarguments to this Note's proposal. These three arguments include: (A) that making smartphones amenable to search warrants would weaken the phone's security; (B) that the technology industry would be overly financially burdened; and (C) that authoritarian governments would be able to harm their citizens through this technology.

A. Any Loss in Personal Security and Privacy Would Be Insignificant

Opponents argue that any effort to make smartphones amenable to search warrants would necessarily weaken the smartphone's security and "thus increase the possibility of a bad actor unlawfully accessing device data."[267] However, any loss in personal security and privacy would be insignificant for at least four reasons.

First, the high-profile security breaches that fueled a nationwide desire for heightened data security and privacy did not involve data at rest[268] on smartphones.[269] Many opponents conflate the concerns regarding compromised end-to-end encryption (data in transit) with full-disk encryption (data at rest).[270] End-to-end encryption involves encryption at the end points of live data transfers or communication

266 *See supra* Part II.

267 Manhattan Dist. Attorney's Office, *supra* note 71, at 14; *see, e.g.*, Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 7; Olsen et al., *supra* note 75, at 1; *Answers to Your Questions About Apple and Security*, Apple, http://www.apple.com/customer-letter/answers/ [https://perma.cc/L2PZ-48FL] (last visited Feb. 6, 2017); Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernardino Attacks*, Wash. Post (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html.

268 Data at rest (also known as device encryption), "in which the keys exist only on locked devices[,] prevents the contents from being read by anyone who does not possess the keys." Olsen et al., *supra* note 75, at 4.

269 *See* Julia Angwin et al., *AT&T Helped U.S. Spy on Internet on a Vast Scale*, N.Y. Times (Aug. 15, 2015), http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html (discussing the NSA wire-tapping event); Blistein, *supra* note 89 (discussing the hacker who leaked the personal contents of information stored in celebrities' cloud accounts).

270 *See* Olsen et al., *supra* note 75, at 4; Brad Reed, *The FBI Has Laid a Clever Trap for*

channels, and "only the original sender and intended recipient possess the keys necessary to decrypt the message."[271] Thus, "the information is (in theory, and as advertised) not capable of being read by anyone who sees it traverse a network between the sender and the receiver, including an intermediary service provider, such as Apple."[272] The ability of law enforcement to "decrypt data in transit presents unique risks that are simply not presented by the ability to decrypt data at rest."[273] Notably, "the ability to decrypt data in transit creates the possibility of unlawful eavesdropping on live communications; such eavesdropping is not at issue in connection with data at rest."[274] At least in regard to Apple, the company's passcode-bypass process cannot be used remotely.[275] Even if a maligned hacker were to learn Apple's decryption process, he would still need the physical iPhone to be able to decrypt and access its data.[276]

Second, an individual's privacy still receives the protection of the Fourth Amendment. In *Riley v. California*,[277] the Supreme Court held that the Fourth Amendment requires warrants for searches of smartphone data.[278] A judge may only issue a search warrant for a smartphone if there is probable cause to believe that it contains evidence or proceeds of a crime.[279] The *Riley* Court acknowledged that cellphones keep "a digital record of nearly every aspect of their lives—from the mundane to the intimate"; however, it ultimately held that the Fourth Amendment and its search warrant requirement are sufficient privacy safeguards.[280] Indeed, Apple and Google seek to unilaterally alter Supreme Court jurisprudence that affords the home the highest level of privacy protection.[281] If "[e]very home can be en-

---

Apple, BGR (Feb. 17, 2016, 4:24 PM), http://bgr.com/2016/02/17/fbi-vs-apple-smartphone-encryption/.

271 OLSEN ET AL., *supra* note 75, at 4.

272 *Id.*

273 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 14.

274 *Id.*

275 *Id.*; *see* Customer Letter, *supra* note 8 ("[T]his software . . . would have the potential to unlock any iPhone in someone's *physical possession*." (emphasis added)).

276 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 14.

277 134 S. Ct. 2473 (2014).

278 *Id.* at 2485.

279 U.S. CONST. amend. IV.

280 *Riley*, 134 S. Ct. at 2490, 2493.

281 *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) ("But when it comes to the Fourth Amendment, the home is first among equals. At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

tered with a search warrant," then "[t]he same should be true of [smartphone] devices."[282]

Third, smartphones have additional security features (beyond encryption) to protect one's data if a user's smartphone were to be stolen. For example, if the user had previously enabled the Find My iPhone App or a certain setting in Android Device Manager, he could remotely wipe the smartphone's data.[283]

Fourth, the privacy and security argument advanced by opponents presumes and depends on the encryption technology being absolutely uncrackable. Critics claim that the tool or software the government asked Apple to build in the San Bernardino case—and presumably the same tool or software that the government eventually got from a third-party hacker—would "[o]nce created . . . be used over and over again, on any number of devices" and thus "expose [Apple's and Google's] customers to a greater risk of attack."[284] Opponents argue that the mere existence of such a decryption tool or software—whether it be held by the mobile operating system provider itself or the government—would invariably "get out" to bad actors.[285] But this argument assumes that such a tool is impossible to create and that Apple's and Google's security is otherwise impenetrable. As mentioned, the government currently has access to an unknown tool or software created by a third-party hacker that can at least access iPhones running iOS 9.[286] And other hackers have been able to "crack" the supposedly inaccessible iOS software.[287] Under this Note's proposed legislation,[288] Apple and Google could save themselves from the imposition of a fine (along with saving the government time in time-sensitive investigations) by constructing the decryption tool or software themselves before the government has to enlist a third-party hacker. Additionally, Apple and Google—companies which have both stated that customer privacy security is important to them[289]—would be able to control the creation and distribution of the tool or software,

---

282 *See* MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 15.

283 *See* APPLE, IOS SECURITY, IOS 9.0 OR LATER, *supra* note 129, at 55; *Remotely Ring, Lock, or Erase a Lost Device*, GOOGLE, https://support.google.com/accounts/answer/6160500 [https://perma.cc/MCV3-ZLNX] (last visited Feb. 6, 2017).

284 Customer Letter, *supra* note 8.

285 *See, e.g.*, Brief for Amazon.com et al. as Amici Curiae, *supra* note 152, at 20; Customer Letter, *supra* note 8.

286 *See* Benner & Lichtblau, *supra* note 3.

287 *See* Perlroth & Benner, *supra* note 145.

288 *See supra* Part V.

289 *See* Brief for Amazon.com et al. as Amici Curiae, *supra* note 152, at 13–14; Customer Letter, *supra* note 8.

rather than have the government outsource decryption to an unknown, third-party hacker.

Endeavoring to create an entirely impenetrable smartphone is against Apple's and Google's business interests. Additional or enhanced security features often make the smartphone "slower" or "clunkier," while companies want to sell and market smartphones that are "sleek" and "intuitive."[290] Further, companies want to sell products to the public at-large and a security feature that frustrates consumers is unworkable.[291] Apple's and Google's full-disk encryption technology is thus more burden than benefit; it only provides, at best, minimal enhanced data protection at the expense of severely weakening Americans' safety from criminal enterprise.

Additionally, under this Note's proposed legislation, the affected companies themselves will ultimately decide whether or not to make smartphones amenable to search warrants.[292] The companies could choose not to reengineer their smartphones to make them amenable to governmental search warrants—completely negating any security or privacy concerns.[293]

B. The Burden Imposed on Technology Companies Would Be Minimal

Opponents contend that legislation requiring companies to make their smartphones amenable to search warrants would impose an undue burden.[294] Manufacturers and mobile operating system providers would have to expend resources reengineering their smartphones to allow for backdoor access as well as unlocking such phones in response to search warrants.[295] Yet, this argument, in part, presumes that tech companies are, and should be, free from any government-imposed burdens designed to advance societal interests. Countless industries in the United States have to expend resources to comply with laws and regulations issued to remedy a societal problem.[296] The tech industry should be no exception.

---

290 Apuzzo & Benner, *supra* note 15.

291 *See id.*

292 *See supra* Part V.

293 *See supra* Part V.

294 *See* Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 23–24; Brief for Amazon.com et al. as Amici Curiae, *supra* note 152, at 15–18.

295 *See* Apple Inc.'s Motion to Vacate Order, *supra* note 151, at 13–14; Apuzzo & Benner, *supra* note 15.

296 *See* Mitchell Holt, *Five Areas of Government Regulation of Business*, HOUSTON CHRON.: SMALL BUS., http://smallbusiness.chron.com/five-areas-government-regulation-business-701.html

The real downfall of this argument is, however, that it completely ignores the possibility that legislation would contain a reimbursement provision. This Note proposes a reimbursement scheme that would compensate companies for the initial start-up costs of compliance and for costs associated with unlocking or extracting data from smartphones in response to a search warrant.[297] Although, admittedly, this proposal may not reimburse companies fully, as stated, companies are expected to bear reasonable costs of compliance with laws and regulations enacted for the public interest.[298]

Apple and Google regularly reengineer their mobile operating systems. Apple released iOS 9 on September 16, 2015.[299] In the six and a half months following its release, there were numerous updates (e.g., iOS 9.0.1, iOS 9.0.2, iOS 9.1, iOS 9.2, iOS 9.2.1, iOS 9.3, iOS 9.3.1).[300] Android released its newest operating system (Nougat 7.0) in October 2016, and its first major update in December of that same year.[301] The constant development of new and updated mobile operating systems belies the notion that this Note's proposal would be overly burdensome. The amendment would not be prompting entirely new development; it would simply be inserting a requirement into a process the companies already undertake.

Additionally, this Note's proposal is not forcing companies to invent novel technology. Apple and Google have the capability to either unlock or extract data from locked iPhones and Android-powered smartphones running "older" mobile operating systems.[302] Furthermore, the proposed amendment also does not require companies to

(last visited Feb. 6, 2017) (listing privacy and safety and health as two areas where the U.S. government has "many business regulations in place").

297 *See supra* Part V.

298 *See supra* Part V.

299 Press Release, *iOS 9 Available as a Free Update for iPhone, iPad & iPod Touch Users September 16*, APPLE (Sept. 9, 2015).

300 *See* Gordon Kelly, *Apple iOS 9.3.1: Should You Upgrade?*, FORBES (Apr. 1, 2016, 10:40 AM), http://www.forbes.com/sites/gordonkelly/2016/04/01/apple-ios-9-3-1-should-you-upgrade/#2bf38d51facf.

301 *See* Matt Swider & James Peckham, *Android Nougat Release Date: When You'll Get It and Everything You Need to Know*, TECHRADAR (Jan. 19, 2017), http://www.techradar.com/news/phone-and-communications/mobile-phones/android-7-what-we-want-to-see-1311290.

302 *See* Declan McCullagh, *How Apple and Google Help Police Bypass iPhone, Android Lock Screens*, CNET (Apr. 2, 2012, 5:19 PM), https://www.cnet.com/news/how-apple-and-google-help-police-bypass-iphone-android-lock-screens/ ("Apple has for at least three years helped police to bypass the lock code, typically four digits long, on iPhones seized during criminal investigations."); *Legal Process Guidelines*, *supra* note 47 (providing that Apple will no longer perform data extractions on devices running iOS 8.0 or later versions).

make any changes to their mobile operating systems.[303] They could elect to pay the civil penalty instead.[304]

C. *Individuals Living Under Authoritarian Governments Would Not Be Harmed*

Opponents argue that any effort to legislate a government backdoor into encrypted smartphones would create a precedent for authoritarian governments demanding similar access.[305] The argument continues that if an authoritarian government exercised that right, dissidents and human rights advocates in the repressive country would be injured because the "repressive government would seek access to smartphones to spy on, prosecute, and otherwise oppress the dissidents and human rights advocates."[306] These fears, however, are unfounded.

Again, as stated, mass surveillance by an authoritarian government would prove difficult—if not impossible—as the government must have the physical smartphone to access its contents.[307] Additionally, a foreign nation's government wanting information from an American company would have to go through lawful process in the U.S., either pursuant to a Mutual Legal Assistance Treaty ("MLAT") or a letter rogatory.[308] If the foreign government used the MLAT process, the executive branch of the federal government would decide whether, in its discretion, the foreign government's request was proper. If the foreign government used a letter rogatory, a federal court would make that determination. In either case, the request could be refused if the information was sought for use in a proceeding that would violate human rights.[309] "At a minimum, the Constitution requires that a request not be honored if the sought-after information would be used in a foreign judicial proceeding that 'depart[s] from our concepts of fundamental due process and fairness.'"[310]

Additionally, Apple and Google could choose to not do business in, or only sell full-disk encrypted smartphones in, countries that have

303 *See supra* Part V.

304 *See supra* Part V.

305 S*ee, e.g.*, OLSEN ET AL., *supra* note 75, at 9; Bruce Schneier, *Security or Surveillance?*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARV. U. app. A.1–2 (2016); Apuzzo & Benner, *supra* note 15; Benner & Mozur, *supra* note 182.

306 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 18.

307 *See supra* notes 275–76 and accompanying text.

308 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 19.

309 *Id.*

310 *In re* 840 140th Ave. NE, 634 F.3d 557, 572 (9th Cir. 2011) (quoting *In re* Request for Judicial Assistance from Seoul Dist. Criminal Court, 555 F.2d 720, 724 (9th Cir. 1977)).

repressive governments and no laws banning such encryption technology.[311]

Conclusion

Investigating and prosecuting in the twenty-first century requires that the government have the tools necessary to crack cases. Without crucial evidence available only on the smartphone itself, cases could go unsolved. However, any legislative remedy to full-disk encryption must balance the interests of law enforcement, tech companies, and consumers. This Note's proposed amendment to the CALEA achieves such balance by subjecting the manufacturer and mobile operating system provider to a civil penalty for each instance that law enforcement cannot decrypt a smartphone it has the legal authority to search.

311 Manhattan Dist. Attorney's Office, *supra* note 71, at 18–19.

APPENDIX

TABLE. COMPARISON OF DATA SOURCES[312]

	Device	iCloud	Google Cloud Storage	Phone Company
iMessage content	Yes	No(1)	N/A	No
iMessage detail (dates, times, phone numbers involved)	Yes	No(1)	N/A	No
SMS/MMS content	Yes	No(1)	Perhaps(2)	Perhaps(3)
SMS/MMS detail (dates, times, phone numbers involved)	Yes	No(1)	Perhaps(2)	Yes
Phone call detail (dates, times, phone numbers involved, duration)	Yes	Yes	Perhaps(2)	Yes
Historical cell site data[313]	No	No	Perhaps(2)	Perhaps(4)
Historical other cell tower-related data[314]	Perhaps(5), (6)	No	Perhaps(7)	No
Historical Wi-Fi network data	Perhaps(6)	Yes	Perhaps(7)	No
Historical GPS or other satellite data[315]	Perhaps(6)	Perhaps, some(2), (8)	Perhaps(7)	No
Contacts	Yes	Perhaps(2)	Perhaps(2)	No
Photos/Videos	Yes	Perhaps(2)	Perhaps(2)	No
Internet Search History	Yes	Perhaps(2)	Unknown	No
Internet Bookmarks	Yes	Perhaps(2)	Unknown	No
Third-Party App Data	Perhaps(6)	No	Unknown	No

312 MANHATTAN DIST. ATTORNEY'S OFFICE, *supra* note 71, at 7 (table and following information taken directly from report).

313 Cell site data, which is typically held by phone companies, is less precise than certain other types of location data because it may tell investigators only the location of a cell tower that was used to transmit a person's communication rather than the caller's location. Further, this type of data is captured only when a communication is made and not at times when a phone is not being used.

314 Certain phones capture data relating to reception of signals from cell towers, including at times when the phone is not being used to communicate. This information may include the location of towers whose signals the phone picked up as well as towers near those towers.

315 Specific types of location data include historical cell site data, historical other cell tower-related data, historical Wi-Fi network data, and historical GPS or other satellite data.

(1) Apple's website states that it can provide this information (http://images.apple.com/privacy/docs/us_le_guidelines_final_20150916.pdf, p. 8). In response to search warrants, however, Apple has not provided such information for backups of phones running iOS 8. [In Apple's September 2014 Security Guide, the company states it "does not log messages or attachments [sent through iMessage], and their contents are protected by end-to-end encryption so no one but the sender and receiver can access them."[316]]
(2) The information would be available to law enforcement only if the device user chose to back up to the cloud and included this type of data. . . .
(3) Most carriers do not retain content. Some that do, retain for only a short period (e.g., 3–5 days).
(4) This data can be obtained by law enforcement while the data is retained by the phone service provider. There is no requirement, however, that wireless carriers maintain this type of data at all or for any particular length of time. In addition, cell site data is not retained by certain phone carriers for text messages. Given than [sic] many people now primarily communicate through text messages, this limits the amount of location information investigators can learn through cell site data.
(5) May be available for only certain devices.
(6) Forensic analysts are able to extract this information from devices. When Apple provides device data pursuant to an unlock order, however, they do not include this data.
(7) May be available from Google when stored in its servers. This type of data does not appear to be stored in Google's cloud.
(8) Certain types (*e.g.*, GPS EXIF data) may be available, but not all (*e.g.*, Google Maps data).

316 iOS Security Guide, *supra* note 107, at 23.

POWER, PERVASIVENESS AND POTENTIAL: THE BRAVE NEW WORLD OF FACIAL RECOGNITION THROUGH A CRIMINAL LAW LENS (AND BEYOND)

Criminal Courts Committee
New York City Bar Association

August 2020

THE ASSOCIATION OF THE BAR OF THE CITY OF NEW YORK
42 West 44th Street, New York, NY 10036
212.382.6600 | www.nycbar.org

Power, Pervasiveness and Potential: The Brave New World of Facial Recognition Through a Criminal Law Lens (and Beyond)

The following report from the New York City Bar Association's Criminal Courts Committee provides an overview of facial recognition technology through a criminal law lens. Notably, however, the use of facial recognition technology is not limited to law enforcement: as the world becomes increasingly technology-oriented and technologically dependent, biometrics—and facial recognition in particular—has become pervasive in both the public and private sectors. This paper therefore also delves into related areas and considerations raised by the collection, storage, use and misuse of biometric information, and offers broad policy recommendations to improve facial recognition technology and protect against infringements on personal privacy, constitutional rights, and racial justice.

TABLE OF CONTENTS

I. WHAT IS BIOMETRICS AND HOW DOES IT WORK?

- Biometrics is the technical term for body measurements/calculations related to human characteristics.[1] Examples of biometrics include fingerprints, palm prints, facial recognition, DNA, retina/iris, and voice.[2]
- Although it is a technology advanced in the Digital Age, there is evidence of handprint biometrics used as early as prehistoric times as well as in 200s BCE China.[3]
- Biometrics function by comparing a piece of information to a data set to verify one's identity.[4] There are both multi and unimodal biometric systems.[5]
- Facial recognition, one form of biometrics, was pioneered in the mid-1960s.[6] It examines the image of a person's face and measures its specific facial features to find a possible match to a face within a database.[7]
- Facial recognition algorithms work in a variety of different ways: some measure the distance between facial features (eyes, jawbone, etc.), while others use 3D sensors to scan the face, and others analyze skin texture.[8] The facial recognition system then compares this information to a database of faces to find a match.[9]

II. WHO USES FACIAL RECOGNITION AND WHY?

- Generally, biometrics are unique to each individual and thus provide a more reliable identity verifier than "token" or "knowledge" based methods such as ID cards or passwords, respectively.[10] While facial recognition can be less accurate than other biometrics, such as iris or fingerprint scans, it is less invasive, which has contributed to the sharp rise in its use.[11]
- This rise is also attributable to increased law enforcement and surveillance activity in the wake of 9/11.[12]
- Use of facial recognition software has expanded vastly since this time. Some entities that use facial recognition software include:
    - Federal, state and local law enforcement (body cameras, lineups, mugshots, surveillance, etc.), including the Federal Bureau of Investigation (FBI) and U.S. Immigration and Customs Enforcement (ICE);
    - Federal government agencies at airports; the Transportation Security Administration (TSA) monitors passengers entering and exiting airports to identify persons under criminal investigation or persons who have overstayed their visas; TSA and U.S. Customs and Border Protection (CBP) are developing a biometric exit program; there are proposals to make airports 100% biometric;
    - Tech companies (i.e. Apple, Samsung, etc.) to unlock mobile devices;
    - Colleges and universities (to take roll in the classroom, combat cheating, and gain entry to sporting events);
    - Social media companies (i.e. Facebook can identify a photo automatically upon upload);

- Video games (Xbox, Nintendo, etc.);
- Healthcare (i.e. iris scans to identify a non-verbal patient);
- Landlords (to monitor tenants in buildings);
- Music and sports venues (in lieu of scanning tickets);
- Schools and summer camps (to provide security);
- Businesses (to monitor/restrict entrance to certain areas and combat wage theft);
- Retail operations (to identify persons suspected of theft);
- Religious institutions (to take congregation roll and target donation requests);
- Airlines (i.e. faces are scanned in lieu of boarding passes); and
- Marketers and advertisers (i.e. may be used to identify and target certain demographics at concerts, etc.).[13]

- Facial recognition (and other biometrics) are also used in some counties for voter registration.[14]

III. CONCERNS THROUGH A CRIMINAL LAW LENS

- While facial recognition is more secure than token and knowledge-based security systems and has also been employed for positive purposes (including helping law enforcement locate child sex trafficking victims), its use presents a unique host of legal and ethical concerns.[15]
- Facial recognition is unique from other forms of biometric surveillance in the following ways: it tracks something that is difficult to hide and easy to observe in the open (i.e. one's face), there already exist vast name and face databases of law-abiding citizens (i.e. driver's license records) from which to draw datasets, and facial recognition surveillance can be set up using pre-existing camera networks.[16] These factors help to augment the concerns listed below.[17]

A. Fourth Amendment Search and Seizure Issues

- While the Supreme Court has ruled that we have no reasonable expectation of privacy with regard to our outward personal characteristics (i.e. our face, voice, etc.) – and thus a lineup is not a "search" with respect to the Fourth Amendment – it has also held that a police "seizure" of a person for the purpose of subjecting that person to an identification procedure does implicate the Fourth Amendment. [18]
- Biometric "virtual lineups" used by law enforcement agencies across the United States—ever-present, latent identifications of persons not in custody for which reasonable suspicion of criminal involvement may not be present— pose possible Fourth Amendment concerns.

B. Fifth and Fourteenth Amendment Due Process Issues

- The Supreme Court has held that reliability, as opposed to unnecessary suggestiveness, is the key to determining if a criminal identification survives a due process challenge.[19] The factors used to gauge reliability include: the eyewitness's

opportunity to view the suspect, the degree of attention the eyewitness is able to direct to the suspect, the accuracy of any description the eyewitness gave, the time between the crime and identification, and others.[20] Use of facial recognition in "virtual lineups" raises due process concerns as it is unclear if the algorithms making these criminal "identifications" are able to meet these factors – especially in the wake of concerns about their ability to function accurately (these concerns are discussed in the following bullet points).

- Additionally, there exists minimal case law that assesses these factors when a lineup was performed by a computer using facial recognition software.

C. Fifth Amendment Self Incrimination Issues

- In United States v. Wade, the Supreme Court established that the Fifth Amendment protects persons against self-incrimination by *testimonial* acts.[21] Testimonial acts are ones that show a person's mental processes – such as a verbal confession stating "I killed the victim," or telling someone a password or combination to a safe. Wade views a person's physical characteristics – such as a fingerprint, eye color, facial measurements, blood type, handwriting or voice – as non-testimonial, as these characteristics are unique to an individual and largely public.[22] Non-testimonial acts, which include facial recognition and other biometric identification, are thus outside the scope of Wade's Fifth Amendment protections.[23]
- Issues arise, however, when more and more companies use this non-testimonial/physical method of biometric identification in place of mental processes or token-based IDs in order to guard electronic devices that contain a wellspring of sensitive and personal information, as well as information that could be germane to an alleged crime. This issue is discussed, below, with respect to the Baust case and others.

D. Sixth Amendment Right to Counsel Issues

- The Supreme Court has held that a person's Sixth Amendment right to counsel attaches if they appear in a lineup after being indicted, as well as if they appear in a pre-indictment showup.[24]
- It is unclear if these "virtual lineups" are more akin to lineups or showups (i.e. scanning faces in a crowd versus focusing on a single person), however, "virtual lineups" trigger potential Sixth Amendment violations as the right to counsel may attach upon the completion of this virtual identification.

E. Accuracy of Facial Recognition Software

- A 2018 study by a British non-profit found that 95% of facial recognition "matches" by law enforcement wrongly identified innocent people as criminals.[25]
- The Perpetual LineUp (TPL), a study by Georgetown Law's Center on Privacy and Technology, found that only two agencies conditioned the purchase of their facial recognition software on the accuracy of the technology.[26]
- In general, the utility of facial recognition software is dependent on law enforcement officers' understanding of how to use it; yet without specialized training, TPL found that persons making decisions on facial matches are wrong

about half the time.[27] TPL also found that only eight of the facial recognition systems it studied had trained personnel reviewing matches (and it is unclear to what extent this training is regulated).

- Although facial recognition software use is widespread amongst government/law enforcement, it is not subject to any real feedback or testing. While the TSA is proposing to invest significant resources in building largescale surveillance infrastructures at airports, there are no existing standards for the public to assess the accuracy of/provide feedback on such a system; which means that surveillance could increase without any proof that this technology keeps us safer.[28]

F. Perpetuation of Racial Bias and Injustice within the Criminal Legal System

- Federal, state and local law enforcement agencies across the United States use facial recognition software, and it is estimated that 117 million American adults are in facial recognition networks used by law enforcement.[29]
- A 2018 MIT Media Lab study found that facial recognition algorithms designed by IBM, Microsoft and Face++ had error rates of up to 35% or higher when identifying darker-skinned women as compared to lighter-skinned men (for which the error rates were under 1%).[30]
- The American Civil Liberties Union (ACLU) demonstrated the problems with Amazon's Rekognition facial recognition system – a *real time* facial recognition system – when it tested the software on the 535 members of Congress.[31] Amazon's system incorrectly matched twenty-eight congresspersons to criminal mugshots; eleven of these twenty-eight false matches misidentified representatives of color (including the late civil rights pioneer John Lewis).[32]
- In Detroit, where African Americans make up a larger portion of residents than in other sizable American cities, studies showed that facial recognition software used by law enforcement was less accurate when attempting to identify persons with darker skin.[33] These inaccuracies resulted, in part, from the software's homogenous dataset consisting mostly of white, male faces.[34]
- On a general level, facial recognition software has a higher chance of disproportionately affecting African Americans when used by law enforcement as African Americans are more likely to be enrolled in these database systems and subject to their processing.[35] This reality demonstrates how the shortcomings of facial recognition at once exacerbate and reflect the pre-existing racial bias currently plaguing our legal system. One aspect of this racial bias includes the rampant over-policing of African American communities and other communities of color which has resulted in individuals from these communities being incarcerated at higher rates than white individuals.[36]
- These concerns have led some software companies to halt the selling of facial recognition software/biometrics to law enforcement.[37]

G. Widespread, Unbridled and Unbeknownst Use

- Concerns about the use of this technology by individuals are exacerbated by the fact that facial recognition software is at once nascent and burgeoning; the New

York Times published an article detailing how its author built a facial recognition software machine for $60 and installed it in Bryant Park (the facial dataset was composed entirely of photos found on public websites, and existing cameras were used).[38] This machine successfully matched some persons with 89% accuracy and highlights how disturbingly accessible facial recognition software is and how easy it is to track people without their knowledge.[39]

- Law enforcement uses facial recognition technology in body cameras, "virtual lineups," mugshots, surveillance, etc. While it is hard to quantify the exact extent to which facial recognition is used across society, Georgetown's TPL study found that "at least one out of four state or local police departments has the option to run face recognition searches through their or another [agency's] technology . . . [and] . . . [a]t least 26 states (and potentially as many as 30) allow law enforcement to run or request searches against their databases of driver's license and ID photos."[40] This same study also found that, ". . . 16 states let the FBI use face recognition technology to compare the faces of suspected criminals to their driver's license and ID photos, creating a virtual line-up of their state residents . . . " and that "Roughly one in two American adults has their photos searched this way."[41]
- Both the FBI and ICE use facial recognition to scan millions of drivers' license photos in state DMV databases without people's knowledge or consent.[42]
- The New York City Police Department (NYPD) also uses "virtual lineups" to identify teenagers and children using juvenile mugshots as a dataset.[43] These efforts produced proof that the facial recognition system used has a higher risk of false matches for younger faces.[44]

H. Assault on Personal Privacy

- NYPD has access to approximately 9,000 cameras in Lower Manhattan, and the extent of other camera systems used by the Metropolitan Transit Authority (MTA) and New York City Department of Transportation (DOT) is unclear.[45]
- One example cited in Georgetown's TPL concerns Maricopa County, Arizona. Upon purchasing facial recognition software in 2006, the Maricopa County Sherriff's Office merged its driver's license and mug shot databases and the U.S. Department of Justice's (DOJ) booking database with Honduran drivers' licenses and booking photos (provided by the Honduran government) to create a large facial recognition database.[46] Maricopa County did not require reasonable suspicion to run a facial recognition search; furthermore, African Americans are likely overrepresented in the system as they were arrested in Arizona at a rate 170% higher than their population share.[47] Within the Sherriff's Office, a Facial Recognition Unit supervises these searches, and employees are instructed to receive supervisor approval before returning possible results.[48] The TPL, however, found that Maricopa County was not conducting any audits of the system.[49]

IV. OTHER CONCERNS AND CONSIDERATIONS

A. Impingement on General Human Dignity and Privacy

- Some academics – including Italian philosopher and author Giorgio Agamben – argue that biometrics fundamentally and permanently alter the relationship between

individuals and the state, whereby we are subject to perpetual surveillance by the state through ". . . the enrollment and the filing away of the most private and incommunicable aspect of subjectivity: I mean the body's biological life."[50]

- Additionally, this form of tracking/control, historically reserved for persons deemed dangerous or criminal, has ballooned to a widespread, habitual method of state-sponsored surveillance of society at large.[51]
- These concerns are augmented by the normalization of this technology: facial recognition suddenly becomes less threatening when you voluntarily use Snapchat, Facebook, video games, Face ID, etc.[52] This mindset obscures the reality that facial recognition is becoming at once more customary and more latent.
- While some social media companies provide users with instructions on how to opt out of biometrics use with respect to its products, others do not, and it is not always easy to opt out of facial recognition surveillance.[53] This is true on both the macro and micro levels (i.e. at the airport, as TSA expands its biometric efforts and with the rise of the Internet of Things and the rapid escalation of a nearly complete "connectivization" of our lives/households with smart devices through Machine Learning).[54]
- Companies have developed methods such as glasses to disrupt facial recognition software's ability to measure one's face (flu/pollution masks and certain makeup are also effective at disrupting the facial measurement algorithms).[55]
- Large tech companies – such as Google, Facebook and Microsoft – as well as some large R1 Universities have amassed huge biometric data sets (some with millions of images) to develop facial recognition systems.[56] While these entities currently have no legal obligation to disclose these datasets, some have voluntarily shared this information for purposes of further development/research.[57]

B. Data Security

- A security breach could have devastating effects on the personal/financial/medical privacy of millions of people, as well as raise concerns about national security.[58]

C. Increased Risk of Criminal "Self-Help"

- The fact that facial recognition/biometrics are more secure than knowledge or token-based systems may motivate more violent efforts when one wants to gain access to a device secured by biometrics (i.e. physically forcing a person to hold up their face to a scan or cutting off their finger for a fingerprint to gain access, as opposed to stealing a person's key or password).[59]

D. Financial and Employment Concerns

- Some large companies use software that measures job applicants' facial movements, word choices and speaking voice to generate an "employability score" and ranks candidates based on these scores.[60]
- It is unclear what research informs these algorithms and if they are actually accurate/fair/or truly identify which employee will be "best" for a job based on these biometric measurements.[61]

E. First Amendment Free Speech Issues

- In the wake of Freddie Gray's death, the Baltimore Police Department employed facial recognition on social media to identify protestors with outstanding warrants.[62] This use of facial recognition software raises concerns that it could chill free speech.
- Georgetown's TPL observed that of the 52 agencies that it found to use (or have used) facial recognition, only one – the Ohio Bureau of Criminal Investigation – has a policy that expressly prohibits its officers from using facial recognition to track individuals engaging in political, religious, or other protected speech.[63]

F. Lack of Governing Law

- The current legal landscape (discussed below) is all but void of regulations to address the concerns listed above.
- Additionally, the facial recognition market is expected to grow to $7.7 billion in 2022 from $4 billion in 2017.[64] This financial incentive may increase opposition by companies toward government efforts to regulate this technology.

V. CRIMINAL AND CIVIL CASES DEALING WITH FACIAL RECOGNITION SOFTWARE AND BIOMETRICS

- Biometrics and facial recognition are very much unbound technologies that have taken root in an ambiguous legal landscape.

A. SCOTUS

- While there is caselaw addressing technology and Constitutional Rights (i.e. Kyllo v. United States (the use of a heat sensor to see inside a house is a search per the Fourth Amendment); United States v. Jones (placement of a GPS tracker on a car is a search per the Fourth Amendment); Riley v. California (warrantless search of a cellphone is not permissible); and, most recently, Carpenter v. United States (a warrant is needed for seven or more days of historic cell site information/cellphone location data, as such information is analogous to an ankle bracelet for near-perfect surveillance), there is currently no case law that specifically addresses facial recognition software.[65]

B. Federal

- Facebook's DeepFace program – a deep learning recognition system – draws from a database of millions of images uploaded to Facebook and is said to be more accurate than other large-scale facial ID systems.[66] Facebook rolled out DeepFace in 2015 and the system has since been the subject of several class action lawsuits alleging that it violates Illinois' Biometric Information Privacy Act (BIPA),[67] the most recent of which was dismissed for lack of jurisdiction/improper venue.[68]
- In Patel v. Facebook, however, the Northern District of California held that a loss of one's statutory biometric privacy rights is enough to sue a company under BIPA – and that a showing of actual harm is not necessary.[69] Privacy advocates lauded Patel as a huge BIPA victory and its rationale akin to Rosenbach v. Six Flags, a

recent Illinois Supreme Court case, discussed below.[70] Plaintiffs in Patel are claiming $35 billion in damages.[71]

- Facebook appealed Patel to the Ninth Circuit Court of Appeals, claiming that plaintiffs did not have standing to sue, as Facebook's biometric analysis of their photos did not cause them to suffer any concrete harm, and that the district court erred in certifying the class.[72]
- In August of 2019, the Ninth Circuit affirmed the District Court's ruling in Patel, holding that Facebook's violation of BIPA was equal to a violation of the plaintiff's substantive privacy rights and was a concrete injury.[73] In its rationale, the Court looked at the "forest" of recent U.S. Supreme Court Fourth Amendment jurisprudence, which has acknowledged how technology has immensely increased the potential for unreasonable invasion into personal privacy and how these new technologies are not comparable to pre-information age methods of surveillance, etc.[74] It is likely Facebook will appeal this ruling to the Supreme Court.
- There are also a host of class action suits currently pending in the Northern District of California against Facebook in response to the Cambridge Analytica data-sharing scandal.[75] This scandal concerned the secret harvesting of personal data from millions of Facebook pages by British political consulting firm Cambridge Analytica, which it then sold for political advertising purposes.[76]
- Some federal district courts have followed the rationale similar to that outlined in Commonwealth v. Baust – a Virginia state court decision, discussed below – that seems to limit Fifth Amendment protections against biometric use, while others have ruled in the opposite direction.[77] In 2016, a federal magistrate judge in California approved a warrant that compelled a defendant to produce her fingerprint to unlock her phone for the FBI, holding that the unlocking of her phone with her finger was a form of authentication of its contents.[78]
- More recently, however, in early 2019, a Northern District of California magistrate judge denied a portion of a warrant that sought to force persons suspected of an extortion scam on Facebook to unlock their iPhones using their fingerprints.[79] The judge held that technology is outpacing the law at a rapid pace and it is nonsensical that the law considers a verbal communication of a passcode testimonial, and thus worthy of Fifth Amendment protections, and not one's fingerprint or face when used for the exact same purpose.[80]
- This ruling is not binding on any other judge or court in the Northern District of California but is a possible indication of change in how courts view biometrics and Constitutional protections.
- That same year, a federal magistrate judge in the Northern District of Illinois granted the government's application for a search warrant for a residence for child pornography, but rejected its request to compel any persons in the residence at the time to unlock their iPhones with their fingerprints.[81] The court held that compelling production of fingerprints from a large group of people present at the execution of a search warrant to unlock seized devices raised Fifth Amendment concerns, specifically for the failure to establish a connection between any specific

resident and the alleged crime.[82] The court further stated that that an act could qualify as testimonial in nature where ". . . the existence, possession and control, and authenticity of information which tends to incriminate . . ." the person in question.[83] Later in the decision, however, the court emphasized that its ruling was highly fact sensitive and was not meant to mean that the government's request for forced fingerprinting will always trigger equivalent Constitutional concerns.[84]

- While this case has a host of positive treatment, there are many cases that have refused to follow the Northern District of Illinois' In re Application for a Search Warrant. Most recently, in the 2019 In the Matter of A White Google Pixel 3 XL Cellphone in a Black Incipio case, the United States District Court of Idaho refused to follow In re application for a Search Warrant, stating that a warrant compelling someone suspected of possession of child pornography to unlock his phone with his finger *did not* violate his Fifth Amendment rights.[85] While it acknowledged the intensity of privacy rights associated with today's cell phones and biometric data, the court in White Google Pixel looked to a host of recent similar cases across district courts which based their rulings in Wade's (and its robust progeny's) notion that the Fifth Amendment Right Against Self-Incrimination protects people against the government compelling them to make *testimonial* acts – or acts that display "the contents of one's own mind."[86] The court concluded that pressing one's finger to a phone, "is simply the seizure of a physical characteristic". . . [and] . . . there is no need to engage in the thought process of the subject at all in effecting the seizure . . .. [as] . . .the fingerprint by itself does not communicate anything."[87]
- On the macro level, White Google Pixel, displays the divergence of federal jurisprudence on Fifth Amendment issues and biometrics and highlights how a well-informed Supreme Court decision might provide much-needed direction on this issue.

C. States

1. *Virginia*

- In Commonwealth v. Baust, a Virginia state trial court held that while police cannot compel a suspect to provide his passcode to unlock his smartphone – as this is a violation of the Fifth Amendment right against self-incrimination – the police *can* compel that same suspect to produce his fingerprint to do the same.[88] Baust distinguishes physical-based (i.e. fingerprint) security from testimonial security (i.e. providing someone with a verbal or written password), deeming it outside the scope of Fifth Amendment protections against self-incrimination.[89]
- Specifically, the judge in Baust held that producing one's fingerprint did not require the communication of knowledge, but rather is more akin to being ordered to produce something physical – such as a DNA sample or a key to a safe – which is permitted per United States v. Wade (which holds that the Fifth Amendment "offers no protection against compulsion to submit to fingerprinting)."[90] Wade deems an act to be "testimonial," and thus worthy of Fifth

Amendment protections, when law enforcement forces a person to reveal his knowledge of facts, thoughts and beliefs relating him to the offense (i.e. "the content of his own mind"); a fingerprint is not testimonial as it does not require the defendant to "communicate any knowledge at all."[91]

- While several recent cases refused to follow Baust, a host of recent state rulings reference Baust and mirror its rationale of the Fifth Amendment's testimonial privilege and biometrics. In 2017, the Minnesota Supreme Court held in State v. Diamond that the Fifth Amendment does not protect a person from being ordered to provide a fingerprint to unlock a seized cellphone because the compelled act is not a testimonial communication.[92] Like Baust, the court's decision hinged on the proposition that providing a fingerprint elicits only physical evidence from a suspect's body and does not reveal the contents of the person's mind.[93]

2. ***Florida***

- In 2016, a Florida district court cited Baust in Florida v. Stahl, where it held that compelling a fingerprint to open an iPhone is not protected by the Fifth Amendment.[94]
- Recently, a Florida state appellate court held that a defendant/appellant had no right to view photos of other suspects identified by FACES, a facial recognition software whose search produced a "one star" ID match of the defendant that led to his arrest.[95] FACES' ID match was not subject to any accuracy audits.[96] This case raises several constitutional issues (i.e. Brady Disclosure, Sixth Amendment issues, Daubert issues, etc.) and was appealed to Florida's Supreme Court.[97]

3. ***Illinois***

- BIPA has been the subject of a host of lawsuits by tech giants – such as Google and Facebook – although these efforts, as of this date, have not yielded any success for them. Facebook has also spent considerable resources lobbying to amend/restructure BIPA.[98]
- In response to BIPA's most recent challenge in Rosenbach v. Six Flags – where parents sued Six Flags upon learning that the amusement park fingerprinted their fourteen year old son without their consent – the Illinois Supreme Court found in favor of the family when Six Flags sued to have the suit dismissed.[99] The court disagreed with Six Flags' argument that BIPA required that one show an injury beyond loss of statutory privacy rights, and held that that a finding of actual harm under the BIPA was not necessary for purposes of being "aggrieved" and the plaintiffs could proceed with their class action against the park.[100] The court held that merely

losing one's biometric privacy is sufficient enough harm for purposes of proceeding with an action under BIPA.[101]

- While advocates lauded Rosenbach as a crucial victory in the fight to preserve personal privacy, critics voiced concerns that it will only encourage what some consider the recent onslaught of BIPA litigation in Illinois in the wake of this lessened standard of harm necessary to pursue a case; over 200 BIPA cases were filed in the two years before Rosenbach, and some of the larger tech companies, such as Facebook, are facing possible damages in the billions.[102]
- In response to BIPA/Rosenbach, some companies have started including provisions requiring consent to biometric security in employee handbooks.[103]

4. ***New York State***

- In 2009, the Court of Appeals ruled in People v. Weaver that the police must first obtain a warrant before tracking a person's vehicle with a GPS device as it violates the Fourth Amendment protection against unreasonable search and seizures (basically establishing Jones protections three years before SCOTUS).[104]

5. ***New Jersey***

- In State v. Andrews, the New Jersey Superior Court held that testimonial aspects of passcodes required to unlock a defendant's smartphones were a "foregone conclusion," and thus compelled production of passcodes did not violate the defendant's Fifth Amendment privilege against self-incrimination under this exception.[105]
- In this regard, Andrews treats Baust negatively in that Baust held that a "password is not a foregone conclusion because it is not known outside of [the defendant's] mind."[106]

- Like the federal landscape, the state jurisprudence is also very divided on the issue of Fifth Amendment protections and biometrics and federal guidance could help bring consistency.
- There seems to be a lag in jurisprudence with respect to assessing the functionality, as opposed to the physicality, of biometrics as it relates to guarding against self-incrimination. One might argue that while, singularly, a finger print is a physical part of your body, Baust/White Google Pixel/etc. ignore the marked rise in the use of biometrics for forensic passwords/identification as they are harder to fake and better at guarding sensitive information. Viewed in this way, a fingerprint may be more analogous to a password than a key.
- While it is true that, like a key, a fingerprint is a physical thing (versus a testimonial verbalization of a thought), it is the *use* of this fingerprint and its potential to extract incriminating evidence from a smartphone, for instance, on which the Fifth Amendment analysis should turn. The intended use (function) should be more significant than the physicality (form). Thus, if fingerprints are being used to unlock a device in order to

explore the device's contents, law enforcement should not be permitted to compel persons to do so because this act is tantamount to providing a password and therefore, in effect, testimonial.

- To these points, when the Supreme Court decided Wade in 1967, computer technology was in its infancy. An updated Supreme Court decision that distinguishes/extends Wade's definition of a "testimonial" act to include biometrics identifiers would be appropriate to protect our Constitutional rights in the Digital Age.

VI. LEGISLATION AND REGULATIONS DEALING WITH FACIAL RECOGNITION SOFTWARE AND BIOMETRICS

- Regulation of facial recognition technology/biometrics can apply to the use, storage or retention of biometric data, as well as to the formal technology itself; however, the current regulatory landscape is inadequate across federal, state and local jurisdictions. This reality augments the concerns listed above.

A. Federal

- Currently, there exists no federal, all-encompassing law that protects user privacy and regulates the storage of personal data (biometric or other) by the private sector.[107]
- The Electronic Communications Privacy Act of 1986 (ECPA) is a federal statute that sets standards for government monitoring of cell phone and internet communications.[108] This law, however, deals more with storage of personal data, rather than limitations on the biometric technology itself.[109] It was also passed long before the extreme technological advancements of the past twenty-five years and thus has many shortcomings with respect to protecting people's privacy.[110]
- 18 USC 2703(d) allows the government to obtain third party electronic data (i.e. data from Facebook, Uber, Verizon, etc.) if it "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[111] This 2703(d) standard is a much lower bar than obtaining a warrant with probable cause. As with the ECPA, however, this law deals more with long term surveillance/third party/Carpenter surveillance issues (discussed in the pages below), rather than biometrics specifically.
- Senators Roy Blunt (R-MO) and Brian Schatz (D-HI) have introduced the Commercial Facial Recognition Privacy Act of 2019 (S.847), or CFRPA, which would require consent before using biometric ID/tracking on individuals by businesses, but *does not* apply to local, state or federal governments.[112]
- In late 2019, Senator Maria Cantwell (D-WA) introduced the Consumer Online Privacy Rights Act (S.2968), or COPRA, the first ever comprehensive federal consumer privacy law.[113] COPRA establishes data and privacy protections, including the right to access and delete one's personal data held by an entity, and protects individuals by imposing data security requirements on companies to ensure their practices are sufficient to safeguard personal data.[114] Additionally, COPRA

establishes a private right of action for individuals to sue in the event a company violates their privacy as well as empowers state attorneys general to enforce the law.[115]

- In July of 2019, U.S. Representative Yvette D. Clark (D-NY-9) introduced the No Biometric Barriers to Housing Act (H.R. 4008), which would ban the use of biometric technology, including facial recognition, in certain federal rental units.[116] H.R. 4008 is co-sponsored by Representative Rashida Tlaib (D-MI-13), whose constituents in Detroit have voiced concerns about large scale facial recognition technology use in federal public housing by law enforcement.[117]
- In late June of 2019, Representative Michael McCaul (R-TX-10) and Senator Martha McSally (R-AZ) introduced the Biometric Identification Transnational Migration Alert Program Authorization Act of 2019 (H.R. 3377/S.1933). These bills direct federal funds to amend the Homeland Security Act of 2002 to establish the Biometric Identification Transnational Migration Alert Program (BITMAP) in the Department of Homeland Security.[118] BITMAP calls for the use of facial recognition and other biometric data to enhance border security.[119] The bills direct the U.S. Department of Homeland Security to coordinate with the U.S. Secretary of State, foreign governments, and other Federal agencies, as appropriate, to voluntarily share biometric information collected by foreign nationals in order to screen these persons to identify any potential threats to the United States.[120]
- While H.R. 3377/S.1933 touch on how biometric data of U.S. citizens captured by BITMAP should be expunged from all databases, it makes an exception to retain this data ". . . for specific law enforcement or intelligence purposes." [121] This exception seems vague and outlines no other details on how the law would curb potential abuses caused by the unbridled gathering of biometric data by the government/law enforcement.
- It is important to note that, with the exception of the No Biometric Barriers to Housing Act (H.R. 4008), the aforementioned federal legislation does not attempt to regulate facial recognition technology itself, but rather proposes limits on the manner in which biometric data is collected/stored. While there are some other federal bills that mention biometric identification, none propose to regulate this technology directly. Additionally, H.R. 4008 does not provide for any kind of uniform/industry-wide standards for facial recognition itself, but rather proposes restrictions on biometrics in a specific situation.[122]
- While the National Institute of Standards and Technology (NIST), a branch of the U.S. Department of Commerce, administers the Face Recognition Vendor Test (FRVT), which tests the accuracy of facial recognition software in different scenarios and across various demographics (i.e. age, race, gender), this test is voluntary. The overall role of the NIST is to gather data rather than promulgate regulations.[123] NIST allows companies to send one submission for FRVT assessment every four months.[124]

B. States

- Most states have not passed any laws regulating biometrics/facial recognition technology. This type of data is being regulated by existing privacy laws, which are not best postured to address the concerns posed by this technology (discussed above). Facial recognition data may be regulated per a privacy policy so long as there is no direct regulation/restriction by a specific federal law (i.e. HIPPA, Privacy Act of 1974, etc.). There are a handful of states, however, that are making efforts to reign in biometrics.
- An important distinction across these various state laws is that some – like Illinois' Biometric Information Privacy Act (BIPA) – create a private right of action for individuals, or classes, to enforce the law and seek damages, while others, like the California Consumer Privacy Act (CCPA), provide a limited right of action; others are only enforceable by a state's attorney general.[125]
- How states define "biometric information" varies as well. Under the CCPA, it is broadly defined to include physiological, biological, and behavioral characteristics – such as also keystroke and gait patterns as well as certain sleep and exercise data – while BIPA and Texas's Biometrics Privacy Law have a more traditional definition – limited to things such as fingerprints, voiceprints, iris and facial scans.[126]
- There has been a recent trend with respect to states proposing laws that would limit the use of facial recognition and biometric identification technologies, including Alaska, Arizona, Florida, Michigan and Delaware.[127] Even within these efforts, however, there is divergence between these proposed laws, and perhaps some kind of federal legislative floor is necessary to ensure a uniform statutory landscape.

1. *Illinois*

- Illinois passed BIPA in 2008, back when Facebook was still in its relative infancy and most companies were not thinking about face-recognition technology.[128] It was the first state in the country to do so.[129] BIPA requires that entities obtain affirmative consent from individuals before obtaining their biometric information and creates a private right of action for individuals to sue to enforce the law.[130]
- Under BIPA, a prevailing party may recover actual damages or liquidated damages of $1,000, whichever is greater*, for each violation*.[131] If the violation is intentional or reckless, however, these liquidated damages go up to $5,000 per violation.[132] Injunctive relief and reasonable attorney fees and costs, as well as expert witness fees and other expenses, are also available to a prevailing party.[133]
- While BIPA has its critics, aims to hold accountable an industry that for years has been collecting individuals' biometric information with near-total impunity.

2. *Texas*

- Texas's 2009 Biometrics Privacy Law defines "biometrics" as more traditional physical characteristics (i.e. voice, face, fingerprints, etc.). and allows for civil penalties of up to $25,000.[134] Unlike BIPA, however, only the Texas Attorney General can enforce biometric privacy violations.[135]

3. *Washington*

- In 2017, Washington passed House Bill 1493, becoming only the third state in the country to pass legislation regulating the use and collection of biometric information.[136] HB 1493 defines "biometric identifier" as data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises or other unique biological patterns or characteristics that are used to identify a specific individual.[137]
- Unlike the Illinois and Texas statutes, HB 1493's definition of "biometric identifier" excludes facial recognition data.[138]
- Currently, the proposed Washington Privacy Act (SB 5376) would allow consumers the right to access and manage their biometric data held by companies.[139] The law also proposes setting standards for the use of facial recognition technology.[140] As of January 2020, this bill is still in committee and several amendments have been proposed.[141]
- By way of House Bill 1071 (HB 1071), Washington recently expanded its existing data breach response law to include biometric data in its definition of personal information.[142] Passed in May of 2019, HB 1071 goes into effect in May of 2020.[143]
- This new definition of "personal information" is expansive and includes: "Biometric data generated by automatic measurements of an individual's biological characteristics such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual."[144]
- HB 1071 also expands the reporting requirement for entities that "maintain *or possess* [emphasis added]" personal information; they now must notify affected person(s) of any breach in security with regard to the maintenance of such information.[145] The law requires that an entity must also notify the Washington Attorney General in the event of a data breach that impacts more than 500 people within 30 days of discovery of such breach.[146]
- HB 1071 makes an exemption to the notification requirement when a data breach "is not reasonably likely to subject consumers to a risk of harm" or when data was acquired in good faith.[147] The law defines a "good faith acquisition of personal information" as when "the personal information is not used or subject to further unauthorized disclosure."[148]

4. ***California***

- In mid-2018, California passed the CCPA which allows Californians more control over their biometric data.[149] The law allows persons to see which information businesses collect on them, request this data be deleted, see to whom their data is being sold, and lets persons stop this data from being sold if they so choose.[150] Set to go into effect in 2020, CCPA also requires that companies get users' permission before collecting data.[151]
- The CCPA amends California's definition of personal information to include biometric data, which the CCPA broadly defines to include physiological, biological and behavioral characteristics.[152]
- Facebook, Google and other software/social media entities vehemently opposed the CCPA, and its previous iterations.[153] Big Tech lobbyists have chipped away at the language in the bill to lessen companies' responsibilities to protect personal information (i.e. including a stipulation that businesses must include a clear button on their websites giving people the ability to opt out of data collection and the requirement that businesses share "accurate names and contact information" for third parties that bought user data over the prior year.[154] That language has since changed, requiring businesses to merely disclose the "categories of third parties" that bought the data).[155]

5. ***New York***

- New York's proposed Biometric Privacy Act (A.1911/S.1203) provides regulations for entities that store biometric data.[156] Specifically, private entities in possession of biometric data would have to develop written record retention schedules and guidelines for permanently destroying biometric data "when the initial purpose for collecting or obtaining data has been satisfied or within three years of someone's last interaction with the company, whichever is earlier."[157]
- Like BIPA, the Biometric Privacy Act also proposes a private right of action,.[158] This bill has failed to gain traction and opponents argue that it was a way for abuse by class action lawyers.[159]
- While New York recently updated its data breach law to include biometric data in its definition of "personal information" (discussed, below), biometric technology itself is not currently regulated directly; however, the New York Department of Labor prohibits the use of forced fingerprinting, "unless allowed by law."[160] This law often affects employers who want to use biometric timeclocks to combat wage theft.[161]
- In July of 2019, Governor Cuomo signed A.5635-B/S.5575-B – the Stop Hacks and Improve Electronic Data Security Act (SHIELD Act) – into law.[162] The SHIELD Act updates New York's data breach

notification law, expanding the types of covered personal information to include biometric data that would trigger notification obligations for entities in possession of "personal information" in the event of a data breach.[163] SHIELD also broadens the data breach notification requirement by mandating notification of unauthorized access *to* protected information, rather than just the acquisition of data.[164] While the law does not create a private right of action, it does authorize the New York State Attorney General to seek civil penalties for non-compliance.[165]

- The proposed A.7790/S.5687 prohibits the use of a facial recognition system by a landlord on any residential premises.[166]
- In Brownsville, Brooklyn, tenants of two rent-stabilized apartment complexes recently filed a complaint with the New York State Department of Homes and Community Renewal to enjoin their landlord from installing facial recognition entry systems in their buildings.[167] While the landlord claims these new systems are to ensure tenant safety, tenants insist that their buildings already have sufficient security and cite personal privacy concerns.[168]
- In the current legislative session, there is a wave of proposed legislation that aims to limit the use of biometrics/biometric data.[169] One of these bills includes A.9767/S.7572.[170] The bill proposes prohibiting the use of biometric surveillance by law enforcement, as well as establishing a biometric surveillance regulation task force.[171]
- While many of these proposed bills regulate data and/or limit the way/scope in which facial recognition/biometrics can be used, A.8042, S.5140 and S.6623 (and a few others) call for a fundamental, information-gathering process for biometrics in order to better understand this technology so that it can be more effectively regulated.[172] There currently exists no analogous legislative efforts at the federal level.

6. *Arkansas*

- In April of 2019, Arkansas passed House Bill 1943 (HB 1943), which amends the state's Personal Information Protection Act to include biometric data in its definition of "personal information."[173] HB 1943 also amends the State Code, requiring an entity in the possession of personal information to notify the Attorney General in the event of a data breach which affects the personal information of more than 1,000 individuals.[174] This bill is similar to the efforts recently taken by Washington's HB 1071, described above.

7. *Massachusetts*

- There are currently two bills pending in the Massachusetts legislature (H. 1583 and S. 1385) that would impose a moratorium on government use of biometric surveillance – including facial

recognition – until laws are passed regulating who may use it and how.[175]

C. Cities

1. *San Francisco, California*

- In mid-May of 2019, San Francisco passed a municipal ordinance banning the use of facial recognition technology, becoming the first city in the United States to do so.[176]
- The grassroots coalition that advocated for the passage of this ordinance cited civil liberties concerns, including widespread use by federal ICE agents, privacy concerns, and perpetuation of racial injustice as reasons for the need to ban facial recognition.[177]

2. *Oakland, California*

- Oakland banned facial recognition technology in July of 2019.[178]

3. *Sommerville, Massachusetts*

- In June of 2019, Sommerville's City Council banned the use of facial recognition technology in police investigations and municipal surveillance programs.[179]

4. *Berkeley, California*

- In mid-October of 2019, Berkeley, California joined its neighbors and passed a ban on all government use of facial recognition technology.[180]

5. *New York, New York*

- The New York City Council recently passed Int. 0487A-2018 (also referred to as the Public Oversight of Surveillance Technology (POST) Act) and it was enacted into law on July 15, 2020.[181] The POST Act increases oversight of the NYPD's use of surveillance technology by requiring reporting and evaluation of surveillance technologies used by the NYPD.[182] It will require the NYPD to draft a surveillance impact and use policy which will be subject to a public comment period.[183]
- In late 2018, New York City Councilman Ritchie Torres, head of the council's Committee on Oversight and Investigations, introduced Int. No. 1170-2018 that would regulate biometric use, to a degree.[184] The bill would amend Section 1, Chapter 5 of Title 20 of the City's Administrative Code and require businesses to provide notice to persons if they are collecting what the bill defines as biometric data.[185] The bill would not, however, apply to government agencies.[186]
- Like BIPA, Int. No. 1170 also creates a private right of action and allows for a prevailing party to recover damages of $1,000 per

violation against a negligent entity and $5,000 per violation against an entity that was reckless/intentional, and allows for attorney's fees and "other relief," including injunctive relief, "that the court deems appropriate."[187]

- Additionally, Int. No. 1170 gives the commissioner of the New York City Department of Consumer Affairs authority to implement a civil penalty of $500 per day for a violation.[188]
- It is important to note that Int. No. 1170 *does not* apply to government entities; this means that the plethora of constitutional concerns, discussed above, are not addressed by this bill.[189] Critics on the other side of the spectrum have voiced concerns that Int. No. 1170 will lead to a BIPA-like influx of litigation.[190]
- In related efforts, Councilman Brad Lander introduced Int. No. 1758-2019 in October of 2019. [191] This law would define the word "key" in the City Code and require that building owners provide mechanical keys to residents for both the exterior door of their buildings and the doors to their individual apartments.[192] It would also prohibit landlords from forcing tenants to use keyless entry technology to enter their buildings.[193]
- In August of 2019, Councilman Donovan J. Richards introduced Int. 1672-2019, which requires real property owners to submit registration statements regarding biometric recognition technology utilized on the premises.[194] The bill would also require the City's Department of Information Technology to establish a database and provide an annual report to the Mayor and the City Council.[195]

D. Other Countries

- The European Union (EU) has been more proactive than the United States with respect to regulating biometric data. In 2016, it passed the General Data Protection Act (GDPA), the world's strongest data protection law, which came into force in mid-2018.[196] One of the goals of the GDPA is to modernize data protection and institute uniformity across the EU's legal landscape.[197]
- The GDPA contains ninety-nine articles that outline the rights of individuals and obligations placed on organizations covered by the law and establishes a penalty scheme and responsibility for organizations to obtain the consent of persons from whom they collect personal data.[198]
- The GDPA defines "personal data" as ". . . any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person . . ." [199]
- The United Kingdom passed its own version of the GDPA – the Data Protection Act of 2018 – which largely mirrors the EU's law, in anticipation of Brexit.[200] It

currently has no law, however, regulating the formal use of biometric facial recognition cameras, specifically.[201]

- In contrast, the London police force recently instituted a large-scale camera network used for a "perpetual lineup."[202] These efforts have been met with protest and pending legal challenges.[203]
- In other counties, use of facial recognition is more widespread. In China, you can use facial recognition to order fast food, while police officers have also begun wearing glasses with facial recognition capabilities that allow them to track and identify individuals within large crowds.[204]
- Chinese tech giant Huawei has installed its "Safe Cities" facial recognition monitoring system in cities across the globe where Chinese companies have made recent, large-scale business investments (such as Belgrade, Serbia and Kampala, Uganda, among others).[205] These countries often have less power and military infrastructure than China.[206] In the wake of these efforts, citizens of these nations have voiced privacy concerns, which have been augmented by claims that Huawei's facial recognition systems will give China unfettered access to its data (because of accusations of government control of the company) which could compromise the privacy of people in poorer countries that may not have the power to stand up to China.[207] If the people in these nations speak out against China or act in ways that China deems threatening to its business interests, critics claim that China could easily spy on them using Safe Cities technology and crush dissent.[208] "Safe Cities" is an example of how government and private entities might use facial recognition software to impinge on human rights and repress dissent. Huawei's "Safe Cities" systems are found in some 230 cities worldwide.[209]
- Aadhaar – India's national ID program – is the world's largest biometric database.[210] It holds profiles of people for their lifetime and was designed to help government agencies deliver public services securely, to a large group of people, using biometric and demographic data.[211]
- Over 500 million residents are enrolled in the system; however, Aadhaar has come under fire from critics because of data security concerns, errors in record keeping which have led to injury and death, and a general concern about personal autonomy/privacy. These concerns led India's Supreme Court to establish privacy as a fundamental right.[212]

- Some academics and others have called for a complete ban on facial recognition because of its power, pervasiveness and potential to completely and permanently alter the dynamic between individuals and the state with respect to personal privacy.[213] They argue that industry guidelines and even legislation itself cannot curb potential abuses of this technology (although a ban at this point seems unfeasible, as the use of facial recognition use is so widespread).[214] Other arguments favor more regulation, as a ban would prohibit positive uses of the technology.[215]

VII. PRIVATE SECTOR EFFORTS TO REGULATE FACIAL RECOGNITION AND BIOMETRICS

- At this time, no industry-wide standards exist that would allow for uniform biometric technology use. While some companies have made efforts to combat bias and inaccuracy in facial recognition software (e.g., IBM is introducing a more diverse dataset in the hopes of combating AI bias), it is unclear how impactful these efforts are.[216]
- Additionally, while not all companies are forthcoming about these efforts, others are informing the public of their contributions to researching and combating these issues.[217]
- Alternatively, Amazon, which came under fire in the ACLU's report of racial bias in its Rekognition facial recognition system, stated that it would not stop selling the software to a host of government and law enforcement agencies, even in the wake of complaints voiced by its own employees.[218] Amazon also refused to have NIST assess Rekognition.[219]
- A February 2019 blog post by Michael Punke, VP of Global Public Policy at AWS, highlights Amazon's concerns associated with AI and called for regulations to increase transparency in its use.[220]
- In 2018, after backlash from its participation in Project Maven – a Pentagon drone project – Google announced that it would no longer work on AI weapons projects and released a set of ethical guidelines for AI use and development (although it continues to work with the US military).[221] Google's own employees have also voiced concerns about Google's involvement with this project, with some resigning in protest.[222]
- The Institute of Electrical and Electronics Engineers, a large professional organization, has authored *Ethically Aligned Design,* a treatise on ethics in AI, and have created a global initiative to set standards to combat AI bias.[223]
- Joy Buolamwini – the researcher at MIT's Media Lab who discovered high rates of racial bias in a host of recognition algorithms – created the Algorithmic Justice League (AJL) to raise awareness of racial bias in biometric systems and work to combat this issue.[224]
- In an op-ed in the New York Times, House minority Leader Kevin McCarthy (R-CA-23) urged that trustbusting of large tech companies is not the answer to guarding against data breaches but, rather, urges a public/private sector partnership that incorporates technologies such as Cryptonetworks (decentralized platforms governed by the community of users themselves).[225] In Cryptonetworks, data would be controlled by blockchain encryptions, rather than the platform itself. McCarthy also calls for Congress to set a federal standard for privacy frameworks.[226]

VIII. FUTURE ACTION AND CONCLUSION

- Facial recognition is, at once, an emerging and rapidly advancing technology that is widely-used with a regulatory framework insufficiently postured to deal with the grave risks it poses to personal privacy, constitutional rights, and racial justice. These issues take the form of a frightening legal Venn diagram that merges two of the most pressing issues currently facing the legal profession: in one circle you find mass incarceration/racial injustice, and in the other, the inability of society to pass laws and issue judicial decisions that keep pace with technology.

- Considering the disjointed judicial landscape, this issue – particularly with respect to Fifth Amendment testimonial protections – is ripe for Supreme Court intervention, however it has no relevant cases on its docket.
- More uniform, comprehensive federal laws are also needed to fill the regulatory void and set minimum accuracy standards across the industry to attempt to curb the bias that infects facial recognition and other biometric technology.[227] The legislative scheme of this industry must also be changed from voluntary to mandatory.
- Augmenting NIST into a true regulatory agency will be crucial with respect to reforming our ability to regulate biometrics as this will allow for enhanced oversight of this industry as well as registration, training and testing of this software. While many of these deep learning algorithms that fuel biometric systems are challenging to send for analysis, because they are extremely large and update in real time, some sort of technological/regulatory scheme needs to be established such that NIST can properly test these systems for bias.[228] One solution may be that NIST establish a corps of inspectors who can travel to facilities to test software.
- This complex and wide-reaching technology may be best regulated through a multi-pronged approach that applies to both government and private entities.[229]
- While addressing the concerns presented by facial recognition and biometrics is an immense undertaking, these efforts present an opportunity for the legal profession to protect individuals' personal privacy and advance justice for society at large.

REFERENCES

[1] *What is Biometrics?*, Biometrics Research Group of Michigan State University, http://biometrics.cse.msu.edu/info/index.html (all websites last visited July 21, 2020).

[2] *Id*.

[3] *The History of Fingerprints*, onin.com, http://onin.com/fp/fphistory.html.

[4] *What is Biometrics?, supra* note 1.

[5] *See* Tarun Choubisa, SR Mahadeva Prasanna and Soyuj Kumar Sahoo, *Multimodal Biometrics Person Authentication: A Review*, IETE Tech. Rev. 2012, https://www.tandfonline.com/doi/abs/10.4103/0256-4602.93139?journalCode=titr20; *See* Danny Thakkar, *Unimodal Biometrics vs. Multimodal Biometrics*, BAYOMETRIC, https://www.bayometric.com/unimodal-vs-multimodal/ (describing how unimodal biometric systems measure one biometric trait [such as voice] while multimodal biometric systems measure two or more biometric trait [such as fingerprint and voice]).

[6] *See* Laura Blanc, *The Face of the Future*, Herta, Dec. 14, 2014, http://www.hertasecurity.com/en/node/210.

[7] *Id*.

[8] *See* Steve Symanovich, *How Does Facial Recognition Work?*, Norton, https://us.norton.com/internetsecurity-iot-how-facial-recognition-software-works.html; *See* Mark Williams Pontin, *Better Face-Recognition Software*, MIT Technology Review, May 30, 2007, https://www.technologyreview.com/2007/05/30/225291/better-face-recognition-software/; *See* Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work – 3D Facial Recognition,* How Stuff Works, https://electronics.howstuffworks.com/gadg ets/high-tech-gadgets/facial-recognition2.htm.

[9] *Id*.

[10] Danny Thakkar, *Biometric Regulations in the U.S. States: The State of Play*, BAYOMETRIC https://www.bayometric.com/biometric-regulations-us-states/.

[11] Danny Thakkar, *Top Five Biometrics: Face, Fingerprint, Iris, Palm and Voice,* BAYOMETRIC, https://www.bayometric.com/biometrics-face-finger-iris-palm-voice/.

[12] Jay Stanley, *How the TSA's Facial Recognition Plan Will Go Far Beyond the Airport*, ACLU, Oct. 23, 2018, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/how-tsas-facial-recognition-plan-will-go-far; *See, The Five Problems with CAPPS II*, ACLU, https://www.aclu.org/other/five-problems-capps-ii; *Testimony of Deputy Assistant Secretary for Policy Kathleen Kraninger and Director Robert A. Mocny Before the House Appropriations Committee and Subcommittee on Homeland Security and "Biometric Identification,"* Mar. 19, 2009, https://www.dhs.gov/news/2009/03/19/testimony-biometric-identification; *See* Transportation Security Administration, *TSA Biometrics Roadmap,* Sept. 2018, https://www.tsa.gov/sites/default/files/tsa_biometrics_roadmap.pdf.

[13] Stanley et. al., *supra* note 12.; Symanovich, *supra* note 8.; Julie Jargon, *Facial Recognition Tech Comes to Schools and Summer Camps*, The Wall Street Journal, Jul. 30, 2019, https://www.wsj.com/articles/facial-recognition-goes-to-camp-11564479008; Drew Harwell, *FBI, ICE Find State Driver's License Photos Are a Gold Mine for Facial-Recognition Searches*, The Washington Post, Jul. 7, 2019, https://www.washingtonpost.com/technology/2019/07/07/fbi-ice-find-state-drivers-license-photos-are-gold-mine-facial-recognition-searches/; Catie Keck, *United Airlines is Expanding Its Creepy Biometric Screening Technology to More Airport Hubs,* Gizmodo, Jul. 29, 2019, https://gizmodo.com/united-airlines-is-expanding-its-creepy-biometric-scree-1836789894; *See UT Introduces Advanced Biometric Security for Quick Access to Games*, KXAN, Oct. 18, 2019, https://www.kxan.com/news/local/austin/ut-introduces-advanced-biometric-security-for-quick-access-to-games/.

[14] International Institute for Democracy and Electoral Assistance, *Use of Biometric Data in Voter Registration,* https://www.idea.int/data-tools/question-view/738.

[15] *See* Tom Simonite, *How Facial Recognition Is Fighting Child Sex Trafficking*, Wired, Jun. 19, 2019, https://www.wired.com/story/how-facial-recognition-fighting-child-sex-trafficking/amp.

[16] Sahil Chinoy, We Built an 'Unbelievable' (but Legal) Facial Recognition Machine, The New York Times, Apr. 16 2019, https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html.

[17] *Id*.

[18] *See* United States v. Dionisio, 410 U.S. 1, 14 (1973); Hayes v. Florida, 470 U.S. 811, 816 (1985); Davis v. Mississippi, 394 U.S. 721, 724 (1969).

[19] *See* Neil v. Biggers, 409 U.S. 188 (1972).

[20] *Id*. at 199-200.

[21] *See* United States v. Wade, 388 U.S. 218, 221-224 (1967).

[22] United States v. Wade, *supra* note 21.

[23] *Id*.

[24] *Id*.; *See* Moore v. Illinois, 434 U.S. 220 (1977).

[25] Big Brother Watch, *Face Off: The Lawless Growth of Facial Recognition in UK Policing,* May 2018, pg. 3-4, https://bigbrotherwatch.org.uk/wp-content/uploads/2018/05/Face-Off-final-digital-1.pdf; *See generally* Madhumita Murgia, *How London Became a Test Case for Using Facial Recognition in* Democracies, The Financial Times, Aug. 1, 2019, https://www.ft.com/content/f4779de6-b1e0-11e9-bec9-fdcab53d6959.

[26] Center on Privacy and Technology, *The Perpetual Lineup: Unregulated Police Face Recognition in America*, Georgetown Law, Oct. 18, 2016, https://www.perpetuallineup.org/.

[27] *Id*.

[28] Stanley, *supra* note 12.

[29] *See* Center on Privacy and Technology, *supra* note 26.

[30] *See Gender Shades*, MIT Media Lab, http://gendershades.org/index.html.

[31] Russell Brandon, *Amazon's Facial Recognition Matched 28 Members of Congress to Criminal Mugshots*, The Verge, July 26, 2018, https://www.theverge.com/2018/7/26/17615634/amazon-rekognition-aclu-mug-shot-congress-facial-recognition.

[32] *Id*.

[33] Amy Harmon, *As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias,* The New York Times, Jul. 8, 2019, https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html.

[34] Steve Lohr, *Facial Recognition is Accurate, if You're a White Guy*, The New York Times, Feb. 9, 2018, https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[35] *Id*.; Clare Garvie and Jonathan Frankle, *Facial Recognition Software Might Have a Racial Bias Problem*, The Atlantic, Apr. 7, 2016, https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/.

[36] *See* Lohr, *supra* note 34.; *See* Garvie and Frankle, *supra* note 35.; *See generally* Xavier Picket, *Policing Black Communities,* Public Justice Report, First Quarter 2007. Vol. 30. No. 1, https://www.cpjustice.org/uploads/Policing_Black_Communities.pdf; *See also* Jennifer Gonnerman, *Before the Law,* The New Yorker, Oct. 6. 2014, https://www.newyorker.com/magazine%20/2014/10/06/before-the-law (discussing how many individuals from communities of color lack the socioeconomic resources to make bail and are often incarcerated for months – or even years – while awaiting trial, or the dismissal of charges, without ever being convicted of a crime).

[37] Garvie and Frankle, *supra* note 35.; Brian Brackeen, *Facial Recognition Software is Not Ready for Use by Law Enforcement,* TechCrunch, July 2018, https://techcrunch.com/2018/06/25/facial-recognition-software-is-not-ready-for-use-by-law-enforcement/; Lauren Goode, *Facial Recognition Software is Biased Towards White Men,*

Researcher Finds, The Verge, Feb. 11, 2018, https://www.theverge.com/2018/2/11/17001218/facial-recognition-software-accuracy-technology-mit-white-men-black-women-error.

[38] Chinoy, *supra* note 16.

[39] *Id.*

[40] Center on Privacy and Technology, *supra* note 26.

[41] *Id*.

[42] Harwell, *supra* note 13.

[43] Joseph Goldstein and Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, The New York Times, Aug. 1, 2019, https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html.

[44] *Id*.

[45] Chinoy, *supra* note 16.

[46] Center on Privacy and Technology, *supra* note 26.

[47] *Id*.

[48] *Id*.

[49] *Id*.

[50] *See* Giorgio Agamben, *No to Bio-Political Tattooing,* from Le Monde, Jan. 10, 2004, https://ratical.org/ratville/CAH/totalControl.pdf.

[51] Id.; Stanley, *supra* note 12; *See* Jay Stanley, *What's Wrong with Airport Face Recognition?*, ACLU, Aug. 4, 2017, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/whats-wrong-airport-face-recognition.

[52] Agamben, *supra* note 50.; Stanley, *supra* note 12.; Stanley, *supra* note 51.

[53] *Id*.; Symanovich, *supra* note 8.

[54] Nadia Kovacs, *What is the Internet of Things*, Norton, https://us.norton.com/internetsecurity-iot-what-is-the-internet-of-things.html.

[55] Maddie Stone, *These Glasses Block Facial Recognition Technology,* Gizmodo, Aug. 8, 2015, https://gizmodo.com/these-glasses-block-facial-recognition-technology-1722826081; *See* Robinson Meyer, *Anti-Surveillance Camouflage for Your Face,* The Atlantic, Jul. 24, 2014, https://www.theatlantic.com/technology/archive/2014/07/makeup/374929/.

[56] Cade Metz, *Facial Recognition Tech Is Growing Stronger, Thanks to Your Face*, The New York Times, Jul. 13, 2019, https://www.nytimes.com/2019/07/13/technology/databases-faces-facial-recognition-technology.html.

[57] *Id*.

[58] *Id*.; Maria Korolov, *What is Biometrics? And Why Collecting Biometric Data is Risky*, CSO, Feb. 12, 2019, https://www.csoonline.com/article/3339565/what-is-biometrics-and-why-collecting-biometric-data-is-risky.html; *See* James A. Martin, *5 Things to Know About Fitness Tracker and Security in 2018*, CSO, Jul. 5, 2018, https://www.csoonline.com/article/3286214/5-things-to-know-about-fitness-trackers-and-security-in-2018.html; *See also*, Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, Forbes, Aug. 14, 2019, https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#70270f9246c6.

[59] Jonathan Kent, *Malaysia Car Thieves Steal Finger*, BBC News, Mar. 31, 2005, http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.

[60] Drew Harwell, *A Face-Scanning Algorithm Increasingly Decides Whether You Deserve the Job,* The Washington Post, Oct. 25, 2019, https://www.washingtonpost.com/technology/2019/10/22/ai-hiring-face-scanning-algorithm-increasingly-decides-whether-you-deserve-job/.

[61] *Id.*

[62] Alison Knezevich and Kevin Rector, *Social Media Companies Rescind Access to Geofeedia, Which Fed Information to Police During 2015 Unrest*, The Baltimore Sun, Oct. 11, 2016, https://www.baltimoresun.com/news/crime/bs-md-geofeedia-update-20161011-story.html; Alvaro Beydoa, *Who's Logging Your Face?,* The Washington Post, Mar. 22, 2017, https://www.washingtonpost.com/opinions/whos-logging-your-face/2017/03/22/47d96142-0e67-11e7-ab07-07d9f521f6b5_story.html?utm_term=.bac654b1913c.

[63] Center on Privacy and Technology, *supra* note 26.

[64] Symanovich, *supra* note 8.

[65] *See* Kyllo v. United States, 533 U.S. 27 (2001).; *See* United States v. Jones, 565 U.S. 400 (2012).; *See* Riley v. California, 573 U.S. 373 (2014).; *See* Carpenter v. United States, 138 S. Ct. 2206 (2018).; *See* Robyn Greene and Michael Pizzi, *The Supreme Court Made a Sweeping Decision About Privacy Rights*, New America, Jul. 26, 2018, https://www.newamerica.org/weekly/supreme-court-made-sweeping-decision-about-privacy-rights/ (discussing how "Carpenter also raises more questions about how law enforcement should handle the surveillance of other data created or stored online. The Electronic Communications Privacy Act of 1986 does not require the government to get a warrant to collect the contents of your online communications that are over 180 days old. Further, the government claims that your web browsing history doesn't constitute communications contents, and thus is not subject to a warrant requirement, so long as it doesn't collect the data after the slash. In other words, the government asserts that it does not need a warrant to learn that you visited www.plannedparenthood.com, but it would need a warrant to learn that you visited its 'learn more: abortion' page. In the government's view, your contacts, buddy lists, and communication logs are also not protected by a warrant requirement. And the list goes on. Whether its data created by Internet of Things devices like Amazon Alexa and smart television sets or DNA databases held by companies like 23andMe or Ancestry.com, Carpenter leaves many other types of personal data in legal limbo.").; *See also* Maynard v. United States, 615 F.3d 544, 562-568 (D.C. Cir. 2010) (discussing the Mosaic Theory, which views collective government surveillance to constitute a search under the Fourth Amendment as it can reveal more about an individual's actions than one single or short terms observation).

[66] Tom Simonite, *Facebook Creates Software That Matches Faces Almost as Well as You Do,* MIT Technology Review, Mar. 17, 2014, https://www.technologyreview.com/s/525586/facebook-creates-software-that-matches-faces-almost-as-well-as-you-do/; *See generally, Technology – Deep Learning*, Herta, https://www.hertasecurity.com/en/technology.

[67] The Biometric Information Privacy Act (BIPA) requires that entities obtain affirmative consent from individuals before obtaining their biometric information and creates a private right of action for individuals to sue to enforce the law. BIPA and other state and federal laws and regulations are discussed in more detail in Section VI of this report "Legislation and Regulations Dealing with Facial Recognition Software and Biometrics" starting on pg. 14.

[68] Dana Herra, *Judge Tosses Illinois Privacy Law Class Action vs Facebook Over Photo Tagging,* The Cook County Record, Jan. 27, 2016, https://cookcountyrecord.com/stories/510660138-judge-tosses-illinois-privacy-law-class-action-vs-facebook-over-photo-tagging-california-cases-still-pending.

[69] In re Facebook Biometric Info. Privacy Litig., 326 F.R.D. 535, (N.D. Cal. 2018).

[70] Jennifer Lynch and Adam Schwartz, *Victory! Illinois Supreme Court Protects Biometric Privacy,* Electronic Frontier Foundation, Jan.25, 2019, https://www.eff.org/deeplinks/2019/01/victory-illinois-supreme-court-protects-biometric-privacy.

[71] *See generally,* Josh Constine, *$350B Face Data Lawsuit Against Facebook Will Proceed*, TechCrunch, Oct. 18, 2019, https://techcrunch.com/2019/10/18/facebook-35-billion-lawsuit/.

[72] Nicholas Iovino, *Facebook Fights $30 Billion Privacy Suit at Ninth Circuit,* Courthouse News Service, Jun. 12, 2019, https://www.courthousenews.com/facebook-fights-30-billion-privacy-suit-at-ninth-circuit/; Patel v. Facebook, Inc., 932 F.3d 1264, 1270 (9th Cir. 2019).; Friends of Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc., 528 U.S. 167, 180-181 (2000) (discussing how the Case or Controversy clause of Article III of the U.S. Constitution requires that a plaintiff has suffered "(1) an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical, (2) the injury must be fairly traceable to the challenged action of the defendant, and (3) it must be likely, as opposed to merely speculative, that this injury will be redressed by a favorable decision.").

[73] *Id*. at 1270-1273.

[74] Id. at 1273 (quoting Riley v. California, 573 U.S. 373 at 393 (2014) ("Technological advances provide 'access to a category of information otherwise unknowable,' and 'implicate privacy concerns' in a manner as different from traditional intrusions as 'a ride on horseback' is different from 'a flight to the moon . . .'").).

[75] Shannon Liao, *Facebook Hit with Four Lawsuits in One Week Over Cambridge Analytica Scandal,* The Verge, Mar. 23, 2018, https://www.theverge.com/2018/3/23/17155754/facebook-cambridge-analytica-data-breach-scandal.

[76] Carole Cadwalladr and Emma Graham-Harrison, *Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*, The Guardian, Mar. 17, 2018, https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election.

[77] *See* Ken Winterbottom, *Court Rules Police ay Compel Suspects to Unlock Fingerprint-Protected Smartphones,* Harvard Journal of Law & Technology, Nov. 12, 2014, https://jolt.law.harvard.edu/digest/court-rules-police-may-compel-suspects-to-unlock-fingerprint-protected-smartphones; *See* Jeff Welty, *Facial Recognition, Biometric Identification and the Fifth Amendment,* North Carolina Criminal Law Blog, (Sept. 18, 2017, 9:25 AM), https://nccriminallaw.sog.unc.edu/facial-recognition-biometric-identification-fifth-amendment/; *See* Bryanna Gutierrez, *Is Your Fingerprint the Golden Ticket for Police?,* Ristenpart Law, Apr. 13, 2017, https://ristenpartlaw.com/case-law-updates-posts/2017/4/11/protecting-fingerprint-scanning-against-unlocking-phones.

[78] *See* Matt Hamilton, *The Government Wants Your Fingerprint to Unlock Your Phone. Should That be Allowed?,* Apr. 30, 2016, The Los Angeles Times, https://www.latimes.com/local/california/la-me-iphones-fingerprints-20160430-story.html.

[79] Matter of Residence in Oakland, California, 354 F. Supp. 3d 1010, 1013 (N.D. Cal. 2019); *See* Thomas Brewster, *Feds Can't Force You to Unlock Your iPhone With Finger or Face, Judge Rules*, Forbes, Jan. 14. 2019, https://www.forbes.com/sites/thomasbrewster/2019/01/14/feds-cant-force-you-to-unlock-your-iphone-with-finger-or-face-judge-rules/#7323bbf042b7.

[80] *Id*. at 1016-1017.

[81] In re Application for a Search Warrant, 236 F. Supp. 3d 1066, (N.D. Ill. 2017).

[82] *Id*. at 1068-1069.

[83] *Id*. at 1071 (citing Fisher v. United States, 425 U.S. 391, 410 (1976).

[84] In re Application for a Search Warrant, *supra* note 81 at 1074.

[85] Matter of White Google Pixel 3 XL Cellphone in a Black Incipio Case, No. 1:19-MJ-10441-DCN, 2019 WL 3401990, at 1 (D. Idaho July 26, 2019).

[86] *Id*. at 4.

[87] *Id*. at 7.

[88] Commonwealth v. Baust, 89 Va. Cir. 267 (Va. Cir. Ct. 2014).

[89] *Id*. at 3 (citing United States v. Kirschner, 823 F.Supp.2d 665, 669 (E.D.Mich.2010)).

[90] Commonwealth v. Baust, *supra* note 88 at 3.; United States v. Wade, *supra* note 21 at 223.

[91] *Id*.; *See* Welty, *supra* note 77.

[92] State v. Diamond, 890 N.W.2d 143, 145 (Minn. Ct. App. 2017).

[93] *Id*. at 150-151.

[94] Florida v. Stahl, 206 So. 3d 124, 135 (Fla. Dist. Ct. App. 2016).

[95] Nathan Freed Wessler and Somil Trivedi, *Florida is Using Facial Recognition to Convict People Without Giving Them a Chance to Challenge the Technology,* ACLU, 2019, https://www.aclu.org/blog/privacy-technology/surveillance-technologies/florida-using-facial-recognition-convict-people; Aaron Mak, *Facing Facts*,

Slate, Jan. 25, 2019, https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html.

[96] *Id*. (discussing how during a deposition of the Jacksonville crime analyst who used FACES to obtain a "one star" match of the defendant, the crime analyst testified that FACES rates the quality of a match using a star system and that while the defendant had a one-star match, other potential matches had none. The analyst also did not know the maximum number of stars possible for a FACES match).

[97] Karen Gullo and Jennifer Lynch, *When Facial Recognition Is Used to Identify Defendants, They Have a Right to Obtain Information About the Algorithms Used on Them, EFF Tells Court*, Electronic Frontier Foundation, Mar. 12, 2019, https://www.eff.org/deeplinks/2019/03/when-facial-recognition-used-identify-defendants-they-have-right-obtain; *See* Lynch v. State, 260 So. 3d 1166 (Fla. Dist. Ct. App. 2018).

[98] Russell Brandom, *Facebook-backed Lawmakers are Looking to Gut Privacy Law*, The Verge, Apr. 10, 2018, https://www.theverge.com/2018/4/10/17218756/facebook-biometric-privacy-lobbying-bipa-illinois; Russell Brandom, *Crucial Biometric Privacy Law Survives Court Fight*, The Verge, Jan. 26, 2019 https://www.theverge.com/2019/1/26/18197567/six-flags-illinois-biometric-information-privacy-act-facial-recognition.

[99] *See* Rosenbach v. Six Flags, 2019 IL 123186 (Jan. 25, 2019).

[100] *Id*. at 38-39; Brandom, *supra* note 98.

[101] *Id*.

[102] Thomas F. Brier Jr. and Jeffrey N. Rosenthal, *Biometrics and the New Wave of Class Action Lawsuits,* The Legal Intelligence Mar. 1, 2019, https://www.law.com/thelegalintelligencer/2019/03/01/biometrics-and-the-new-wave-of-class-action-lawsuits/; *See* Jeffrey D. Neuburger, *Wow! Illinois Biometric Privacy Suits Proliferate,* The National Law Review, Sept. 27, 2017, https://www.natlawreview.com/article/wow-illinois-biometric-privacy-suits-proliferate; *See* Chris Burt, *EEF Urges Appeals Court to Side with Plaintiff Interpretation of Harm in Facebook Biometric Privacy Suit*, Biometric Update, Dec. 18, 2018, https://www.biometricupdate.com/201812/eff-urges-appeals-court-to-side-with-plaintiff-interpretation-of-harm-in-facebook-biometric-privacy-suit.

[103] *Id*.

[104] People v. Weaver, 12 N.Y.3d 433 (2009).

[105] *See* State v. Andrews, 457 N.J. Super. 14, 22-24 (App. Div. 2018) (discussing how if the government already knows that a defendant has a password to a device, then compelling the defendant to produce the password is not considered a testimonial act and thus not violate of the Fifth Amendment. Specifically, this occurs when (1) the Government has knowledge of the evidence, (2) the defendant possessed or controlled the evidence and (3) the evidence is authentic. In this case, the information provided by the defendant would be a "foregone conclusion.").

[106] *Id*. at 34; Commonwealth v. Baust, *supra* note 88.

[107] Thakkar, *supra* note 10.

[108] *Electronic Communications Privacy Act Primer*, cdt, May 13, 2015, https://cdt.org/insight/electronic-communications-privacy-act-primer/.

[109] *Electronic Communications Privacy Act Primer*, *supra* note 109.

[110] *Id*.

[111] 18 U.S.C. § 2703(d) (West).

[112] S.847 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/847/text.

[113] S.2968 – 116th Congress (2019-2020, https://www.congress.gov/bill/116th-congress/senate-bill/2968; *Consumer Online Privacy Rights Act of 2019*, Maria Cantwell United States Senator for Washington, https://www.cantwell.senate.gov/imo/media/doc/COPRA%20One-Pager.pdf.; Cantwell, Senate Democrats Unveil Strong Online Privacy Rights, 2019, https://www.cantwell.senate.gov/news/press-releases/cantwell-senate-democrats-unveil-strong-online-privacy-rights; Tony Romm, *Top Senate Democrats Unveil New Online Privacy Bill, Promising Tough Penalties for Data Abuse*, The Washington Post, Nov. 26, 2019, https://www.washingtonpost.com/technology/2019/11/26/top-senate-democrats-unveil-new-online-privacy-bill-promising-tough-penalties-data-abuse/.

[114] *Id*.

[115] *Id*.

[116] H.R. 4008 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/4008?s=1&r=7.

[117] *See* Todd Spangler, *Rep. Rashida Tlaib Sponsors Bill Cracking Down on Use of Facial Recognition Technology*, Detroit Free Press, Jul. 25, 2019, https://www.freep.com/story/news/local/michigan/2019/07/25/rep-rashida-tlaib-cracking-down-facial-recognition-technology/1824706001/; Harmon, *supra* note 33.

[118] S.1933 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/senate-bill/1933; H.R. 3377 – 116th Congress (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/3377/text?r=2&s=2.

[119] *Id*.

[120] *Id*.

[121] *Id*.

[122] *See*, H.R. 4008, *supra* note 116.

[123] National Institute of Standards and Technology (NIST), Face Recognition Vendor Test, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt; *See generally*, NIST, Topics, https://www.nist.gov/topics.

[124] NIST, Face Recognition Vendor Test – Ongoing, https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt-ongoing.

[125] *See* Kenn Brotman & Molly K. McGinley, *The Biometric Bandwagon Rolls On: Biometric Legislation Proposed Across the United States*, The National Law Review, Mar. 25, 2019, https://www.natlawreview.com/article/biometric-bandwagon-rolls-biometric-legislation-proposed-across-united-states.

[126] *Id*.

[127] *Several States Consider Laws Regulating the Collection of Biometric Data*, Lexology, Feb. 6, 2019, https://www.lexology.com/library/detail.aspx?g=a545aec6-37b8-49a8-8487-74b61883a0e1.

[128] 740 Ill. Comp. Stat. 14 (2008).

[129] Daniel Healow, Stuart D. Levi, Brian O'Connor, William Ridgway and James S. Talbot, , *Illinois Supreme Court Holds that Biometric Privacy Law Does Not Require Actual Harm for Private Suite,* Skadden, Jan. 29, 2019, https://www.skadden.com/insights/publications/2019/01/illinois-supreme-court.

[130] 740 Ill. Comp. Stat., *supra* note 128 at 14/10 & 15.

[131] 740 Ill. Comp. Stat., *supra* note 128 at 14/20(1).

[132] *Id*. at 14/20(2).

[133] *Id*. at 14/20(3).

[134] Tex. Bus. & Com. Code Ann. § 503.001 (West 2019).

[135] *Id*.

[136] Brotman & McGinley, *supra* note 126.

[137] Wash. Legis. Serv. Ch. 299 (S.H.B. 1493) (West).

[138] *Id*.

[139] *See* Bill Information, SB 5376-2019-20, Washington State Legislature, https://app.leg.wa.gov/billsummary?BillNumber=5376&Year=2019&Initiative=false.

[140] *Id*.

[141] *Id*.

[142] *See* HB 1071 - 2019-20 – Bill Information, Washington State Legislature, https://app.leg.wa.gov/billsummary?BillNumber=1071&Year=2019.

[143] *Id*; *See also*, *Washington's New Data Breach Law Follow Enhanced Privacy Protection* Trends, Thompson Hine, May 20, 2019, https://www.thompsonhine.com/publications/washingtons-new-data-breach-law-follows-enhanced-privacy-protection-trends.

[144] HB 1071, Washington State Legislature, http://lawfilesext.leg.wa.gov/biennium/2019-20/Pdf/Bills/House%20Passed%20Legislature/1071-S.PL.pdf (*see* specifically Sec. 1.(2)(a)(i)(I)).

[145] *Id*. at Sec. 2.(1) and (7).

[146] HB 1071, *supra* note 144 at Sec. 5.(7).

[147] *Id*. at Sec. 2.(1).

[148] *Id* at Sec. 1.(2).

[149] Issie Lapowsky, *California Unanimously Passes Historic Privacy Bill*, Wired, Jun. 28, 2018, https://www.wired.com/story/california-unanimously-passes-historic-privacy-bill/.

[150] Cal. Civ. Code § 1798.100 **(**West 2018).

[151] Lapowsky, *supra* note 149.

[152] Cal. Civ. Code, *supra* note 150.

[153] *Id*.

[154] *Id*.

[155] Lapowski, *supra* note 149; *See* JD *Amendments to California Consumer Privacy Act Head to Governor's Desk*, Supra, Sept. 6, 2018, https://www.jdsupra.com/legalnews/amendments-to-california-consumer-92796/.

[156] A.1911/S.1203, *supra* note 156.

[157] *Id*.

[158] A.1911/S.1203, 243rd Session (N.Y 2019), https://www.nysenate.gov/legislation/bills/2019/s1203 (introduced in 2018 at A.9793/S.8547).

[159] *NetChoice's Internet Advocates' Watchlist for Ugly Laws (iAWFUL) Targets Worst Bills and Laws for Online Consumers and Entrepreneurs,* April 4, 2018, NetChoice, https://netchoice.org/media-press/the-iawful-7-state-federal-and-international-legislation-placing-barriers-to-innovation-and-commerce/ (last visited Aug. 7, 2020).

[160] *See* 2019 N.Y. Laws ch. 117, *available at* https://www.nysenate.gov/legislation/bills/2019/s5575; N.Y. LAB. Law § 201-a (McKinney 2019).

[161] Annemaria Duran, *New York Employers Can Eliminate Buddy Punching With Biometric Time Clocks,* Swipeclock, Jan. 8, 2018, https://www3.swipeclock.com/blog/new-york-employers-can-eliminate-buddy-punching-biometric-time-clocks/.

[162] Chp. 117, *supra* note 158; *See New York SHEILD Act Expands Privacy and Cybersecurity Obligations,* Thompson Hine, Jul. 29, 2019, https://www.thompsonhine.com/publications/new-york-shield-act-expands-privacy-and-cybersecurity-obligations.

[163] Chp. 117, *supra* note 158.

[164] *Id*.

[165] *Id*.

[166] A.7790/S.5687, 243rd Session (N.Y. 2019), https://www.nysenate.gov/legislation/bills/2019/s5687.

[167] Elizabeth Elizalde and Michael Gartland, *Brooklyn Tenants in Rent-Regulated Apartments Push State to Nix Landlord's facial Recognition Software*, Daily News, May, 1, 2019, https://www.nydailynews.com/new-york/brooklyn/ny-facial-recognition-brownsville-nelson-20190501-5gb32fncjrcmvijwbriimwpcsa-story.html.

[168] *Id*.

[169] Some of this proposed legislation includes: A.235/S.2500 – Relates to the use of biometric data for marketing purposes; A.465 – Enacts the "personal information protection act"; A.1911/S.1203 – Establishes the biometric privacy act; A.2114 – Relates to identity theft; clarifies personal identifying information and what acts constitute the offense of identity theft; A.2614 – Establishes a driver safety course and a driver safety course fund; A.2830 – Establishes the Medicaid identification and anti-fraud biometric technology pilot program appropriation; A04030 – Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof; A.4076-B/S.4352-B – Relates to providing for electronic notarization; A.4299 – Relates to unlawfully purchasing or selling personal identifying information; A.5635-B/S.5575-B – Relates to a notification of a security breach; A.5757 – Relates to the use of biometric identity verification devices for the purchase of alcoholic beverages and tobacco products; A.6351/S.4411 – Allows consumers the right to request from businesses the categories of personal information a business has sold or disclosed to third parties; A.6787-D/S.5140-B – Relates to the use of biometric identifying technology; A.6788-B/S.5125-B – Relates to limitations on smart access systems for entry; A.7613/S.7724 – Relates to establishing the New York Data Protection Act; A.7736 – Establishes the "It's Your Data Act"; A.7913/S.5222 – Relates to the crimes of commercial bribery and larceny; A.8169 – Relates to protecting personal information; A.8526/S.5642 – Relates to enacting the NY privacy act; S.1749 – Relates to creating a private right of action for the breach of a consumer's identifying information; A.10725/S.1844 – Establishes and redefines offenses involving fraud, scheme to defraud and larceny; S.5146 – Relates to offenses involving thefts of identity; S.6007 – Relates to the use of biometric identity verification devices for the purchase of alcoholic beverages and tobacco products; S.6776 – Relates to prohibiting facial recognition technology to be used in connection with an officer camera; A.1692 – Prohibits the state, state agencies and departments and contractors doing business with the state, its agencies or departments from retaining facial recognition images; A.4030 – Regulates the use of unmanned aerial vehicles by the state and political subdivisions thereof; A.7790/S.5687 – Prohibits the use of a facial recognition system by a landlord on any residential premises; A.8042/S.6623 – Enacts the "facial recognition technology study act; A.8373 – Prohibits the use of a facial recognition system by any person on public school premises; A.9931-A/S.6435-B – Imposes limitations on the use of drones for law enforcement purposes; S.6776 – Relates to prohibiting facial recognition technology to be used in connection with an officer camera. Relevant bill text can be accessed through https://www.nysenate.gov/search/legislation.

[170] A.9767/S.7572, 243rd Session (N.Y 2020), https://www.nysenate.gov/legislation/bills/2019/s7572.

[171] *Id*.

[172] *See* The New York State Assembly, *supra* note 169.

[173] HB 1943, Arkansas State Legislature, http://www.arkleg.state.ar.us/assembly/2019/2019R/Bills/HB1943.pdf.

[174] *Id*.

[175] Katie Lannan, *Sommerville Bans Government Use of Facial Recognition Technology*, wbur, Jun. 28, 2019, https://www.wbur.org/bostonomix/2019/06/28/somerville-bans-government-use-of-facial-recognition-tech.

[176] Kate Conger, Richard Fausset and Serge F. Kovaleski, *San Francisco Bans Facial Recognition Technology,* The New York Times, May 14, 2019, https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html; *See* Harwell, *supra* note 13.

[177] *Id*.; Harwell, *supra* note 13.; Rachel Metz, *Beyond San Francisco, More Cities Are Saying No To Facial Recognition*, CNN Business, Jul. 17, 2019, https://www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.

[178] *Id*.

[179] Sarah Wu, *Sommerville City Council Passes Facial Recognition Ban,* The Boston Globe, https://www.bostonglobe.com/metro/2019/06/27/somerville-city-council-passes-facial-recognition-ban/SfaqQ7mG3DGulXonBHSCYK/story.html.

[180] Tom McKay, *Berkeley Becomes the Fourth U.S. City to Ban Face Recognition in Unanimous Vote*, Gizmodo, Oct. 16, 2019, https://www.msn.com/en-us/news/technology/berkeley-becomes-fourth-us-city-to-ban-face-recognition-in-unanimous-vote/ar-AAIRKiD.

[181] Local Law No. 65 (2020) of City of New York, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0&Options=ID|Text|&Search=0487. .

[182] *Id*.

[183] *Id*.

[184] *See* Council of City of NY Int. 1170-2018, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3704369&GUID=070402C0-43F0-47AE-AA6E-DEF06CDF702A&Options=&Search=.

[185] *Id*. (describing how Int. 1170-2018 defines "biometric identifier information" as ". . . a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, any of which is collected, retained, converted, stored or shared to identify an individual." The Bill also requires (1) businesses to provide conspicuous notice that biometric data is being collected and (2) make available online, "1. The amount of time for which the commercial establishment retains or stores biometric identifier information; 2. The kind of biometric identifier information the commercial establishment collects, retains, converts, stores or shares from its customers; 3. Any privacy policy governing, and any purpose for, the commercial establishment's collection, retention, conversion, storage or sharing of biometric identifier information of customers, including but not limited to, any protective measures the commercial establishment utilizes to safeguard biometric identifier information; and 4. Whether the commercial establishment shares biometric identifier information with third-parties.").

[186] Int. 1170-2018, *supra* note 184.

[187] *Id*.

[188] *Id*.

[189] *Id*.

[190] Stephanie Kapinos, *New York City Considers Facial Recognition Bill – Will New York Be the Next Forum for Biometric Privacy Litigation?,* Proskauer – New Media and Technology Law Blog, Jan. 31, 2019, https://newmedialaw.proskauer.com/2019/01/31/new-york-city-considers-facial-recognition-bill-will-new-york-be-the-next-forum-for-biometric-privacy-litigation/.

[191] *See* Council of City of NY Int. 1758-2019, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4085862&GUID=1D415200-95B9-440B-AE2B-F0B5F9668B0A&Options=&Search=.

[192] *Id*.

[193] *Id*.

[194] *See* Council of City of NY Int. 1672-2018, https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=4146261&GUID=435ECCD7-D2E0-4029-AEB2-3167FB9F6714&Options=&Search=.

[195] *Id*.

[196] *See 2018 Reform of EU Data Protection Rules*, European Commission, https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en#abouttheregulationanddataprotection.

[197] *Id*.

[198] Regulation 2016/679, Art. 1, 2016 O.J. (L 127) (EU).

[199] *Id*. at Art. 4, 1.

[200] *See* Data Protection Act, 2018, c. 12 (U.K.).

[201] Big Brother Watch, *supra,* note 25 at 47.

[202] Madhunita Murgia, *London Could Shape the Future of Facial Recognition,* OZY, Aug. 5, 2019, https://www.ozy.com/fast-forward/london-could-shape-the-future-of-facial-recognition/95951/.

[203] *Id*.

[204] James Vincent, *The Tech Industry Doesn't Have a Plan for Dealing with Facial Bias*, The Verge, Jul. 26, 2018, https://www.theverge.com/2018/7/26/17616290/facial-recognition-ai-bias-benchmark-test; Stephen Mayhew, *Police in China Using Facial Recognition Glasses*, Biometric Update, Feb. 7, 2018, https://www.biometricupdate.com/201802/police-in-china-using-facial-recognition-glasses.

[205] *Chinese Facial Recognition Tech Installed in Nations Vulnerable to Abuse*, CBS News, Oct. 16, 2019, https://www.cbsnews.com/news/china-huawei-face-recognition-cameras-serbia-other-countries-questionable-human-rights-2019-10-16/.

[206] *Id*.

[207] *Id*.

[208] *Chinese Facial Recognition Tech Installed in Nations Vulnerable to Abuse*, *supra* note 206.

[209] Id.; *See also*, Sharon Weinberger, *Private Surveillance Is a Lethal Weapon Anyone Can Buy*, The New York Times, Jul. 19, 2019, https://www.nytimes.com/2019/07/19/opinion/private-surveillance-industry.html?action=click&module=Opinion&pgtype=Homepage (discussing how large American tech companies and defense contractors have also sold biometric surveillance tools to foreign governments for purposes of spying on their citizens and instituting human rights violations; the selling of biometric surveillance technology to governments has become a multibillion-dollar industry.).

[210] *See generally*, *About UIDAI*, Unique Identification Authority of India, https://uidai.gov.in/about-uidai/unique-identification-authority-of-india/about.html.

[211] Id.; *See* The Aadhaaar (Targeted Delivery of Financial And Other Subsidies, Benefits and Services) Act, No. 18 of 2016.

[212] Reetika Khera, *These Digital IDs Have Cost People Their Privacy – and their Lives,* The Washington Post, Aug. 9, 2018, https://www.washingtonpost.com/news/theworldpost/wp/2018/08/09/aadhaar/?utm_term=.6273ab2e1fcc; *See* Pranav Rai, *The Indian Supreme Court's Aadhaar Judgement – A Privacy Analysis,* IAPP, Oct. 9, 2018, https://iapp.org/news/a/the-indian-supreme-courts-aadhaar-judgement-a-privacy-perspective/.

[213] Woodrow Hartzog and Evan Selinger, *Facial Recognition is the Perfect Tool for Oppression*, The Medium, 2017, https://medium.com/s/story/facial-recognition-is-the-perfect-tool-for-oppression-bc2a08f0fe66; Woodrow Hartzog & Evan Selinger, *Why We Must Ban Facial Recognition Software Now*, The New York Times, Oct. 17. 2019, https://www.nytimes.com/2019/10/17/opinion/facial-recognition-ban.html; *See* Evan Greer, *Opinion: Don't Regulate Facial Recognition. Ban It.*, BuzzFeed, Jul. 18, 2019, https://www.buzzfeednews.com/article/evangreer/dont-regulate-facial-recognition-ban-it.

[214] Hartzog and Evan Selinger, *supra* note 214.; Hartzog and Evan Selinger, *supra* note 214.; Greer, *supra* note 214.

[215] Anna Parsons, *Why a Blanket Ban of Facial Recognition Technology Would be Bad Policy*, The Hill, Sept. 16. 2019, https://thehill.com/blogs/congress-blog/technology/461618-why-a-blanket-ban-of-facial-recognition-technology-in-schools.

[216] Vincent, *supra* note 205.; James Vincent, *IBM Hopes to Fight Bias in Facial Recognition with New Diverse Dataset*, The Verge, Jun. 27, 2018, https://www.theverge.com/2018/6/27/17509400/facial-recognition-bias-ibm-data-training.

[217] *See generally,* FATE - Fairness Accountability, Transparency and Ethics in AI, Microsoft, https://www.microsoft.com/en-us/research/group/fate/ (one example of a company making efforts to combat bias in its biometric software).

[218] Nick Statt, *Amazon Told Employees it Would Continue to Sell Facial Recognition Software to Law Enforcement*, The Verge, Nov. 11, 2018, https://www.theverge.com/2018/11/8/18077292/amazon-rekognition-jeff-bezos-andrew-jassy-facial-recognition-ice-rights-violations.

[219] *Id*.

[220] Michael Punke, *Some Thoughts on Facial Recognition Legislation,* AWS Machine Learning Blog (Feb. 7, 2019) https://aws.amazon.com/blogs/machine-learning/some-thoughts-on-facial-recognition-legislation/.

[221] Nick Statt and James Vincent, *Google Pledges Not to Develop AI Weapons, but Says it Will Still Work with the Military*, The Verge, Jun. 7, 2019, https://www.theverge.com/2018/6/7/17439310/google-ai-ethics-principles-warfare-weapons-military-project-maven; *Artificial Intelligence at Google – Our Principals,* Google, https://ai.google/principles.

[222] *Id*.

[223] IIIE, *Ethics in Action*, https://ethicsinaction.ieee.org/.

[224] *See generally* Algorithmic Justice League, https://www.ajlunited.org/.

[225] Kevin McCarthy, *Don't Count on Governments to Protect Your Privacy,* The New York Times, Jul. 14, 2019, https://www.nytimes.com/2019/07/14/opinion/kevin-mccarthy-privacy-blockchain.html.

[226] Id.

[227] *See generally,* Karen Weise and Natasha Singer, *Amazon Pauses Police Use of Its Facial Recognition Software*, The New York Times, Jun. 10, 2020, https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html?auth=login-email&login=email; Hannah Klein, *IBM Says It Will Stop Developing Facial Recognition Tech Due to Racial Bias,* Slate, Jun. 9, 2020, https://slate.com/technology/2020/06/ibm-facial-recognition-racial-bias.html; Nathan Sheard, *Victory! New York's City Council Passes the POST Act,* Electronic Frontier Foundation, Jun. 18, 2020, https://www.eff.org/deeplinks/2020/06/victory-new-yorks-city-council-passes-post-act. (In the wake of worldwide protests stemming from the May 2020 killing of George Floyd - an unarmed African American man who died of asphyxiation after a Minneapolis police officer refused to remove his knee from Mr. Floyd's neck as he lay face down in handcuffs repeatedly pleading "I can't breathe" - several private sector companies, including Amazon and IBM, publicly stated that they would halt their development of facial recognition software due to concerns over racial bias and the use of their software by law enforcement. Relatedly, some municipalities have recently passed laws regulating law enforcement's use of personal data: just weeks after George Floyd's killing, the New York City Council passed the POST Act (*see supra* note 181). We must continue to build on the momentum of this moment and craft comprehensive legislative and policy reforms aimed at eradicating racial bias from facial recognition and other biometric technology).

[228] Vincent, *supra* note 205.

[229] *See* Angela Chen, *How to Kick Facial Recognition Out of Your Town*, MIT Technology Review, Oct. 4, 2019, https://www.technologyreview.com/s/614477/facial-recognition-law-enforcement-surveillance-private-industry-regulation-ban-backlash/.

Compelled Decryption and the Privilege Against Self-Incrimination

Orin S. Kerr*

This Essay considers the Fifth Amendment barrier to orders compelling a suspect to enter in a password to decrypt a locked phone, computer, or file. It argues that a simple rule should apply: an assertion of privilege should be sustained unless the government can independently show that the suspect knows the password. The act of entering a password is testimonial, but the only implied statement is that the suspect knows the password. When the government can prove this fact independently, the assertion is a foregone conclusion and the Fifth Amendment poses no bar to the enforcement of the order. This rule is both doctrinally correct and sensible policy. It properly reflects the distribution of government power in a digital age when nearly everyone is carrying a device that comes with an extraordinarily powerful lock.

*Frances R. and John J. Duggan Distinguished Professor, University of Southern California Gould School of Law. Thanks to Sasha Natapoff, Laurent Sacharoff, Kevin Cole, Riana Pfefferkorn, Leah Litman, Jonathan Glater, Cristine Scott-Hayward, Robert Graham, Tracey Maclin, and participants at the Southern California Criminal Justice Roundtable for comments on an earlier draft.

Introduction

Encryption is everywhere. Ninety-four percent of Americans aged eighteen to twenty-nine carry smartphones, many of which encrypt their data by default when not in use.[1] Laptops, tablet computers, and thumb drives can be and often are encrypted.[2] Although users can decrypt electronic devices in different ways, one popular method is to enter a password.[3] To unlock the device and decrypt its contents, a person must type in a unique combination of characters that acts as the key and unlocks the device.

The widespread use of encryption has triggered an increasingly common Fifth Amendment question in criminal investigations: When can the government require a suspect to decrypt an encrypted device by entering the password?[4] The issue typically arises when investigators have a warrant to search a cell phone or computer, but they cannot execute the search because the data is encrypted. Investigators obtain a court order directing a suspect to produce a decrypted version of the data by entering the password without disclosing it to the government. The suspect then objects, claiming a Fifth Amendment privilege against complying with the order.[5]

The difficult legal question is how a court should rule on the assertion of privilege: When is the order enforceable, and when would enforcing the

---

1. *See Mobile Fact Sheet*, PEW RESEARCH CTR.: INTERNET & TECH. (Feb. 5, 2018), http://www.pewinternet.org/fact-sheet/mobile/ [https://perma.cc/K876-Z2JM] (reporting that 94% of those aged eighteen to twenty-nine own a smartphone).

2. *See generally* Whitson Gordon, *The One Thing That Protects a Laptop After It's Been Stolen*, N.Y. TIMES (Mar. 13, 2018), https://www.nytimes.com/2018/03/13/smarter-living/how-to-encrypt-your-computers-data.html [https://perma.cc/XB2S-9WTU] (describing how to encrypt a laptop computer or individual computer file).

3. I use the term "password" here broadly to refer to any string of numbers, letters, or other characters that can be typed in to access data. Therefore, I will label passcodes, passwords, and passphrases all as passwords. *See* Orin Kerr & Bruce Schneier, *Encryption Workarounds*, 106 GEO. L.J. 989, 994 n.24 (2018) (noting the technical differences among passcodes, passwords, and passphrases).

4. Recent cases that have addressed this question include *In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011*, 670 F.3d 1335, 1349 (11th Cir. 2012) (declaring that the government could not compel decryption); *United States v. Apple MacPro Computer*, 851 F.3d 238, 248 & n.7 (3d Cir. 2017) (allowing compelled decryption), *cert. denied*, 138 S. Ct. 1988 (2018) (mem.); *United States v. Spencer*, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) (same); *United States v. Fricosu*, 841 F. Supp. 2d 1232, 1237 (D. Colo. 2012) (same); *United States v. Mitchell II*, 76 M.J. 413, 424–25 & n.5 (C.A.A.F. 2017) (Ryan, J., dissenting) (same, in dissenting opinion); *State v. Stahl*, 206 So. 3d 124, 136–37 (Fla. Dist. Ct. App. 2016) (same); *Seo v. State*, 109 N.E.3d 418, 425–31 (Ind. Ct. App. 2018) (not allowed), *transfer granted, opinion vacated*, 2018 WL 6565988 (Ind. Dec. 6, 2018); and *Commonwealth v. Gelfgatt*, 11 N.E.3d 605, 614–15 (Mass. 2014) (allowed).

5. *See* cases cited *supra* note 4. This Essay solely addresses the Fifth Amendment framework for compelling acts of decryption by entering a password without disclosing it to the government. Compelled use of biometrics and compelled disclosure of passwords raise different Fifth Amendment issues. *See* Kerr & Schneier, *supra* note 3, at 1001–04 (summarizing the different ways of compelling action from suspects to decrypt data on their devices).

order violate the right against self-incrimination? Put another way, how much power does the government have to compel a person to decrypt a device by entering a password? About a dozen court decisions have grappled with this question in the last decade.[6] Courts have disagreed on the correct answer,[7] as have scholars,[8] with both offering a range of standards for how the Fifth Amendment privilege should apply.[9]

This Essay answers that question in two ways. First, it offers a simple doctrinal rule that explains how the Fifth Amendment should apply. Expanding on my online writings about this subject,[10] this Essay argues that the Fifth Amendment poses no barrier to compelled decryption as long as the government has independent knowledge that the suspect knows the password and the government presents the password prompt to decrypt the device to the suspect. When a suspect is presented with a password prompt and is ordered to enter in the password, the only implied testimony in complying is

6. *See* cases cited *supra* note 4.

7. *Compare In re Grand Jury Subpoena Duces Tecum*, 670 F.3d at 1349 (holding that the privilege applies unless the government can describe the incriminating files that are on the device with reasonable particularity), *with Spencer*, 2018 WL 1964588, at *3 (holding that the privilege does not apply when the government can show the suspect has the ability to decrypt the device).

8. As Professor Sacharoff has recently explained, this is a "fundamental question bedeviling courts and scholars." Laurent Sacharoff, *Unlocking the Fifth Amendment: Passwords and Encrypted Devices*, 87 FORDHAM L. REV. 203, 207 (2018).

9. The scholarship on this question divides roughly between those who would interpret the Fifth Amendment as imposing a high bar to compelling a password and those who would interpret the Fifth Amendment as imposing a low bar. *Compare* Aaron M. Clemens, *No Computer Exception to the Constitution: The Fifth Amendment Protects Against Compelled Production of an Encrypted Document or Private Key*, UCLA J.L. & TECH., Spring 2004, at 1, 11 (high bar), Sacharoff, *supra* note 8, at 251 (same), *and* Jason Wareham, Note, *Cracking the Code: The Enigma of the Self-Incrimination Clause and Compulsory Decryption of Encrypted Media*, 1 GEO. L. TECH. REV. 247, 268 (2017) (same), *with* Joseph Jarone, Comment, *An Act of Decryption Doctrine: Clarifying the Act of Production Doctrine's Application to Compelled Decryption*, 10 FLA. INT'L U. L. REV. 767, 797 (2015) (low bar), Dan Terzian, *The Fifth Amendment, Encryption, and the Forgotten State Interest*, 61 UCLA L. REV. DISCOURSE 298, 300 (2014) (same), *and* Timothy A. Wiseman, *Encryption, Forced Decryption, and the Constitution*, 11 I/S: J.L. & POL'Y FOR INFO. SOC'Y 525, 526 (same). I have also written several blog posts on this subject that argue for a low bar. See *infra* note 10 for a discussion of those posts.

10. In 2015 and 2016, I wrote several blog posts for the Volokh Conspiracy blog on the Fifth Amendment limits to decryption. In light of the continuing significance of the issue, it seemed worthwhile to expand on those posts. As a result, Part II of this Essay is a greatly expanded version of arguments I have presented at the Volokh Conspiracy blog. The two most relevant blog posts are: Orin Kerr, *The Fifth Amendment Limits on Forced Decryption and Applying the 'Foregone Conclusion' Doctrine*, WASH. POST (June 7, 2016) [hereinafter Kerr, *Fifth Amendment Limits on Forced Decryption*], https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/06/07/the-fifth-amendment-limits-on-forced-decryption-and-applying-the-foregone-conclusion-doctrine [https://perma.cc/5ZHA-DH3C] and Orin Kerr, *Fifth Amendment Protects Passcode on Smartphones, Court Holds*, WASH. POST (Sept. 24, 2015) [hereinafter Kerr, *Fifth Amendment Protects Passcode on Smartphones, Court Holds*], https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/09/24/fifth-amendment-protects-passcode-on-smartphones-court-holds [https://perma.cc/DDU3-6FAV] (cited in *Spencer*, 2018 WL 1964588, at *3 n.2).

that the suspect knows the password. That testimony will be a foregone conclusion that defeats the assertion of the privilege when the government can independently show that the person already knows the password.

My approach explains why the only federal appellate decision that squarely answers this issue, the Eleventh Circuit's 2012 decision in *In Re Grand Jury Subpoena Duces Tecum*,[11] either is wrongly decided or else is very confusingly reasoned. The Eleventh Circuit appears to have held that the government can compel decryption only when it can first describe with reasonable particularity what decrypted files will be found on the device.[12] This holding is incorrect. It erroneously equates the act of decrypting a device with the act of collecting and handing over the files it contains. The two acts may seem similar at first, but they have very different Fifth Amendment implications.

The Essay next goes beyond doctrine and offers a broader perspective. In recent criminal procedure cases such as *Carpenter v. United States*,[13] the Supreme Court has signaled a willingness to rethink old constitutional doctrines in light of technological change. Instead of applying old doctrines mechanically, the Court has suggested that courts should reconsider old rules in light of how technology has shifted the balance of government power—a process I have elsewhere called "equilibrium-adjustment."[14] To the extent equilibrium-adjustment extends to the Fifth Amendment, beyond the Fourth Amendment sphere where it originated, cases like *Carpenter* hint that the Fifth Amendment framework for compelled decryption should look beyond precedent to the normative question: What Fifth Amendment rule offers an appropriate test in light of the role of encryption in modern life?

Here the correct doctrine is also the appropriate rule. Technology has given almost every citizen a technological tool unimaginable decades earlier. Today almost everyone carries their records in an electronic box that can be very difficult or even impossible for the government to break open. Strong encryption for everyone shifts the balance of power towards the citizen and away from the state. Before the spread of strong encryption, the search process only presented Fourth Amendment issues. Today the search process raises Fourth Amendment issues plus technological barriers plus the prospect of a Fifth Amendment bar. The result is a reverse-*Carpenter*. To the extent the doctrine is unclear, courts should interpret the Fifth Amendment so that the technology does not dramatically shift the balance of power too much against the public interest in investigating crime.[15]

---

11. 670 F.3d 1335 (11th Cir. 2012).

12. *See infra* notes 86–95 and accompanying text.

13. 138 S. Ct. 2206 (2018).

14. *See generally* Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011) (introducing the concept in the Fourth Amendment context).

15. *See infra* subpart III(B).

The Essay proceeds in three parts. Part I explains the Supreme Court's case law on the Fifth Amendment implications of compelled acts, namely the act of production doctrine and the foregone conclusion doctrine. Part II applies these doctrines to compelled decryption and explains the apparent errors in the Eleventh Circuit's decision. Part III takes a broader view and argues that its proposed doctrinal rule offers an appropriate test in light of the role of encryption in modern life.

I. Acts of Production and the Foregone Conclusion Doctrine

The Fifth Amendment states that "[n]o person . . . shall be compelled in any criminal case to be a witness against himself . . . ."[16] This Part presents an overview of the relatively specific aspect of Fifth Amendment doctrine raised by government efforts to compel the entering of a password. The framework, established in *Fisher v. United States*,[17] deals with government compulsion of acts that lead to governmental knowledge of nontestimonial information. It has two parts. The first part, the act of production doctrine, assesses whether a compelled act is testimonial.[18] The second part, the foregone conclusion doctrine, nonetheless permits compelled testimonial acts when their testimonial content is already known.[19] This Part explains the two doctrines. It then explains how the two doctrines fit together by introducing the idea of distinguishing between door-opening evidence and treasure in criminal investigations.[20]

A. The Act of Production Doctrine

The privilege against self-incrimination applies when three conditions are met.[21] First, the person must face legal compulsion to cooperate with the government.[22] Second, the compelled conduct must be testimonial, which means that it must force a person "to disclose the contents of his own mind" and therefore communicate a "factual assertion" or "convey[] information to the Government."[23] Third, the compelled testimony must be incriminating, which means that the prospect of complying "must establish reasonable ground to apprehend danger to the witness from his being compelled to answer[.]"[24] A court must recognize an individual's privilege and block the

16. U.S. CONST. amend. V.

17. 425 U.S. 391 (1976).

18. *See infra* subpart I(A).

19. *See infra* subpart I(B).

20. *See infra* subpart I(C).

21. Hiibel v. Sixth Judicial Dist. Court, 542 U.S. 177, 189 (2004).

22. *Id.*

23. Doe v. United States, 487 U.S. 201, 208, 210–11, 215 (1988).

24. *Hiibel*, 542 U.S. at 190 (quoting Brown v. Walker, 161 U.S. 591, 599 (1896)) (internal quotations omitted).

government's effort to compel compliance only when all three conditions are satisfied.[25]

The act of production doctrine considers when a compelled act is testimonial. An act is testimonial, the doctrine holds, when the act implies "tacit averments" that have "communicative aspects."[26] The basic idea is that complying with an order to *do* something can send a message just like complying with an order to *say* something. For example, say I want to find out who in my Criminal Procedure class has already taken Evidence. I can ask the class that question and let them answer in words. Alternatively, I can ask those who have taken Evidence to raise their hands. In context, the act of raising a hand communicates the same fact as saying "yes."

The act of production doctrine was first adopted in *Fisher*.[27] The case considered whether it would be testimonial for a taxpayer to respond to an IRS summons seeking certain tax documents prepared by the taxpayer's accountant on Fisher's behalf.[28] According to the Court, the act of handing over papers in response to the summons implicitly testified about three different beliefs.[29] First, it implicitly testified that the requested documents existed; second, it implicitly testified that the documents were in the person's possession; and third, it implicitly testified that the papers handed over were the documents requested.[30]

It's important to see why these three testimonial statements are implicit in the act of compelled production. An act of compliance with an order implies two kinds of beliefs. First, it implies beliefs that are necessary to comply with the order.[31] Second, an act of compliance communicates the person's belief that the act amounts to compliance.[32] In *Fisher*, producing

25. *Id.* at 189.

26. Fisher v. United States, 425 U.S. 391, 410 (1976).

27. *See id.* ("The act of producing evidence in response to a subpoena . . . has communicative aspects of its own . . . .").

28. In a confusing twist of *Fisher*, this was only a hypothetical question in that case. *Fisher* consolidated two cases in which the government issued summons for tax documents held by the parties' attorneys. *Id.* at 393–94. In one of the cases, No. 74-611, the attorney invoked the attorney–client privilege as a basis for refusing to comply with the summons. *Id.* at 395. The parties stipulated that whether the attorney–client privilege provided a lawful basis for refusal to comply was answered by whether the client would have had a valid Fifth Amendment privilege against complying with the summons if, hypothetically, he had possessed the documents and if the summons had been directed at *him*. *Id.* at 402–05 & n.8. Thus, the "facts" of *Fisher* are really a hypothetical that was answered as a result of the parties' stipulation. To simplify matters, I will simply refer to this hypothetical as the "facts of *Fisher*" and refer to the client as "Fisher."

29. *Id.* at 410.

30. *Id.*

31. That is, if doing act X requires knowing fact Y, then doing act X implies that the person knows fact Y.

32. Courts label this the "act of production" doctrine because it typically applies to government orders to produce items sought by the government. The doctrine applies more broadly, however, to determine the testimony implicit in government-compelled action.

papers in response to an order to disclose certain tax documents implies a belief that the tax documents exist because you can't hand over papers that you don't think exist. Producing them implies a belief that you possess the documents because you can't hand over what you don't think you possess. The act of production implies a belief that the papers are the tax documents requested because the production was presented as an act of compliance.[33] The act of production implicitly states, "I think these are the documents you seek." It exposes the person's thoughts about the documents' existence, possession, and authenticity.

B. The Foregone Conclusion Doctrine

That brings us to the second part of *Fisher*'s framework, the foregone conclusion doctrine. The foregone conclusion doctrine teaches that when the testimonial aspect of a compelled act "adds little or nothing to the sum total of the Government's information,"[34] any implied testimony is a "foregone conclusion"[35] and compelling it does not violate the Fifth Amendment. To apply the foregone conclusion doctrine, courts look at what the government knows before the act is compelled and ask whether the testimony implied by a compelled act is "in issue" and would add to the government's case.[36] A valid privilege exists only when the compelled act is testimonial under the act of production doctrine but is not a foregone conclusion.

The best way to understand the foregone conclusion doctrine is to study *Fisher*. The Court held that the testimony implicit in handing over the tax documents was a foregone conclusion because the government was "in no way relying on the 'truthtelling' of the taxpayer" to prove it.[37] The documents "belong[ed] to the accountant, were prepared by him, and [we]re the kind usually prepared by an accountant working on the tax returns of his client."[38] As a result, Fisher's concession that he had the documents "add[ed] little or nothing to the sum total of the Government's information[.]"[39]

Further, Fisher's implied statement that the documents were authentic was insufficient because that implied statement did not give the government an advantage at trial.[40] "The documents would not be admissible in evidence against the taxpayer without authenticating testimony," the Court noted, and Fisher's implied statement that he believed the documents were what the

33. Production would be a "voucher of their genuineness." People v. Defore, 150 N.E. 585, 590 (N.Y. 1926) (Cardozo, J.) (quoted in *Fisher*, 425 U.S. at 412–13 n.12).

34. *Fisher*, 425 U.S. at 411.

35. *Id.*

36. *Id.* at 412.

37. *Id.* at 411.

38. *Id.*

39. *Id.*

40. *Id.* at 413.

government claimed was insufficient to authenticate them.[41] Fisher had not prepared the papers himself, and for purposes of authenticating documents he "could not vouch for their accuracy."[42] He was therefore not competent to authenticate the documents,[43] and his implied assertion that he believed the documents were authentic was simply his belief and not a sufficient basis to admit the documents at trial.

Three aspects of the foregone conclusion doctrine remain surprisingly unclear. The first uncertainty is whether the foregone conclusion doctrine concerns whether the implied testimony is incriminating or whether it is testimonial. *Fisher* provides no obvious answer. Because the compelled testimony implicit in the act was a foregone conclusion, *Fisher* states that the act "would involve no incriminating testimony within the protection of the Fifth Amendment."[44] In my view, the doctrine is better understood as concerning whether implied testimony is incriminating. The inquiry focuses on what the government knows and can otherwise prove, which doesn't change the implied statement in the act but does change whether making that implied assertion itself poses a danger to the speaker in context. But however it is characterized, the doctrine focuses on prosecutorial advantage. If the government already knows the fact or belief that is implicitly asserted, and it has some other way to prove it, then it gains no testimonial advantage by obtaining the defendant's assertions implicit in his compelled acts.

A second uncertainty about the foregone conclusion doctrine is the burden of proof to establish that a conclusion is foregone. The cases are surprisingly murky.[45] On one hand, courts are clear that the burden rests with the government.[46] On the other hand, there is no clear answer to how much certainty the government must establish. As Judge Calabresi recently noted

41. *Id.*

42. *Id.*

43. *Id.* The bookend to *Fisher*'s application of the foregone conclusion was provided decades later in *United States v. Hubbell*, 530 U.S. 27 (2000). Hubbell had been required to fully disclose his business and tax dealings as part of a prior plea agreement. *Id.* at 30. In a later effort to prove that Hubbell had not complied fully with that requirement, the government subpoenaed a wide range of documents from Hubbell relating to his finances. *Id.* at 30–31. Hubbell responded by producing 13,120 pages of documents, from which the government showed that Hubbell had in fact violated his earlier deal. *Id.* at 31. The Supreme Court ruled that the foregone conclusion doctrine did not apply and that Hubbell had a valid privilege against complying with the subpoena: "[T]he Government has not shown that it had any prior knowledge of either the existence or the whereabouts of the 13,120 pages of documents ultimately produced by respondent." *Id.* at 45.

44. *Fisher*, 425 U.S. at 414 ("We do hold that compliance with a summons directing the taxpayer to produce the accountant's documents involved in these cases would involve no incriminating testimony within the protection of the Fifth Amendment.").

45. *See generally* WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 8.13(a) (4th ed. 2015) (noting the uncertainty).

46. *See, e.g.*, *In re* Grand Jury Proceedings, Subpoenas for Documents, 41 F.3d 377, 380 (8th Cir. 1994) ("The government . . . bears the burdens of production and proof on the questions of . . . possession[] and existence of the summoned documents.").

for the Second Circuit, "[B]oth our court and our sister circuits have struggled with the extent of Government knowledge necessary for a foregone-conclusion rationale to apply."[47] The apparent cause of the uncertainty is that the cases typically arise when the government orders a suspect to turn over a described category of documents. In that context, courts have tended to express the burden in terms of the specificity of the government's description of the documents sought rather than the certainty of the government's knowledge.

The most-often-mentioned standard is that the foregone conclusion doctrine applies if the government establishes its knowledge of the testimonial aspects of production "with reasonable particularity."[48] The basic idea is that a specific description of what the government seeks necessarily reflects greater government knowledge about it. If the government's specific description of the documents to be handed over shows that the government already knows their existence, possession, and authenticity—the testimonial aspect of production—then the foregone conclusion doctrine applies.[49] If the government can pinpoint what it needs, the thinking runs, then it is not relying on the truth-telling of the person complying with the order to figure out its case.

Whatever the merits of the "reasonable particularity" standard in the specific context of subpoenaed documents, the test is notably unilluminating as to the government's burden outside that context. The government can compel an act that has testimonial qualities, but the standard does not require the government to describe the evidence it is seeking. The act may be to do something, not to go get something. As a result, there may be no evidence for the target to retrieve that can be described with "reasonable particularity." The burden of proof in contexts outside of orders to compel documents remains surprisingly unclear.

A final uncertainty with the foregone conclusion doctrine is whether the government can introduce the defendant's testimonial act at trial. Here's the question: If the government orders a testimonial act as part of the investigation, and it then overcomes an assertion of privilege by showing that it has independent knowledge of the implied testimony that renders it a foregone conclusion, can the government later tell the jury about the defendant's implied testimony to help prove the defendant's guilt? Or is the government barred from relying at trial on testimonial foregone conclusions?[50]

---

47. United States v. Greenfield, 831 F.3d 106, 116 (2d Cir. 2016).

48. *Id.* (quoting *In re* Grand Jury Subpoena Duces Tecum Dated Oct. 29, 1992, 1 F.3d 87, 93 (2d Cir. 1993)).

49. *Id.* at 116–17.

50. Notably, this question is distinct from whether the government can grant immunity to a suspect limited to the act of production and then use the documents obtained as a result of the

There is surprisingly little case law on this question.[51] In my view, it would be appropriate for governmental reliance on the foregone conclusion doctrine to imply a subsequent bar to using that implied testimony at trial. This is a sensible limit based on estoppel principles: if the government's power to compel an act depends on not needing testimony the act implies, the government should not be allowed to later use the implied testimony it claimed not to need.[52] But this is only my view of a question that the case law has not clearly settled.

C. The Foregone Conclusion as a Bar to Manipulation Between Door-Opening Evidence and Treasure

Some readers may be wondering how these two doctrines fit together. The act of production doctrine is reasonably intuitive. It measures implicit testimony in an act, relating the act to the Fifth Amendment's core concern of compelled testimony. But the foregone conclusion doctrine may seem strange. The doctrine acts as an exception to the act of production doctrine. But why? There is no obvious analogue to it when the government compels an answer to a direct question. It's fair to wonder why the doctrine exists.[53]

---

production. The Supreme Court answered that latter question "no" in *United States v. Hubbell*, 530 U.S. 27, 42–43 (2000). *See* United States v. Ponds, 454 F.3d 313, 321 (D.C. Cir. 2006) (noting that *Hubbell* held that if immunity is granted, "the use of the contents of produced documents [are a] barred derivative use of the compelled testimonial act of production"). How far a grant of immunity must extend involves a separate question from whether the government can introduce evidence at trial when no immunity has been granted. *See* United States v. Doe, 465 U.S. 605, 616 (1984) (declining to allow the government to compel acts of production on the promise that the incriminating aspects would not be used at trial in the absence of a formal statutory request for immunity); Kastigar v. United States, 406 U.S. 441, 453 (1972) (upholding the compulsion of testimony where the government has granted transactional immunity from use and derivative use of that testimony against the witness).

51. One district court decision has held that the government cannot rely on the foregone conclusion doctrine and then introduce evidence of the defendant's testimonial act at trial. *See* United States v. Spencer, No. 17-cr-00259-CRB-1, 2018 WL 1964588, at *3 (N.D. Cal. Apr. 26, 2018) ("Once Spencer decrypts the devices, however, the government may not make direct use of the evidence that he has done so." (citing Robert P. Mosteller, *Simplifying Subpoena Law: Taking the Fifth Amendment Seriously*, 73 VA. L. REV. 1, 110 n.108 (1987))). The D.C. Circuit has dicta somewhat relevant to this issue that can be read either way. *See In re* Sealed Case, 832 F.2d 1268, 1281 n.8 (D.C. Cir. 1987) (stating in dicta that if the government seeks to use the testimonial aspect of production at trial that had been earlier declared a foregone conclusion, the defendant can then challenge for a second time whether the foregone conclusion test was satisfied).

52. The Supreme Court adopted a somewhat similar limit in *Braswell v. United States*, 487 U.S. 99 (1988), where the Court held that the government can compel a corporate custodian to produce records but cannot then use the act of production against the custodian in his personal capacity. *Id.* at 117–18; *see also Spencer*, 2018 WL 1964588, at *3 ("If it really is a foregone conclusion[,] . . . the government of course should have no use for evidence of the act of production itself.").

53. *See, e.g.*, Samuel A. Alito, Jr., *Documents and the Privilege Against Self-Incrimination*, 48 U. PITT. L. REV. 27, 48–50 (1986) (noting that *Fisher* "left substantial doubt about what it meant by 'a foregone conclusion'"); Mosteller, *supra* note 51, at 29–34 (1987) (considering different rationales for the foregone conclusion doctrine).

As I see it, the foregone conclusion doctrine exists to prevent suspects from exploiting the act of production doctrine to create a bar to accessing nontestimonial evidence. The problem is rooted in an important difference between the investigative consequences of compelling answers and compelling acts. When the government forces a person to answer a question, it collects only one kind of evidence. The government asks a question, and the person answers it. The government learns only the answer. The situation is different when the government compels acts instead of words. In most cases, the purpose of compelling acts is to obtain evidence that the acts can help reveal. The government wants the person to open a door to obtain some treasure that opening the door reveals.

This means that, when the government compels acts, it acquires two different kinds of evidence at once. First, it learns the testimonial statements implicit in the act identified by the act of production doctrine. Let's call that "door-opening evidence." Second, the government also obtains the nontestimonial evidence revealed as a consequence of that act. Let's call that "the treasure." When the government compels a person to open the door and let the government see the treasure inside, it obtains both the door-opening evidence and whatever treasure is revealed.

Consider a case like *Fisher*, where the government compels a person to hand over the accountant's tax documents.[54] The act of compliance provides the government with two things. First, compliance establishes the person's testimonial door-opening evidence: the implicit beliefs about possession, existence, and authenticity of the tax documents. Second, it provides access to the treasure, the documents that the government is seeking. The door-opening evidence is compelled testimony. But the treasure, what the government finds in the documents, is *not* compelled testimony.[55] As a practical matter, the door-opening evidence operates causally as a testimonial gateway to the nontestimonial treasure. The government may be unable to obtain the treasure without the door-opening. But the two are analytically distinct, and only the latter is compelled testimony.

The best explanation for the foregone conclusion doctrine is that it prevents the causal relationship between door-opening evidence and treasure from being used to shroud the treasure in the Fifth Amendment protection properly limited to the door-opening. Without the foregone conclusion doctrine, suspects could take simple steps to introduce testimonial doors that block government access to their nontestimonial treasure. For example, a

54. Or at least this was the hypothetical on which the decision in *Fisher* rests. *See* discussion *supra* note 28.

55. The fact that government action leads to the acquisition of contents of the documents does not raise Fifth Amendment problems, *Fisher* explains, because the contents of the documents are not themselves compelled. Fisher v. United States, 425 U.S. 391, 409–10 (1976).

person in Fisher's situation could just gather all of his records and keep them in his possession. Any act of production would have to be compelled from him instead of from the accountant, introducing an act that implies the person's testimony under the act of production doctrine.[56]

The foregone conclusion doctrine blunts the advantage from such manipulation. It evaluates if the door-opening testimony is significant or is merely a matter of easily manipulated form. If opening the door implies incriminating testimony that the government does not already know, then the risk of compelled self-incrimination is real and the person has a privilege against opening the door that then necessarily blocks access to the treasure. On the other hand, if opening the door gives the government no prosecutorial advantage, then the risk of compelled self-incrimination is only a matter of form. At that point, as *Fisher* recognized, quoting Justice Holmes, "The question is not of testimony but of surrender."[57] When the testimony implicit in the door-opening is not in play, and is only an incidental matter of form rather than substance, access to the treasure should not be blocked by the Fifth Amendment privilege.

II. Applying the Fifth Amendment to Compelled Entering of Passwords

We can now apply these doctrines to a compelled act of decryption. Let's return to the scenario described in the introduction. The government has a seized electronic storage device in its possession, but efforts to search the device are blocked by encryption. Seeking access, the government obtains a lawful order directing a particular person to enter in the password to unlock the device. If the person pleads the Fifth, how should a court rule?

This Part argues that a court should reject the claim of privilege when the government has independent knowledge that the person knows the password. Entering a password that unlocks a device has a testimonial component: it testifies that the person knows the password that unlocks the device. But the foregone conclusion doctrine applies when the government has independent knowledge of that fact. This standard allows the government to compel a suspect to enter a password in many but not all cases. It also shows the Eleventh Circuit's apparent confusion in the first federal circuit court decision on compulsion to enter a password, *In re Subpoena Duces Tecum*.[58] This Part begins by applying the act of production doctrine, turns next to the foregone conclusion doctrine, and concludes with a critical take on the Eleventh Circuit's decision.

---

56. Because the Fifth Amendment privilege is personal, the accountant could not assert the privilege on the client's behalf. *Id.* at 397.

57. *Id.* at 411 (quoting *In re* Harris, 221 U.S. 274, 279 (1911)). As Justice Holmes explained in *Harris*, "The right not to be compelled to be a witness against oneself is not a right to appropriate property that may tell one's story." *Harris*, 221 U.S. at 279–80.

58. 670 F.3d 1335 (11th Cir. 2012).

A. The Testimonial Aspect of Entering in a Password

The first question is whether the compelled act of entering in the password that unlocks the device amounts to testimony under the act of production doctrine. The answer is clearly "yes." Entering a password is testimonial because it communicates a simple statement: "I know the password." A person can be successfully ordered to do only what he has sufficient knowledge to do. If a person knows the password, he can enter it and unlock the device. If a person doesn't know the password, however, he can't enter it. As a result, the act of entering in the password and unlocking the device has simple testimonial significance. It amounts to an assertion that the person knows the password.

Importantly, "I know the password" is the only assertion implicit in unlocking the device. Because the password is entered without revealing it to the government, any communicative content that its characters might contain (such as a hypothetical password, "ISELLDRUGS") is not asserted to the government.[59] In addition, the act of unlocking the device does not communicate knowledge about the device's contents. Knowing the password and knowing the contents of a decrypted device are two different things. One person might know the device's contents but not know the password. Another person might know the password but not know the device's contents.

The distinction is worth illustrating with an example. I happen to know the passcode to my sister's smart phone.[60] I learned it at a family event when I wanted to use her phone to google something. I asked her for the passcode, and she told me. If the government obtained a court order requiring me to enter in the password, I could comply with the order because I know the password.[61] But critically, I have no idea what files are stored in my sister's phone. The only thing I know about my sister's phone is its password. Unlocking the phone would admit I know the passcode, but it wouldn't admit that I know what is on the phone. Because I don't.

At this point the reader may push back. Unlocking a device doesn't necessarily indicate knowledge beyond the password. But doesn't it give some good hints? After all, we normally know the passwords to devices that we regularly use. A statement admitting knowledge of a password can reveal some good clues about the device's ownership or use. Use could give the government some idea about a person's knowledge of its contents. Given all

59. In that sense compelled decryption is more like being forced to surrender a key to a strongbox containing incriminating documents than being compelled to reveal the combination to a wall safe. *See* Doe v. United States, 487 U.S. 201, 210 n.9 (1988) (using these as examples).

60. This example is adapted from my blog post, Kerr, *Fifth Amendment Limits on Forced Decryption*, *supra* note 10.

61. At least assuming my sister hasn't since changed it.

of this, it might seem that there is more testimonial content to unlocking the phone than merely the statement that the person knows the passcode.

I think this argument is wrong. It mistakenly assumes that a testimonial statement about one subject also testifies to plausible implications to be drawn from that statement. The plausible implications of a statement may make the statement incriminating, but they don't amount to additional testimony. To see this, imagine a witness who is asked on the stand if she was present at the crime scene. Answering that question may be incriminating, as it may place her in danger of being implicated in the crime.[62] Knowing the witness was at the crime scene could help the prosecutor show her involvement in the crime. Nonetheless, admitting presence at the crime scene is distinct from admitting criminal involvement. The ability to draw an inference from testimony does not amount to testimony about that inference.[63]

Some have argued that compelled decryption has broader testimonial significance because it effectively creates the evidence decrypted.[64] The apparent thinking is that decryption causes information to exist that did not exist before, itself resembling an act of speech that adds to the testimony inherent in the act.[65] This argument is wrong because it misses the distinction explained earlier between door-opening evidence and treasure.[66] To be sure, the treasure revealed by door-opening can be extremely incriminating speech. It might include a signed confession. It might contain video of the defendant

62. *See* Resnover v. State, 507 N.E.2d 1382, 1389 (Ind. 1987) (recognizing a Fifth Amendment privilege for a witness facing compulsion to testify that she was present at the crime scene).

63. My friend Laurent Sacharoff offers a different view in his response essay. Laurent Sacharoff, *What Am I Really Saying When I Open My Smartphone? Response (to Orin S. Kerr)*, 97 TEXAS L. REV. ONLINE (forthcoming Mar. 2019). Professor Sacharoff contends that the testimony implicit in entering a password to decrypt a device includes additional statements, specifically that "the device likely belongs to the person" who entered the password "and that the person possesses, perhaps knowingly, the files on the device." *Id.* (manuscript at 105). In my view, Professor Sacharoff is mixing up the implied testimony inherent in an act with its evidentiary value. The implied testimony of an act is what a person must have been thinking to complete the act. On the other hand, the evidentiary value of an act is what conclusions a fact-finder might be more or less inclined to reach upon learning of the act. An act of decryption no doubt can have broad evidentiary significance in many cases. A fact-finder informed that a person decrypted a device may be more inclined to think that the person owns the device and may have knowledge of its contents. But the privilege against self-incrimination harnesses different principles than evidence law. What matters for the privilege is the state of mind that the act necessarily reveals, not what facts about the world an act suggests are more likely to be true.

64. *See, e.g.*, Seo v. State, 109 N.E.3d 418, 431 (Ind. Ct. App. 2018) ("We also consider [the act of decryption] testimonial because her act of unlocking, and thereby decrypting, her phone effectively recreates the files sought by the State."), *transfer granted, opinion vacated*, 2018 WL 6565988 (Ind. Dec. 6, 2018).

65. *See id.* ("Because compelling Seo to unlock her phone compels her to literally recreate the information the State is seeking, we consider this recreation of digital information to be more testimonial in nature than the mere production of paper documents.").

66. *See supra* subpart I(C).

committing the crime. The door-opening may make that evidence exist in a way it did not exist in encrypted form. But all of this is irrelevant to the privilege against self-incrimination. The act of production doctrine considers the actor's communication implicit in the act, not what communications may result from the act. How incriminating the treasure may be, or what the computer does when a person opens the door, does not change the testimony implicit in the door-opening act.[67]

A similar error is to claim that entering a password has broader testimonial significance because it is akin to translating the entire encrypted contents from ciphertext to plaintext. On this thinking, entering the password is like a witness taking the stand and translating documents from a secret language into English. But this analogy doesn't work. Assuming that an act of translation could be incriminating,[68] and that the act of production doctrine would apply to it, the testimonial aspect of translation is knowing how to translate from one language to another. In contrast, entering a password implies no such knowledge. Take the case of my sister's phone. If I enter the password and the phone unlocks, my entering the password implies no knowledge about how the phone's encryption software works. I don't even know what kind of phone my sister has. The only testimony implicit in unlocking her phone is the only thing I know: The password.

A final wrong turn worth addressing is the claim that the wall safe hypothetical in *Doe v. United States* ("*Doe II*")[69] can settle the testimonial content of entering in a password. *Doe II* held that being compelled to sign your signature to a consent directive is not testimonial.[70] Dicta in a footnote echoed Justice Stevens's view, expressed in dissent, that a suspect "be[ing] compelled to reveal the combination to his wall safe[] by word or deed" would be testimonial but that "in some cases be[ing] forced to surrender a key to a strongbox containing incriminating documents" would not be.[71] It's fair to ask whether *Doe II*'s dicta answers how the Fifth Amendment applies to compelled decryption.

---

67. *Cf. In re* Search Warrant Application, 279 F. Supp. 3d 800, 805–06 (N.D. Ill. 2017) (explaining why use of a biometric to decrypt does not gain testimonial significance based on the information revealed; "this argument . . . relies on conflating what it means for an act to be inherently testimonial versus an act yielding an incriminating result").

68. *Cf.* United States v. Burr, 25 F. Cas. 38, 39–41 (C.C.D. Va. 1807) (No. 14,692e) (Marshall, C.J.) (ruling that Aaron Burr's private secretary could not be compelled to testify about the meaning of Burr's encoded communications).

69. 487 U.S. 201 (1988). The label "*Doe II*" distinguishes the case from another Fifth Amendment case, *United States v. Doe*, 465 U.S. 605 (1984).

70. *See Doe II*, 487 U.S. at 219 ("Because the consent directive is not testimonial in nature, we conclude that the District Court's order compelling petitioner to sign the directive does not violate his Fifth Amendment privilege against self-incrimination.").

71. *Id.* (Stevens, J., dissenting). Justice Stevens suggested this distinction in his dissent, and the majority then indicated in a footnote that the Court agreed with the basic distinction. *Id.* at 210 n.9 (majority opinion).

In my view, *Doe II*'s dicta sheds no light either way on the Fifth Amendment implications of being forced to enter a password. Both statements in the dicta are truisms. That revealing the combination to a wall safe is testimonial should be obvious. It is a statement of a person's thoughts revealed to the government. That does not answer how the same principles apply to an act of decryption, however, because an act of decryption does not reveal the password. Granted, it's possible that the idea of revealing the combination "by deed" was intended to include opening a combination safe for investigators without actually revealing the combination. If so, that passage suggests the same conclusion reached in this section: using the combination to open the safe testifies that the person knows the combination, just as entering a password to decrypt data testifies that the person knows the password. But that meaning is not at all clear from the brief line in *Doe II*, which on its face is about "reveal[ing] the combination"[72] and not just unlocking the safe.

Similarly, the Court's apparent view that being compelled to surrender a key would not be incriminating "in some cases" is also unilluminating. Note the caveat: in some cases. It's easy to think of examples where surrendering a key would not be incriminating. Imagine the police search a business, find a locked safe, and see a suspect with the safe key in his hand. The police order the suspect to drop the key and put his hands up. In that case, surrendering the key would not be testimonial. Compliance with the order would not reveal the contents of the suspect's mind. But that sheds no light on how the Fifth Amendment might apply to other efforts to force a person to surrender a key, such as issuing a subpoena requiring the target to collect the key and give it to the grand jury. That kind of "surrendering" the key would be testimonial, in my view, as it admits to the existence, authenticity, and possession of the key just like the documents sought in *Fisher*. The answer must come from the framework identified in *Fisher*, not from the vague and unilluminating dicta from *Doe II*.

B. Applying the Foregone Conclusion Doctrine to Password Entering

We now turn to how the foregone conclusion doctrine applies to an act of compelled decryption. Recall that to apply the foregone conclusion doctrine, we ask if the government gained a prosecutorial advantage by obtaining the testimony implied by the compelled act. In the language of *Fisher*, the question is whether the implied testimony is "in issue" or if obtaining it "adds little or nothing to the sum total of the Government's information" for purposes of a future prosecution.[73]

Although the foregone conclusion doctrine is often applied in a fact-

72. *Id.* at 210 n.9 (majority opinion).

73. Fisher v. United States, 425 U.S. 391, 411–12 (1976).

specific way, a simple rule emerges when the government orders a suspect to enter a password to decrypt a device. As explained above, the only assertion implied by entering the correct password is that the person compelled knows that password. That yields a simple insight: the implied testimony cannot be in issue, and cannot add to the sum total of the government's information, when the government provides the device to the suspect at the password prompt and the government already knows that the person knows the password. The testimony is a foregone conclusion, and a court should not recognize the privilege because the government has independent proof of the entire testimonial content of the compelled act.

A bright-line rule results: when investigators present a suspect with a password prompt, and they obtain an order compelling the suspect to enter in the correct password, the suspect cannot have a valid Fifth Amendment privilege if the government independently can show that the suspect knows the password. The government's independent evidence that the suspect knows the password means that the suspect's knowledge is not in issue. It adds nothing to the sum total of the government's information for the government to learn what it already knows. As a result, the government's independent knowledge that the person knows the password makes the implied testimony of entering it a foregone conclusion.[74]

This standard should be easy for the government to satisfy in many common cases. Individuals ordinarily must know the password of devices that they regularly use. As a result, evidence that the person regularly uses a particular device should generally be sufficient to show knowledge of the password and trigger the foregone conclusion doctrine. Imagine the government seizes an encrypted smart phone from a suspect's pocket incident to his arrest.[75] The suspect's fingerprints are on the phone. Calling the suspect's known phone number makes the phone ring. In such a case, the evidence will likely indicate that the person knows the password and therefore establishes a foregone conclusion.

There are a few important caveats to make. First, a different analysis is called for when a person's awareness of the password is in issue. In such a case, the Fifth Amendment should impose a bar to compelling the act. Imagine the government obtains a search warrant to search a home for computer-stored images of child pornography. The home has three residents. The search yields one computer, and that computer has an encrypted hard drive that requires a password to use. Further assume that investigators have no evidence about which resident owns or uses the computer. In an effort to bypass the encryption, investigators obtain court orders requiring each of the three residents to enter the password.

74. *Accord* Jarone, *supra* note 9, at 796–97 (reaching a similar conclusion).

75. *Cf.* Riley v. California, 134 S. Ct. 2473, 2485 (2014) (requiring a warrant to search a cell phone seized incident to arrest).

In such a case, each resident would have a valid Fifth Amendment privilege against complying with the order. Entering the password would show knowledge of it. Establishing knowledge would help show criminal possession of the images that may be on the computer. In a prosecution for possession of those images, a person's awareness of the password required to access the images would be "in issue."[76] If the prosecution had no information that any particular resident knew the password, each resident would have a privilege not to be compelled to enter the password to reveal they knew it. Knowledge of the password would not be a foregone conclusion.

A second important caveat is that a valid privilege can exist when the government's order includes an implicit search requirement. The critical difference is between an order to enter a password at a password prompt and an order to take a broader set of steps to produce the files in decrypted form. When agents present the user with a password prompt and compel him to enter the password, the implicit testimony is a foregone conclusion when the government can show the user knows that password. But it's a different case if agents obtain an order to produce a decrypted version of all files on the device. An order to produce all encrypted files can have an implicit search requirement: compliance can require more than just entering a password.

The reason for the difference is that encryption is not all or nothing. A user might first encrypt a particular file and then encrypt the entire device that includes that file. A user might encrypt files in a "hidden volume" that the government can't tell exists and can't locate without the user's help.[77] In these situations, producing the files on the device in encrypted form has more testimonial significance than merely stating knowledge of the password. Depending on the case, the production might require admitting to knowledge of the hidden volume or the presence and location of additional encrypted files. Put another way, complying with an order to produce all of the files on a device in decrypted form may require knowledge beyond just how to bypass a password gate presented to the user. In such a case, the foregone conclusion doctrine would apply only if all of the implicit statements required to conduct the search are themselves foregone conclusions. Mere knowledge of a password would not be enough.

One way to deal with this complication would be for decryption orders to require bypassing password gates instead of producing plaintext. The order could command the subject of the order to enter in passwords needed to

76. *Fisher*, 425 U.S. at 412.

77. *See* Aloni Cohen & Sunoo Park, *Compelled Decryption and the Fifth Amendment: Exploring the Technical Boundaries*, 32 HARV. J.L. & TECH. (forthcoming 2019) (manuscript at 28–29), https://ssrn.com/abstract_id=3117984 [https://perma.cc/4UHS-26WT] (discussing hidden volumes).

bypass password gates presented to the subject on a particular device. The order would compel only the act of entering a password and it would not compel any searching.[78] If at any point the target asserts his Fifth Amendment right, a court could address whether the government can show independently that it knows the target knows that particular password. This approach to drafting decryption orders could avoid the possibility of an implicit search requirement that could complicate the Fifth Amendment analysis.

C. *The Eleventh Circuit's Apparent Misstep in* In re Subpoena Duces Tecum

An important implication of my argument is that the only federal court of appeals decision directly addressing this issue, the Eleventh Circuit's ruling in *In re Subpoena Duces Tecum*,[79] is either wrongly decided or at least very confusingly written. Other courts may be understandably reluctant to disagree with a precedential circuit court opinion. But the opinion appears to be based on a mistake that other courts should not make.

Here's a quick rundown of the facts. A suspect, known only as John Doe, was served a subpoena requiring him to produce the decrypted contents of several of his hard drives believed to contain child pornography.[80] A forensic examination of Doe's hard drives showed that they were partially encrypted with a program called TrueCrypt.[81] The examiner could access parts of the hard drives, but they were blank.[82] At the same time, the examiner was "unable to access certain portions of the hard drives" that were encrypted using TrueCrypt.[83] The examiner could see the raw data on the drives and knew that TrueCrypt had been used.[84] But he could not know what information (if anything) would be revealed when decrypted.[85]

---

78. The language of my proposed Decryption Order might state: "John Doe is hereby ordered, when presented with a password prompt on the device described below, to enter in the password needed to bypass that password prompt." The order could then describe the device. It is possible that a device could be configured with multiple passwords, including a special password that does not decrypt all data but instead presents users with only some of the decrypted data. *See id.* (manuscript at 28–31) (describing "deniable encryption"). But use of such a password seems unlikely to raise significant Fifth Amendment issues. The deniability of the encryption means that the government will not realize what the user has done. Further, whether use of such a password violates the Decryption Order depends on how the order is drafted. If the government has reason to think that a suspect has used such technologies, that raises practical problems with proceeding by compelled decryption rather than Fifth Amendment challenges. *See also* Kerr & Schneier, *supra* note 3, at 1005 (discussing remedies for failure to comply with court orders to decrypt).

79. 670 F.3d 1335 (11th Cir. 2012).

80. *Id.* at 1337.

81. *Id.* at 1340.

82. *Id.* at 1340 n.10.

83. *Id.* at 1339.

84. *Id.* at 1340.

85. *Id.*

In an opinion by Judge Tjoflat, the Eleventh Circuit concluded that Doe had a valid privilege against self-incrimination and could not be compelled to comply with the subpoena.[86] Unfortunately, the court's analysis of the testimonial aspect of compulsion was very brief. According to Judge Tjoflat, complying with the subpoena would amount to Doe's testimony of his "knowledge of the existence and location of potentially incriminating files; of his possession, control, and access to the encrypted portions of the drives; and of his capability to decrypt the files."[87] The opinion contains no analysis of why these assertions would be implicit in completing the ordered act.

The court then concluded that the foregone conclusion doctrine did not apply.[88] According to Judge Tjoflat, the doctrine would apply only "if the Government can show with 'reasonable particularity' that, at the time it sought to compel the act of production, it already knew of the materials[.]"[89] That was not the case, however, because "we simply do not know what, if anything, was hidden based on the facts before us."[90] According to Judge Tjoflat, the foregone conclusion doctrine could not apply because the government did "not know what, if anything, is held on the encrypted drives."[91]

The problem with applying the foregone conclusion doctrine, the Eleventh Circuit concluded, was that the government did not describe the documents it was seeking with sufficient specificity.[92] The government had not shown sufficient "knowledge as to the *files* on the hard drives at the time it attempted to compel production from Doe."[93] Without knowing "to any degree of particularity what, if anything, was hidden behind the encrypted wall," the government could not describe the files it was seeking with reasonable particularity and the foregone conclusion doctrine could not apply.[94]

The Eleventh Circuit's reasoning is not a model of clarity. It can be read different ways. In my view, the most faithful reading is that the opinion requires the government to describe with reasonable particularity the decrypted documents it will find before an act of decryption is a foregone

86. *Id.* at 1352–53.

87. *Id.* at 1346.

88. *Id.* at 1349.

89. *Id.* at 1346.

90. *Id.* at 1347.

91. *Id.*

92. *See id.* ("Case law from the Supreme Court does not demand that the Government identify exactly the documents it seeks, but it does require some specificity in its requests—categorical requests for documents the Government anticipates are likely to exist simply will not suffice.").

93. *Id.* (emphasis in original).

94. *Id.* at 1349.

conclusion.[95] If so read, the Eleventh Circuit's analysis is wrong. It fails to distinguish two different roles a target can serve in carrying out a search. If evidence is in a locked box, investigators might order a suspect to unlock the box and do no more. Investigators can then take over the search, investigating the contents of the box themselves and looking for the evidence. On the other hand, investigators might order a suspect to unlock the box and then execute the search himself on the government's behalf. The suspect might be ordered to unlock the box, search it, find a particular set of documents described, and then bring those responsive documents to the government. The first target role is unlocking; the second target role is unlocking and searching.

Under my reading of the case, the Eleventh Circuit missed this distinction. It treated a case in which the target's role was unlocking the device as if the target's role had been unlocking the device and then searching it for the described evidence. When a suspect is ordered to produce a decrypted version of an electronic device, the compelled act ordinarily will be only to unlock the device. Any additional searching is the government's job, and the government need not know what it will find when it begins to look. Whether the government knows enough about the incriminating evidence it hopes to find to describe it with reasonable particularity is simply irrelevant if the government, not the target, is going to look for it. If the target doesn't have to search for the evidence the government is seeking, the target doesn't need a specific description to establish a foregone conclusion.

Granted, there is a sense in which the government does need to particularly describe the evidence sought—but for the Fourth Amendment, not the Fifth Amendment. Most compelled decryption helps the government execute a search warrant. The Fourth Amendment requires the warrant to particularly describe the evidence to be searched for and seized.[96] It might seem, at first blush, that the Fourth Amendment's particularity requirement serves the same function as the common Fifth Amendment foregone conclusion requirement of reasonable particularity. Both help limit the searcher's discretion as to what is seized.[97]

But they do so for quite different reasons. The Fourth Amendment's particularity requirement prevents general searches.[98] It limits the searcher's

95. This interpretation is perhaps easiest to establish by how the Eleventh Circuit distinguished the contrary result in *In re Boucher*, No. 2:06-mj-91, 2009 WL 424718 (D. Vt. Feb. 19, 2009). According to the Eleventh Circuit, "it was crucial" to the result in *Boucher* "that the Government knew that there existed a file under [an incriminating] name." *In re Subpoena*, 670 F.3d at 1348–49. In the Eleventh Circuit's view, it appears, the foregone conclusion doctrine hinged on the government's knowledge of the file.

96. U.S. CONST. amend. IV.

97. A classic (if plainly exaggerated) statement of the role of Fourth Amendment particularity is that "[a]s to what is to be taken, nothing is left to the discretion of the officer executing the warrant." Marron v. United States, 275 U.S. 192, 196 (1927).

98. Andresen v. Maryland, 427 U.S. 463, 480 (1976).

discretion to ensure that he does not take away too much.[99] In contrast, the particularity standard relied on in Fifth Amendment foregone conclusion cases prevents implied statements. It limits a target's discretion to ensure that the government isn't relying on assertions implicit in the choices a target makes to carry out the order. The two doctrines serve different roles and satisfy different standards. When the government obtains a search warrant and a related decryption order, the only relevant particularity requirement comes from the Fourth Amendment's warrant clause.[100] After the target unlocks the device, his work is done. The government must now execute the warrant to search for the evidence particularly described within it.

I noted above that there is a second way to read the Eleventh Circuit's opinion. Under the second interpretation, the opinion is confusing and poorly written but its result may be correct. Here's why. Recall that Doe was ordered to produce a decrypted version of the files on his devices that were encrypted using TrueCrypt. TrueCrypt allows users to place files in hidden volumes.[101] It's possible that Doe's Fifth Amendment objection was to being ordered to identify hidden volumes on his device. If so, perhaps the Eleventh Circuit's objection was only to compelling Doe to identify the hidden volumes in the course of the act of producing a decrypted version of the files on his device.[102] From that perspective, Doe would have a valid Fifth Amendment privilege against revealing that there was a hidden volume—something the government did not know and, therefore, was not a foregone conclusion. I think parts of the opinion make this reading a stretch.[103] But it points to the possibility that the Eleventh Circuit may have been inarticulately reaching the right result rather than misapplying the law.

However the Eleventh Circuit's decision is read, the case exposes how courts have so far failed to articulate a standard of proof for the foregone conclusion doctrine. Whatever the merits of the "reasonable particularity" standard when investigators seek to enforce an order to hand over certain documents, it has no application when the government seeks to enforce an order to unlock. Fifth Amendment challenges to decryption orders require

99. *Marron*, 275 U.S. at 196.

100. *See* United States v. Grubbs, 547 U.S. 90, 97 (2006) ("The Fourth Amendment, however, does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and 'the persons or things to be seized.'" (alteration in original)).

101. *See generally* Jill Scharr, *How to Encrypt Your Files Using TrueCrypt*, TOM'S GUIDE (Aug. 7, 2013, 9:46 AM), https://www.tomsguide.com/us/how-to-encrypt-truecrypt,review-1832.html [https://perma.cc/6D8S-X9JN] (explaining TrueCrypt).

102. For such an interpretation, see Robert Graham's Twitter thread that begins at Robert Graham (@ErrataRob), TWITTER (Sept. 14, 2018, 2:44 PM), https://twitter.com/ErrataRob/status/1040718035236020230 [https://perma.cc/L93B-HVEN].

103. *See supra* note 95.

courts to identify the government's burden of proof: How clear must it be that the government already knows that the target knows the password?[104]

The novelty of the question is demonstrated by the fact that the two cases that have directly confronted the question have both involved compelled decryption using a Fifth Amendment framework along the lines that I have advocated in this Essay. In one recent district court case, *United States v. Spencer*,[105] Judge Breyer adopted the correct standard for the foregone conclusion doctrine—citing, I was pleased to see, a blog post of mine[106]—and then applied a clear and convincing evidence standard.[107] He picked the burden of proof on policy grounds: a high burden was appropriate, Judge Breyer wrote, given the law's "jealous protection of the privilege against self-incriminating testimony."[108] Another district court case on compelled decryption, *United States v. Fricosu*,[109] applied the preponderance of the evidence standard to measure the government's knowledge.[110] But *Fricosu* simply states the standard without explanation or citation: "My findings of fact," the district judge stated, "are based on a preponderance of the evidence."[111]

Notably, *Spencer* and *Fricosu* applied different standards but neither cited any directly related precedent. And the reason may simply be that there is little or no precedent to cite. Particularity-based standards of proof articulated in the context of subpoenas for documents have kept courts from confronting the degree of certainty required for a fact to be a foregone conclusion. Whatever the best answer is,[112] a proper understanding of the foregone conclusion doctrine now requires courts to answer it.

---

104. The government has the burden of proof to show a foregone conclusion. *E.g.*, United States v. Bright, 596 F.3d 683, 693 (9th Cir. 2010); United States v. Rue, 819 F.2d 1488, 1493 n.4 (8th Cir. 1987). However, how high that burden is remains surprisingly unclear. *See, e.g.*, Kevin R. Reitz, *Clients, Lawyers and the Fifth Amendment: The Need for a Projected Privilege*, 41 DUKE L.J. 572, 631 (1991) ("A critical issue, to date unresolved by the courts, is the burden of proof borne by the government in demonstrating that a particular testimonial fact is indeed a foregone conclusion."). Although Professor Reitz wrote that comment in 1991, it remains true today.

105. No. 17-cr-00259-CRB-1, 2018 WL 1964588 (N.D. Cal. Apr. 26, 2018) (Breyer, J.).

106. *Id.* at *3 n.2 ("The details of what records are on the phone should be irrelevant to whether the foregone conclusion doctrine applies because access to the phone is independent of what records are stored inside it. Handing over the passcode has the same testimonial aspect regardless of what is on the phone." (quoting Kerr, *Fifth Amendment Protects Passcode on Smartphones, Court Holds*, *supra* note 10)).

107. *Id.* at *3.

108. *Id.*

109. 841 F. Supp. 2d 1232 (D. Colo. 2012).

110. *Id.* at 1234.

111. *Id.*

112. A formalist approach to answering this might start with mining the Supreme Court's foregone conclusion cases for clues. *Fisher* has two particularly interesting ones. First, *Fisher* says the Court is "confident" that the act of production would not itself involve testimonial self-incrimination in light of the foregone conclusion doctrine. Fisher v. United States, 425 U.S. 391,

III. Compelled Decryption and Equilibrium-Adjustment

This Essay has so far offered a doctrinal argument for a particular application of the Fifth Amendment to compelled acts of entering in passwords. This Part takes a broader view. In recent Fourth Amendment decisions, including *Carpenter v. United States*,[113] the Supreme Court has indicated that courts should not apply constitutional doctrines mechanically to the new facts of computers and the Internet.[114] Instead, courts should look to how old rules alter the new power dynamic between the government and the citizen in light of current and future technology.[115] This Part considers whether that directive applies to compelled decryption, and if so, what Fifth Amendment standard that rule might produce. Put another way, let's put current doctrine aside and consider the implications of rules in their technological context: What kind of Fifth Amendment standard is best suited to the role of encryption in modern life?

This Part argues that the correct doctrinal answer is also appropriate given the broader role of encryption. Encryption is now everywhere. Most Americans carry an encrypted device with them, and all are free to use strong encryption to protect their data. As a result, technology has inserted a remarkably powerful password gate in the way of routine searches across a wide range of cases. The government has various possible ways of bypassing encryption, and compelling decryption is only one of them. But adopting a high Fifth Amendment standard for compelled decryption could wrongly hide personal data from government access even when the government has a Fourth Amendment search warrant for that data and the data the government seeks is not itself compelled under the Fifth Amendment. To the extent courts are concerned with the broader shifts of power that technology creates in criminal investigations, the "seismic shifts"[116] of technological change triggered by encryption suggest that uncertainty in the Fifth Amendment standard should be resolved in the government's favor.

410–11 (1976). Second, *Fisher* adds that the Court was "doubtful" that assertions implicit in production were enough for the privilege to apply. *Id.* at 411. Words like "confident" and "doubtful" might plausibly suggest a clear and convincing evidence standard along the lines of *Spencer*. I recently argued along these lines in support of the clear and convincing evidence standard in a case pending before the Supreme Judicial Court of Massachusetts. Brief of Amicus Curiae Professor Orin Kerr in Support of Neither Party at 9–10, Commonwealth v. Jones, No. SJC-12564 (Mass. Oct. 11, 2018), https://ssrn.com/abstract=3264866 [https://perma.cc/5Z2R-TJT5].

113. 138 S. Ct. 2206 (2018).

114. *See id.* at 2223 ("[T]he progress of science has afforded law enforcement a powerful new tool to carry out its important responsibilities. At the same time, this tool risks Government encroachment of the sort the Framers . . . drafted the Fourth Amendment to prevent."); *see also id.* at 2233 (Kennedy, J., dissenting) (citing Kerr, *supra* note 14, but ultimately preferring a legislative fix).

115. *See infra* notes 117–121 and accompanying text.

116. *Carpenter*, 138 S. Ct. at 2219.

This Part makes that argument in three steps. First, it explains why there is at least a plausible case that the principles of equilibrium-adjustment should extend to the right against self-incrimination. Second, it argues that if equilibrium-adjustment is relevant, it counsels in favor of the relatively modest Fifth Amendment rule I have advocated. Third, it considers the relevance of this approach to the Fifth Amendment for the "going dark" debate in surveillance law.

A. Does Equilibrium-Adjustment Apply to the Right Against Self-Incrimination?

In 2011, in an article titled *An Equilibrium-Adjustment Theory of the Fourth Amendment*,[117] I argued that the Supreme Court has a recurring approach to interpreting the Fourth Amendment in response to changing technology. Traditional Fourth Amendment rules presupposed a balance of power.[118] New technologies constantly threaten that balance because old rules can apply to new technologies in ways that dramatically expand or restrict government power.[119] To ensure that mechanical application of old rules does not create a dystopia in which new technologies either give the government too much power (which could lead to abuses) or too little power (which would not protect the public), the Court often adjusts old rules to restore the prior equilibrium of government power.[120] "The resulting judicial decisions," I wrote, "resemble the work of drivers trying to maintain constant speed over mountainous terrain. In an effort to maintain the preexisting equilibrium, they add extra gas when facing an uphill climb and ease off the pedal on the downslopes."[121]

Since 2011, the Supreme Court's application of equilibrium-adjustment principles has become particularly dramatic and explicit in Fourth Amendment cases involving digital technology.[122] The zenith of the approach appeared in the recent blockbuster decision in *Carpenter v. United States*,[123] which held that collection of historical cell-site records is a search that requires a warrant.[124] The precedents, and the circuit court case law, indicated that no search occurred in *Carpenter* because the location of the phones had

117. Kerr, *supra* note 14.

118. *Id.* at 485.

119. *Id.* at 485–87.

120. *See id.* at 487–89 (coining the term "equilibrium-adjustment").

121. *Id.* at 488.

122. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2485 (2014) (holding that a warrant is required to search a cell phone incident to arrest); United States v. Jones, 565 U.S. 400, 404 (2012) (holding that installing a GPS on a car is a Fourth Amendment search).

123. 138 S. Ct. 2206 (2018).

124. *Id.* at 2223.

been disclosed to the third-party cell phone companies.[125] The Court rejected this result on the ground that "seismic shifts in digital technology" gave the government so much power that it upset traditional expectations of limited government power and threatened law enforcement abuses.[126] "When confronting new concerns wrought by digital technology," the Court wrote, it is important "not to uncritically extend existing precedents."[127]

Should *Carpenter*-like arguments about equilibrium-adjustment extend to the Fifth Amendment right against self-incrimination? I'm not sure. On one hand, perhaps equilibrium-adjustment is solely a Fourth Amendment dynamic that should not extend beyond it. Search and seizure law can helpfully be understood as a way to impose a societal cost/benefit framework on police collection of evidence.[128] Methods of evidence collection often hinge on technological change. As technology changes, then, the societal costs and benefits of investigative steps regulated by the Fourth Amendment also change. It is therefore understandable that courts would want to adjust Fourth Amendment rules to restore the rough cost/benefit framework.[129]

The right against self-incrimination, by contrast, only involves using a person's own testimony against them. The Fifth Amendment focuses on the gathering of information from a person's mind, not on the technological world in which he lives. The implications for government power from this person-focused exchange are likely more stable. From that perspective, perhaps equilibrium-adjustment stops at the water's edge of search and seizure and does not flood into Fifth Amendment law.[130]

But perhaps matters are not so simple. There is at least a plausible argument that the meaning of the right against self-incrimination should be attuned to equilibrium-adjustment concerns. Consider two such arguments. First, the spheres of the Fourth and Fifth Amendments are often intertwined in practice. When the government gathers evidence, it might collect the evidence itself (a Fourth Amendment concern) or it might try to get a confession directly from the suspect (a Fifth Amendment concern). The two regimes arise in the same investigation, suggesting that the dynamic from one legal regime may be appropriately considered in the other.[131]

---

125. *See id.* at 2219–20 (addressing the government's reliance on the "third-party doctrine").

126. *Id.* at 2219.

127. *Id.* at 2222.

128. *See* Orin Kerr, *An Economic Understanding of Search and Seizure Law*, 164 U. PA. L. REV. 591, 595 (2016) ("[S]earch and seizure law is a way to account for investigative externalities and impose a rough cost–benefit test.").

129. *See id.* at 616–18 (providing an economic explanation for equilibrium-adjustment).

130. *Cf.* Braswell v. United States, 487 U.S. 99, 128 (1988) (Kennedy, J., dissenting) (arguing that the Fifth Amendment "does not permit balancing the convenience of the Government against the rights of a witness . . .").

131. *See* Dan Terzian, *Forced Decryption as Equilibrium—Why It's Constitutional and How* Riley *Matters*, 109 NW. U. L. REV. ONLINE 56, 60 (2014) (arguing that the Fifth Amendment

Second, some Fifth Amendment case law has considered the effectiveness of government regulatory regimes in interpreting the right against self-incrimination. For example, in *Baltimore v. Bouknight*,[132] a juvenile court ordered a mother to produce her child suspected of being abused.[133] The mother refused and asserted her right against self-incrimination.[134] The Court recognized that the mother's act of producing the child would be an admission of custody of the child, which could have potentially been used to prosecute her with child abuse.[135] But it nonetheless held the order enforceable because "the government's noncriminal regulatory powers" acted to "reduce[]" the privilege.[136] The government's regulatory interest altered the scope of the privilege.[137] If the effectiveness of a government regulatory regime can alter what the Fifth Amendment protects, something like the "special needs" doctrine in Fourth Amendment law,[138] then perhaps the Fifth Amendment is properly sensitive to the new technological implications of doctrine.

In the end, the uncertain theoretical basis of the privilege against self-incrimination counsels against resolving this disagreement. As many scholars of the privilege against self-incrimination have noted, the theoretical justification of the privilege is disputed territory.[139] If judges and scholars are unsure of what the right against self-incrimination is supposed to do, then it

---

privilege against self-incrimination should be included within the zone of equilibrium-adjustment); *cf.* Orin Kerr, *Does Carpenter Revolutionize the Law of Subpoenas?*, LAWFARE (June 26, 2018, 6:44 PM), https://www.lawfareblog.com/does-carpenter-revolutionize-law-subpoenas [https://perma.cc/RR6U-27HR] (suggesting that *Carpenter*'s Fourth Amendment standard for reasonableness reflects an interest in equilibrium-adjustment in light of Fifth Amendment rules).

132. Balt. City Dep't of Soc. Servs. v. Bouknight, 493 U.S. 549 (1990).

133. *Id.* at 552.

134. *Id.* at 553.

135. *Id.* at 555.

136. *Id.* at 558.

137. *Id.*

138. *See* Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001) (describing the special needs doctrine).

139. Justice Arthur Goldberg, quoting Professor Kalven, once noted that "the law and the lawyers . . . have never made up their minds just what it is supposed to do or just whom it is intended to protect." Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 56 n.5 (1964) (quoting Harry Kalven, Jr., *Invoking the Fifth Amendment—Some Legal and Impractical Considerations*, 9 BULL. ATOMIC SCIENTISTS 181, 182 (1953)). William Stuntz has added that "most people familiar with the doctrine surrounding the privilege against self-incrimination believe that it cannot be squared with any rational theory." William J. Stuntz, *Self-Incrimination and Excuse*, 88 COLUM. L. REV. 1227, 1228 (1988). Akhil Amar and Renée Lettow Lerner make a similar point more memorably: "The Self-Incrimination Clause of the Fifth Amendment," they write, "is an unsolved riddle of vast proportions, a Gordian knot in the middle of our Bill of Rights." Akhil Reed Amar & Renée B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 857 (1995); *see also* Ronald J. Allen & M. Kristin Mace, *The Self-Incrimination Clause Explained and Its Future Predicted*, 94 J. CRIM. L. & CRIMINOLOGY 243, 245–46 (2004) (contending that while "there is no general theoretical justification for the Fifth Amendment, there is a powerfully explanatory positive theory").

becomes difficult to answer whether it should fall within equilibrium-adjustment. This Essay instead takes a more modest path. If the right against self-incrimination does not consider equilibrium-adjustment, then I rest my argument on the doctrinal claim of Part II. On the other hand, if equilibrium-adjustment is relevant, what lessons does it teach for compelled decryption? The remainder of my Essay considers that question.

B. Modern Devices Insert Password Gates into Routine Searches

Applying equilibrium-adjustment to compelled decryption should recognize an important dynamic: the computer era has inserted powerful password gates into what would have been routine searches. Investigative steps that in the past would have only been Fourth Amendment searches now require Fourth Amendment searches plus encryption workarounds. Investigators ordinarily don't seek to compel decryption because they want testimony. They seek to compel decryption because in some cases there is no other way to execute searches. They need to open the door to find the treasure. Because the technology is effectively hiding routine evidence behind password gates, courts should be reluctant to interpret the Fifth Amendment as imposing a high barrier to compelled decryption.

To appreciate this point, we need to begin with old-fashioned searches. Traditional searches raise mostly Fourth Amendment problems. Take the case of a house. The government ordinarily needs a warrant to search a house. Once investigators have that warrant, however, there are few practical or legal barriers to conducting a highly invasive house search. Officers can break down the door if need be,[140] detain anyone found inside,[141] and search everywhere in the house where the evidence might be stored. No special equipment is needed.

Computer searches are different. The law of computer searches is still evolving and uncertain.[142] As a result, it is too early to draw direct comparisons. But the spread of encryption has introduced a major technological difference: in the case of end devices, and especially cell phones, it is common for computer searches to include a new investigative step of having to bypass encryption.[143] Widespread encryption has introduced what Bruce Schneier and I have called "encryption workarounds," in which

140. *See, e.g.*, United States v. Banks, 540 U.S. 31, 38 (2003) (allowing forcible entry after fifteen to twenty seconds of no response).

141. *See* Michigan v. Summers, 452 U.S. 692, 705 (1981) (holding that a warrant to search for contraband carries an implied authorization to detain occupants while the search is conducted).

142. *See generally* ORIN S. KERR, COMPUTER CRIME LAW ch. 5 (4th ed. 2018) (laying out the state of Fourth Amendment law with respect to computer crimes).

143. *See* Kerr & Schneier, *supra* note 3, at 991 ("For government investigators, encryption adds an extra step: They must figure out a way to access the plaintext form of a suspect's encrypted data.").

investigators who have satisfied the Fourth Amendment warrant requirement must nonetheless figure out a way to circumvent the powerful blocking technology of encryption that is now in routine use.[144] Encryption inserts a door in front of many forms of electronic treasure.

A range of different encryption workarounds exists.[145] Investigators might try to guess the passcode or find a copy of it. They might try to purchase hardware or software that could be used to crack the encryption in some cases.[146] A suspect may have biometric access set up on his phone, such that investigators can use the suspect's thumbprint to unlock the phone without raising any Fifth Amendment issues.[147] But despite these various means of access, efforts to compel a suspect to enter a password are a useful and important default: it can be used in a wide range of cases, it is scalable, and it requires only relatively modest law enforcement resources.[148]

As a result of this change, the shift from search-only to search-plus-hunt-for-encryption-workaround counsels against extravagant interpretations of the Fifth Amendment in the context of compelled entering of a password. Bypassing a password is a challenge for investigators, not an opportunity. Encryption is a barrier to evidence that must be overcome. Investigators seek a suspect to enter a password to decrypt the device so they can enable a subsequent search through plaintext pursuant to a warrant. Compelling testimony from the target is beside the point in most cases. It is a consequence of how the technology works, not evidence the government wants. The police don't want to know the password itself—and won't learn it anyway. The implied testimony in merely entering it without disclosing it is usually unimportant.

This is critical because of the function of the foregone conclusion doctrine explained earlier in subpart I(C).[149] As explained there, the foregone conclusion doctrine prevents testimonial door-opening from denying the government access to the causally revealed treasure when the testimony of the door-opening is not in play as part of building the government's case.[150] The introduction of device encryption creates a door-opening act requirement for the purpose of blocking access to treasure. That is the very point of having an encrypted device, of course. It gives the user sole control over who accesses the information stored in the device.

---

144. *Id.*

145. *See id.* at 996–1011 (identifying six categories of encryption workarounds).

146. *See id.* at 1014 (recognizing that such methods can be "very costly and require significant technical expertise").

147. *Id.* at 1003.

148. *See id.* at 1004 ("Notably, compelling a key raises practical and legal hurdles rather than technical ones. Sophisticated technological resources are not required, but a person who knows the key may refuse to hand it over or use it.").

149. *See supra* subpart I(C).

150. *See supra* subpart I(C).

This is a net good in most cases. But from a Fifth Amendment perspective, it inserts a door that ordinarily is of no testimonial interest to the government as a potential barrier to all of the computer-stored treasure that may be on the device. This is exactly the kind of nonsubstantive barrier that the foregone conclusion doctrine was designed to keep from blocking legitimate investigations.

Consider the choice users face of whether to configure their smart phones so that a biometric form of identification such as a thumbprint can be used to decrypt them. A thumbprint is nontestimonial: the government can order a suspect to place his thumb on a fingerprint reader without triggering the privilege at all.[151] But investigators would rather suspects use nontestimonial biometric access than passwords, as the former is an easier door to open than the latter. Similarly, those hoping to keep the government away emphasize the benefits of using passwords and the risks of biometrics.[152] From both the standpoint of investigators and possible suspects, the relevance of using a password is the practical challenge of bypassing the lock on the door and not whatever testimony it may reveal.

In effect, the widespread use of strong encryption by users amounts to a reverse-*Carpenter*. Instead of technology expanding government power in ways that call for new rules to avoid Big Brother, widespread encryption limits government power to execute otherwise lawful searches. I don't think this requires new Fifth Amendment rules. The analysis in Part II argues that the government already can legally compel entering in a password in a range of situations under a correct reading of the doctrine, and there is no need for a shift to a new pro-government rule. But the role of encryption counsels against broad readings of the Fifth Amendment privilege that might further, rather than counterbalance, the technological shift.[153]

A counterargument might be that computer searches are tremendously invasive. The Supreme Court recognized in *Riley v. California*[154] that computers (and especially cell phones) can store an astonishing amount of very personal information.[155] Perhaps this means that the Fifth Amendment

151. *See, e.g.*, State v. Diamond, 905 N.W.2d 870, 875 (Minn. 2018) ("[P]roviding a fingerprint to unlock a cellphone is *not* a testimonial communication under the Fifth Amendment.").

152. *See, e.g.*, Tim Cushing, *State Appeals Court Says Unlocking a Phone with a Fingerprint Doesn't Violate the Fifth Amendment*, TECHDIRT (Jan. 25, 2017, 3:11 PM), https://www.techdirt.com/articles/20170121/08510936531/state-appeals-court-says-unlocking-phone-with-fingerprint-doesnt-violate-fifth-amendment.shtml [https://perma.cc/4PFQ-L3YG] ("[Y]ou might be better off securing your phone with a passcode than your fingerprint. While a fingerprint is definitely unique and (theoretically. . .) a better way to keep thieves and snoopers from breaking into your phone, it's not much help when it comes to your Fifth Amendment protections against self-incrimination.").

153. *Accord* Terzian, *supra* note 131, at 62–63 (urging courts to allow compelled decryption in order to maintain the equilibrium).

154. 134 S. Ct. 2473 (2014).

155. *Id.* at 2490.

standard should be high to counteract the reality that computers give the government greater access to information, much like *Riley* imposed a warrant standard for searches incident to arrest only for phones? Put another way, perhaps the treasure of digital evidence is so valuable that the law should give special protections against being compelled to open the door?

I disagree. The problem is that the greater access to information on a phone is a Fourth Amendment problem rather than a Fifth Amendment problem. Fourth Amendment rules impose a sliding scale on how much burden the government should have to find information. Technological changes that enable more invasive searches through more information are readily met with tightening the rules. This is what happened in *Riley*, after all. The Court engaged in equilibrium-adjustment by ratcheting up Fourth Amendment protection. And I have argued in other scholarly work that courts should take similar steps in the execution of warrants, such as imposing use restrictions on nonresponsive data.[156]

In contrast, the greater amount of information that can be accessed on a computer has no obvious Fifth Amendment resonance. The testimonial aspects of entering in a password are distinct from the evidence that the unlocked device may reveal. The greater treasure does not change the testimony implicit in opening the door. And the Fifth Amendment generally acts as an absolute barrier to government access rather than a sliding scale of regulation. Technology's expansion of government power for computer searches merits a response from Fourth Amendment doctrine rather than the law of self-incrimination.

C. Compelled Decryption and the "Going Dark" Debate

A related policy argument for the Fifth Amendment standard I have advocated concerns the broader debate over "going dark" in surveillance law. The Fifth Amendment standard I propose should undercut government efforts to encourage legislation imposing more effective decryption standards. The correct Fifth Amendment standard already opens much of the door the government needs. It should go a long way toward addressing government concerns about "going dark," and it therefore can direct attention away from more draconian approaches that otherwise may be in play.

Some context may be helpful. In the last few years, law enforcement officials have frequently complained that the default use of powerful encryption tools threatens public harm by thwarting criminal investigations. The post-crypto investigative environment, they fear, is "going dark."[157] In

156. *See generally* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 TEX. TECH L. REV. 1 (2015) (mapping out how use restrictions should be implemented).

157. *See generally Going Dark: Encryption, Technology, and the Balance Between Public*

their view, this shift justifies considering new laws that either mandate the availability of a technical means of decryption or at least provide means that can facilitate access. Civil libertarians have responded that this is not so. The shift to computerization has actually created a golden age of surveillance, they argue, in which the government has access to more and more information that would have been impossible to access before.[158] New laws would therefore solve a problem that does not exist while weakening computer security.

It is too early to say how history will judge these arguments. The systematic effect of encryption on government power is a complex subject, in part because the government has a range of different encryption workarounds that may or may not work to bypass encryption.[159] It is also a rapidly evolving subject, as the technical means of encryption and its uses change from year to year. With that said, I think the Fifth Amendment standard that applies to compelled decryption has an important role in that broader debate. Knowing how the Fifth Amendment applies tells you something important about whether a more draconian solution is desirable.

The reason Fifth Amendment law can impact the debate over "going dark" is that the public interest in solving crime is something like the force of a river. Technology can influence it, but the water will flow downhill somehow. If those concerned about going dark turn out to be right, and investigators can't get into electronic devices at a high enough rate even with a warrant, the public's interest in solving crimes will encourage other alternatives. If there is no other way to ensure that the government has enough power to solve crimes involving digital evidence—which increasingly includes most crimes—then even draconian legislation may begin to seem appealing.

Adoption of the Fifth Amendment standard proposed in this Essay can act as a safety valve that lessens the pressure to enact heavy-handed legislative solutions. If my analysis is right, governments already have considerable powers to get into encrypted devices. They will often know who knows the password, and they can then get lawful court orders compelling individuals to unlock the devices or face jail time for contempt. It won't work every time, of course. Those who know the password may be unavailable or dead. They may accept contempt sanctions rather than comply. But the Fifth

Safety and Privacy: Hearing Before the S. Comm. on the Judiciary, 114th Cong. (2015), https://www.judiciary.senate.gov/meetings/going-dark-encryption-technology-and-the-balance-between-public-safety-and-privacy [https://perma.cc/8AXV-YSA4] (providing written statements and video on the "going dark" debate).

158. *See, e.g.*, Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 420 (2012) (arguing that existing technology, including encryption "is actually enabling 'a golden age of surveillance'").

159. *See generally* Kerr & Schneier, *supra* note 3 (exploring various encryption workarounds).

Amendment's right against self-incrimination does not leave prosecutors powerless to get into encrypted devices.

For too long, the debate over "going dark" has proceeded assuming the Eleventh Circuit's standard that leaves investigators unable to compel decryption unless investigators already knew details about what they would find. Recognizing that standard as wrong means that investigators have far broader decryption powers than they realize. Investigators can harness a suspect's own awareness of his passwords to gain access to devices regardless of how strongly encrypted they are. The Fifth Amendment's limits to compelled decryption are much more modest than governments may realize.

Conclusion

The rise of widespread encryption gives every person a remarkable new technological tool to ensure privacy in the contents of their electronic devices. The Fourth Amendment fully protects those contents. But the Fifth Amendment right against self-incrimination offers more modest protection against compelled decryption than some, including the Eleventh Circuit, have thought. It offers no protection against being compelled to enter a password when the government can show independent knowledge that the person knows the password. Proof of ability to enter in the password disarms the privilege against self-incrimination by rendering the testimonial aspect of production—knowledge of the password—a foregone conclusion.

New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 258—NO. 21
TUESDAY, AUGUST 1, 2017

White-Collar Crime

Expert Analysis

Executing Search Warrants In the Digital Age: 'United States v. Wey'

By **Robert J. Anello**

And **Richard F. Albert**

Three years ago, following the Supreme Court's unanimous decision in *Riley v. California* barring warrantless searches of cellphones, this column expressed the "hope that, in the digital age, the courts may breathe a bit more life back into the Fourth Amendment after years of cutting back on its protections."[1] That cautious statement of optimism also came in the wake of a U.S. Court of Appeals for the Second Circuit panel's reversal of a tax evasion conviction in *United States v. Ganias* based on the government's violation of the defendant's Fourth Amendment rights by its lengthy, unauthorized retention of his personal files located on a hard drive seized via a search warrant in an earlier investigation. Alas, the need for caution was confirmed when an en banc Second Circuit later reversed the *Ganias* panel's decision, finding that the agents executing the warrant acted in good faith, and declining to rule on whether or not Stavros Ganias' Fourth Amendment rights were violated in the first place. 824 F.3d 199 (2d Cir. 2016).

A recent high-profile Fourth Amendment victory for the defense, a June 2017 decision from Southern District of New York Judge Alison J. Nathan suppressing the fruits of two search warrants in *United States v. Wey*, (__F. Supp.3d __, 2017 WL 2574026 (S.D.N.Y. June 14, 2017)), provides another occasion to assess the state of play as prosecutors, defense counsel, and the courts continue to wrestle with applying Fourth Amendment precedents to today's "big data." In this article, we consider *Wey* in light of the Second Circuit's final opinion in *Ganias*, as well as a recent decision by Southern District of New York Judge Kathleen Forrest in *In re 650 Fifth Avenue and Related Properties*, which declined suppression despite agents' reliance on a search warrant having constitutional infirmities strikingly similar to those in *Wey*.

> 'Wey' and 'Ganias' illustrate continuing questions regarding what meets the Fourth Amendment test of "reasonableness" for searches of electronic files.

These cases demonstrate that the government's tendency to use broadly drafted search warrants to obtain documents in white-collar investigations continues to cause legal and logistical problems.[2] *Wey* and *Ganias*, in particular, illustrate continuing questions regarding what meets the Fourth Amendment test of "reasonableness" for searches of electronic files mirror-imaged at the searched premises and then later reviewed off site by government agents, as permitted by Fed. R. Crim. P. 41(e)(2)(B). For investigators striving to make a case, it is undoubtedly tempting to conduct additional searches of a vast trove

ROBERT J. ANELLO *and* RICHARD F. ALBERT *are partners at Morvillo Abramowitz Grand Iason & Anello P.C.* GRETCHAN R. OHLIG, *an attorney, assisted in the preparation of this article.*

of the subject's electronic files that have been sitting for months in the government's evidence locker. But *Wey* and *Ganias* show that succumbing to that temptation may draw the investigation into largely uncharted and perilous legal territory. Finally, these decisions also illustrate that whether a flawed search may be saved by a finding that government agents acted in "good faith" is a highly fact specific and unpredictable inquiry.

'United States v. Wey'

A Southern District of New York grand jury indicted financier Benjamin Wey in 2015 on eight counts of securities fraud, wire fraud, conspiracy to commit securities and wire fraud, and money laundering. The indictment was issued almost four years after the government executed search warrants on the offices of Wey's company, New York Global Group (NYGG), and on Wey's private apartment, seizing data from more than 24 computers and cell phones and over 4,500 pages of hard copy documents. Judge Nathan granted Wey's motion to suppress the fruits of the warrants in a detailed decision identifying serious flaws with the warrants themselves, their execution, and the government's actions after the seizure.

First, the court found that the warrants were constitutionally deficient, describing them as "facially lacking in particularity and so sweepingly broad" to be—in function if not in form—general warrants. The warrant applications submitted to the issuing magistrate judge were supported by lengthy affidavits from federal agents detailing the FBI's ongoing investigation of Wey, Wey's sister and NYGG. These affidavits described a scheme where Wey would retain an undisclosed beneficial interest in public companies through reverse merger transactions and then manipulate the trading activity of those companies in order to reap large profits.

The search warrants themselves, however, did not contain any similar detail, nor were the agents' detailed supporting affidavits attached to or specifically incorporated into the warrants, as required by relevant Supreme Court precedent. Rather, the warrants defined the property to be seized through the attachment of two exhibits. Exhibit A set forth by category the types of materials to be seized, including very broad generalized groupings such as financial records, correspondence, computers, hard drives and corporate documents, and Exhibit B set forth a list of 220 individuals and entities linked to Wey's alleged schemes to whom the items on Exhibit A had to be related.

Critically, the list of individuals and entities in Exhibit B included, at the very top, the names NYGG and Wey (and, for the apartment warrant, Wey's wife), thus having the circular effect of authorizing the seizure of effectively all conceivable documents from NYGG's offices and Wey's apartment, because all such documents could be said to relate to NYGG and/or the Weys.

In addition, the warrants failed to specify the crimes under investigation and lacked any date limitations. As a result, the court found that "those [w]arrants, by their terms, authorized essentially limitless search and seizure—targeting all documents in both the NYGG offices and the Wey apartment, regardless of their potential connection to any criminal conduct and bounded only by the illusory 'limitation' that they relate to NYGG or the Weys."

In considering whether the good faith exception could save the searches, the court also took issue with the government's execution of the warrants. The good faith exception provides that where the officers have a reasonable, good faith belief that they are acting according to legal authority, such as by relying on a search warrant that is later found to have been legally defective, the illegally seized evidence may be admissible. Pursuant to Second Circuit case law, courts are required to consider first whether the officers acted in an objectively reasonable manner. If not, they must determine whether the officers' conduct constituted isolated negligence such that the exclusion of the evidence would serve little deterrent purpose.

On the threshold question, the court found that there could be no objectively reasonable reliance on such facially unparticularized warrants, and that there were no exigent or other unusual circumstances that might excuse such fundamental flaws. As to the execution of the warrants, the court found that, without

reason, the government rushed to execute the warrants, not allowing the 17 to 20 executing agents time to be trained regarding the investigation or to review the detailed supporting affidavit, and that the agent who had drafted the affidavit provided no meaningful guidance limiting the scope of the seizure. As a result, there was extensive evidence that the government "overseized," confiscating items that were unrelated to the crimes at issue, including educational records and scholastic mementos of the Wey's children, X-rays, and family photographs.

Another critical factor in the court's rejection of the good faith argument was the government's lengthy and ever-expanding search of the electronically stored files it held after the original search. An evidentiary hearing revealed that over the course of more than three years prior to indictment, government agents searched such materials, including files previously deemed unresponsive to the warrants, for evidence of alternative charging theories and used search terms (including the name of a co-defendant) generated from witness proffer sessions held long after the warrants were executed. This material was neither included in the original warrant application nor presented to the issuing magistrate. The court opined that this conduct might be "independently violative of the Fourth Amendment," because if the government had conducted additional physical searches of NYGG's office or the Weys' apartment years later for hard copy documents deemed irrelevant and left behind in the original search, such searches would be impermissible in the absence of a new warrant. The court found that the agents' conduct "if nothing else…constitutes further evidence of the agents' culpability in making affirmative choices to treat the warrants as though they were the functional equivalent of general warrants. Such conduct can and should be deterred."

Distinguishing 'Ganias'

In finding that the good faith exception did not apply, the *Wey* court distinguished the circumstances in *Ganias*. In that case, the defendant, Stavros Ganias' accounting offices were searched pursuant to a warrant in connection with the investigation of two of his clients for fraud and theft of government property in connection with a government contract. While executing the warrant in November 2003, government agents made forensic mirror images of the hard drives of Ganias' computers.

There was extensive evidence that the government "overseized," confiscating items that were unrelated to the crimes at issue, including educational records and scholastic mementos of the Wey's children, x-rays, and family photographs.

The government completed its review of the imaged hard drives and segregated responsive documents by the end of 2004, but did not return the nonresponsive files to Ganias. In April 2006, the government obtained a new warrant to search the hard drives for Ganias' personal financial records in connection with its expanded investigation into potential tax violations. The government subsequently obtained Ganias' indictment on charges of tax evasion.

On appeal, a unanimous three-judge panel of the Second Circuit held that the fruits of the search should have been suppressed because the government had violated the Fourth Amendment's reasonableness requirement when it held onto the nonresponsive documents for 16 months before it developed probable cause to search and seize them.

The full Second Circuit reheard the case, and in May 2016, over a forceful dissent from Judge Denny Chin, the author of the original decision, the court reversed the panel's ruling. The court's decision turned on the agents' good faith, and it did not rule on the underlying Fourth Amendment issue. The opinion includes a thoughtful review of scholarly commentary on the complexities faced by the courts in analyzing searches of electronic media and notes that the government may have a legitimate interest in the preservation of digital evidence, including an entire set of the defendant's data. Significantly, the court noted that "parties with an interest in retained storage media are not without recourse" as they can make a motion for the return of property under Fed. R. Crim. P.

41(g), a process that Ganias did not pursue, formally or informally.

Critical to the Second Circuit's holding that the agents in Ganias acted in good faith was that before they undertook additional searches of files previously found unresponsive to the original warrant, they (unlike the agents in *Wey*) sought and obtained a fresh search warrant. In the process the government disclosed to a magistrate judge its lengthy retention of Ganias' records and its new theories of criminal conduct. According to the Second Circuit, the agents acted reasonably throughout the investigation, and thus their conduct fell within the good faith exception.

'In re 650 Fifth Avenue'

Another recent Southern District of New York decision also addresses many of the same seemingly easily avoided warrant-drafting mistakes present in *Wey*. The decision also demonstrates, however, that these errors need not be fatal.

In *In re 650 Fifth Avenue and Related Properties* (2017 WL 2062983 (S.D.N.Y. May 15, 2017)), a civil forfeiture action in which the United States is seeking the forfeiture of properties and assets owned by organizations tied to the Iranian government, the admissibility of evidence seized from the organizations pursuant to a subsequently invalidated warrant was at issue. In December 2008, FBI agents obtained a warrant to search offices and a storage space located at 500 Fifth Avenue that was used by the Iranian-tied organizations. Several hundred boxes of records and a number of computers were seized. Agents subsequently reviewed the seized material and returned nonresponsive documents to the owners on a rolling basis.

The Second Circuit later found that the warrant was constitutionally deficient because, like the deficient warrants in *Wey*, it did not identify the specific crimes under investigation, it did not sufficiently specify the particular categories of electronic information to be seized, and it did not include any limits in its temporal scope. Just as in *Wey*, the affidavit submitted in support of the warrant applications contained detailed information about the alleged crimes, but the affidavit was not specifically incorporated into or attached to the warrant itself.

On remand, Judge Forrest held that suppression was not the appropriate remedy. Unlike the agents in *Wey*, those who drafted and executed the warrant in *In re 650 Fifth Avenue* were acting under exigent circumstances following a member of the organization's attempt to destroy documents. In addition, the agents followed typical protocol with respect to preparing for the warrant's execution—the agent assigned to lead the search was personally familiar with the investigation and the team assembled to conduct the search reviewed the warrant and the specific items that were being sought.

Finally, there was evidence that the agents left a significant number of documents behind, which the court found to negate any claim that the agents overseized because they were unfamiliar with the limits of the warrant. Based on these facts, Judge Forrest found that the agents acted in good faith. The court also concluded that all of the documents at issue would have been inevitably discovered.

Conclusion

These recent decisions illustrate that in the era of ever-increasing data storage and ever-evolving technology, questions regarding what meets the Fourth Amendment's baseline requirement of reasonableness in the execution of search warrants will continue to vex prosecutors, defense counsel, and courts in white collar criminal cases.

1. See Robert J. Anello and Richard F. Albert, "When the Government Searches Your Hard Drives," N.Y.L.J. (Aug. 5, 2014).

2. This column has previously discussed one such category of logistical problems—the government's use of taint teams to segregate potentially privileged documents. See Robert J. Anello and Richard F. Albert, "Government Searches: The Trouble With Taint Teams," N.Y.L.J. (Dec. 6, 2016).

Biographies

Daniel R. Alonso, a founding member of the New York American Inn of Court, is a three-time recipient of the Inn's Innie Award, for his portrayals of figures vaguely reminiscent of Donald Trump, Phil Donahue, and Professor Kingsfield. He has studied acting and improv at Cornell University, HB Studio in Greenwich Village, and Manhattan Comedy School, and appeared on stage with Cornell's Whistling Shrimp improv troupe. In his spare time, Dan practices law at Buckley LLP, where he became a partner in early 2020 after a long career as a federal and state prosecutor and in other positions in the public and private sectors. As relevant to tonight's performance, he was proud to have proposed the creation of the Thomas E. Dewey Medal, awarded each year since 2005 by the New York City Bar Association to outstanding Assistant District Attorneys practicing in New York City, and he previously co-chaired the Historical Trial Team's production of *People v. Jimmy Hines,* the most prominent of Dewey's cases while he served as District Attorney of New York County.

Laurie Brecher is a litigator who has focused her practice on white-collar criminal and regulatory enforcement defense and prosecutions, internal investigations, and complex federal and state civil litigation. She served for a decade as an AUSA in the Criminal Division of the U.S. Attorney's Office for the Southern District of NY, holding several positions, including Chief of the General Crimes Unit and Senior Trial Counsel of the Securities & Commodities Fraud Task Force. After her government service, she was Deputy General Counsel, Litigation & Regulatory for Pitney Bowes, Inc. Prior to her government service, she was a litigation associate at Cravath, Swaine & Moore, and Howard, Darby & Levin. (now Covington & Burling). She was also honored to have served as a law clerk to the Hon. Jon O. Newman, U.S. Court of Appeals for the Second Circuit. She earned her law degree with highest honors from New York University School of Law (1983), where she was the Senior Articles Editor of the *NYU Law Review.* She received her undergraduate degree, *summa cum laude*, from Union College in 1980, where she was elected to *Phi Beta Kappa.* She has been active in the NY City Bar Assn. (former member of International Law and Judiciary Committees) and the ABA (former Chair of Criminal Litigation Committee and former Division Director for the Litigation Section). Among her public service commitments, she is a college coach for Yonkers Partners in Education, a board and founding member of Friends of Chappaqua Performing Arts Center, and working on a Domestic Violence Project with a domestic abuse services agency in CT.

Glenn Colton is a partner in the White Collar and Government Investigations practice at Arent Fox. Glenn represents individuals, companies and boards of directors in white collar criminal and civil enforcement investigations. Glenn previously served as an Assistant United States Attorney both the civil and criminal divisions in the Southern District of New York. In addition to his law practice, Glenn is a sports radio host on SiriusXM and one of approximately 20 members of the Fantasy Sports and Gaming Association Hall of Fame.

Mary Diaz is a law clerk at Walden Macht & Haran LLP where she focuses on white collar defense and investigations. She is a member of the Hispanic National Bar Association and the Cafecitos Network and enjoys international travel, cooking, dancing, and running during her free time. After graduating from Wesleyan University with a Bachelor of Arts degree in Government in 2014, Mary earned her Juris Doctor from Fordham University School of Law in 2020. While at Fordham Law she was a member of the Fordham Moot Court, *Environmental Law Review,* Stein Scholars for Public Interest, LALSA, Fordham Law Advocates for Voter Rights, and held internships at the U.S. Securities and Exchange Commission and Department of Justice.

Prior to law school, Mary spent three years as a paralegal at the U.S. Attorney's Office for the Southern District of New York in the Securities and Commodities Fraud Unit. Mary is a new member of the Inn and is looking forward to meeting everyone and collaborating on programs.

Eugene Frenkel is an attorney in the public sector, protecting consumers and markets from fraud. He has helped negotiate settlements in the hundreds of millions of dollars with companies and stopped several businesses with harmful and unfair practices, including several that attempted to take advantage of the health crisis. In his downtime, Eugene serves as co-program chair for the Inn and as co-chair of the Young Lawyers Section at NYCLA. He enjoys reading fantasy books and is always ready to talk about Star Wars or Marvel tv shows or movies.

Milosz Gudzowski is a Trial Attorney at the Department of Justice – Antitrust Division. Milosz has been at the Antitrust Division for ten years and has prosecuted both criminal and civil antitrust matters in a variety of industries, including construction, municipal contracting, airlines, telecommunications, and automotive. Milosz likes to play tennis and lives on the upper east side in Manhattan.

Meredith Jones is General Counsel of New York City Economic Development Corporation. NYCEDC's mission is to create shared prosperity across the City's five boroughs by strengthening neighborhoods and growing good jobs. It is the City's official economic development corporation. Before joining NYCEDC, she was a transactional lawyer in Palo Alto, California. Prior thereto, she served as Chief of the Cable Services Bureau of the Federal Communication Commission in Washington, D.C., involved in multichannel video and telecom competition issues. Before joining the FCC, she was General Counsel to the National Oceanic and Atmospheric Administration in Washington, D.C., which includes the National Weather Service and is the nation's trustee for marine mammals and anadromous fish and the lead agency for oceanic and atmospheric issues. She was a member of the legal team of the Bechtel group of companies in San Francisco, California and was a partner in a San Francisco law firm. Jones began her legal career in New York City.

Eugene Meyers is a Litigation Partner at Meister Seelig & Fein LLP. He concentrates his practice on the representation of clients involved in complex commercial litigation. His representations have included real estate developers, private equity investors, media companies, energy suppliers and industrial manufacturers. Mr. Meyers has appeared before federal courts throughout the United States and the state courts of New York and New Jersey. He has also represented clients in alternative dispute resolution forums, including domestic and international arbitrations.

David Pohl is a business and civil litigator at his firm, Parker Pohl LLP. Prior to co-founding Parker Pohl in 2017, he was solo for seven years. Over the past ten years, David has been fortunate to represent hundreds of individuals, as well as businesses big and small, in a variety of disputes and settings – from pre-litigation negotiations to trial. After graduating from NYU School of Law in 2005, David cut his teeth at a major international law firm and an elite litigation boutique. David also clerked for the Honorable Nina Gershon in the Eastern District of New York. During law school at NYU, David's most meaningful studies included a clinical program at the Equal Justice Initiative in Montgomery, Alabama, an organization committed to a

variety of racial and economic justice issues. When not practicing law, David hangs out with his wife and kids and co-produces a successful, annual charity concert in his home community – a rock'n'roll spectacle (in which he also performs) that has raised tens of thousands of dollars for the public school music program.

Jared M. Rosen is an Assistant District Attorney with the Bronx District Attorney's Office. As an ADA with the Public Integrity Bureau, he is involved in the prosecution and investigation of corruption committed by public servants, including government employees and appointed and elected officials, as well as excessive uses of force and misconduct by police officers. He was formerly in the Rikers Island Prosecution Bureau, where he was involved in the investigation and prosecution of criminal activity in New York City jails, including gang assaults and contraband smuggling. Previously, Mr. Rosen was an Executive Agency Counsel and the Market Manager at the Business Integrity Commission, an agency tasked with eliminating organized crime influence, anti-competitive practices and corruption from New York City's trade-waste industry and public wholesale markets. Prior to this, Mr. Rosen was an Assistant Counsel at the Waterfront Commission of New York Harbor, a bi-state agency created to eliminate corruption and unfair hiring practices in the Port of New York/New Jersey. Mr. Rosen graduated from Cornell University with a B.S. in Industrial & Labor Relations and received his law degree from Brooklyn Law School.

Steven Tugander is a Trial Attorney in the New York Office of the United States Justice Department's Antitrust Division and has investigated and prosecuted numerous criminal antitrust cases affecting various industries in jurisdictions located throughout the Northeast. In 2017 and 2018, Mr. Tugander served as the Antitrust Division's Criminal Special Projects Coordinator, reporting directly to the Deputy Assistant Attorney General and the Director of Criminal Enforcement. Mr. Tugander has served on the Executive Committee of the New York State Bar Association's Antitrust Law Section since January 2000. He served as Chair of the Section from January 2005 through January 2006, having previously served as Vice-Chair and Secretary of the Section. In addition, he also currently serves on the Section's Cartel and Criminal Practice sub-committee. Since 2004, Mr. Tugander has been a member of the New York American Inn of Court. During his tenure with the Inn, Mr. Tugander has organized a number of Continuing Legal Education programs related to various white collar criminal law topics. In December 2017, Mr. Tugander was honored as the first recipient of Antitrust Division's Ralph T. Giordano Award. The award recognizes excellence in cartel enforcement.