CYBER-PRIVACY AND THE INTERNET

Theodore Roosevelt Inn of Court
February 3, 2020

Elizabeth E. Schlissel, Esq.
Thomas A. O'Rourke, Esq.
Andrew M. Thaler, Esq.
Ellen Tobin, Esq.
Emma Bausert
Kimberly E. Capuder
Ron Eniclerico
NallyAnn Scaturro

TABLE OF CONTENTS

Tannenbaum Helpern
Syracuse & Hirschtritt LLP

Elizabeth E. Schlissel

ASSOCIATE
schlissel@thsh.com
212-508-6714
LinkedIn

Practice Areas

→ Employment Law
→ Criminal Defense

Areas of Focus

→ Employment Law

Biography

Elizabeth Schlissel is an associate in Tannenbaum Helpern's Employment Law practice representing clients in employment litigation, investigation, regulation, and other aspects of employment law.

Employment Litigation

Elizabeth represents companies in all types of employment litigation in state and federal court including wage and hour matters, discrimination, workplace harassment, retaliation, hostile work environment, breach of employment contracts and restrictive covenants, and failure to accommodate disabilities.

Workplace Investigations

Elizabeth conducts internal workplace investigations concerning allegations of sexual harassment, discrimination, retaliation, employee misconduct, workplace assault, and employee theft. Elizabeth's fact-finding investigations include interviewing witnesses, obtaining and reviewing documents and electronic evidence, drafting comprehensive investigative reports, and guiding employers with regard to corrective action in order to minimize exposure to liability.

Employment Trainings

Elizabeth regularly conducts on-site trainings with employees and management in order to prevent sexual harassment and discrimination and to promote appropriate responses by management in the event of workplace complaints.

Employment Counseling

Elizabeth counsels employers, management teams, and HR executives regarding compliance with federal, state, and local employment laws and regulations. Counseling includes advising clients on a daily basis regarding personnel issues, wage and hour compliance, and preventing, investigating and responding to discrimination and sexual harassment complaints. In addition, Elizabeth regularly works with employers to draft, review, and update employee handbooks and policies.

State and Federal Department of Labor Audits

Elizabeth also represents employers in connection with audits and investigations conducted by the U.S. and New York State Department of Labor.

⊕ Education

College:

- *College*: Boston University

Law School:

- *Law School*: Hofstra University School of Law

⊕ Prior Affiliations

- Elizabeth previously served as an Assistant District Attorney for the Nassau County District Attorney's Office, serving under District Attorney Kathleen Rice, prosecuting misdemeanors and felonies.

⊖ Memberships

Professional:

- Theodore Roosevelt American Inn of Court, Executive Committee Member
- Long Island Association Young Professionals Committee
- Nassau County Bar Association, Labor and Employment Committee

⊕ Bar Admissions

- New York State
- U.S. District Court for the Eastern District of New York
- U.S. District Court for the Southern District of New York

Case Studies

→ Investigation of Alleged Sexual Assault
→ Sexual Harassment and Retaliation Investigation

Publications

→ NY Bans Reproductive Health Decision Discrimination and Imposes Obligations on Employers
→ New York and New Jersey Ban Employers from Asking About Salary History
→ NY Broadens Workplace Sexual Harassment and Discrimination Protections
→ Lactation Stations: Accommodation Sensation Sweeping the Nation!
→ NYC Passes Legislation to Ban Pre-Employment Drug Testing for Marijuana
→ $15 Minimum Wage Coming to New Jersey
→ Video: Avoiding Sexual Harassment Complaints at Summer Outings
→ Video: How employers can avoid complaints of harassment at firm functions
→ How Can-a-Biz Handle Employees Using Cannabis
→ New York Minimum Wage and Exempt Employee Salary Thresholds Set to Increase in 2019
→ Holiday Party Liability: Keep Your Employees Off The Naughty List

Events

→ An Employer's Guide to Managing Workplace Harassment Complaints | Lawline · 03.10.2020
→ 5 Key Employment Practices Employers Need to Know About in the New Year · 02.06.2020
→ Ethics 101 for In-House Counsel · 11.21.2019
→ New Trends and Developments in the Hiring and Onboarding Process | Lawline · 09.26.2019
→ NY Employment Laws: What To Know For 2019 · 03.28.2019

Thomas A. O'Rourke
Bodner & O'Rourke
425 Broadhollow Rd.
Melville, N. Y. 11747
631-249-7500

Thomas A. O'Rourke is a founding partner of the firm Bodner & O'Rourke. Mr. O'Rourke's practice involves all areas of patent, trademark and copyright law. For over thirty years he has been registered to practice before the United States Patent & Trademark Office. Mr. O'Rourke has counseled clients regarding the procurement and enforcement of patents, trademarks, copyrights and trade secrets in a variety of technologies including mechanical, and computer technology. In addition, his practice involves domestic and international technology transfer, acquisition and licensing. He is a member of the bar of the States of New York and California. He has also been admitted to numerous Federal District Courts and Courts of Appeal across the country including, the Court of Appeals for the Federal Circuit.

Mr. O'Rourke has been a member of the Board of Directors of the New York Intellectual Property Law Association. Mr. O'Rourke is Co-Chairman of the Suffolk County Bar Association's Committee on Intellectual Property Law and has been a member of the Advisory Board of the Licensing Journal. He has lectured on Intellectual Property Law at numerous Continuing Legal Education programs, including programs presented by the American Bar Association, the Connecticut Intellectual Property Law Association and the Suffolk County Bar Association. He was also the Editor of the New York Intellectual Property Law Association Bulletin and the author of numerous articles on patents, trademarks and copyrights for the New York Intellectual Property Law Association. Mr. O'Rourke has also authored monthly articles on intellectual property law licensing, which have appeared in the Licensing Journal. Mr. O'Rourke has also been named as a Super Lawyer.

Mr. O'Rourke has a B.S. degree from Fordham University and obtained his J.D. degree from St. John's University School of Law, where he was a member of the Law Review.

ANDREW M. THALER ▪ THALER LAW FIRM PLLC

▪ ***Bankruptcy*** ▪ ***Mediation*** ▪

675 Old Country Road, Westbury, NY 11590
516-279-6700 • ATHALERLAW.com

Andrew M. Thaler

Founding Member
athaler@athalerlaw.com

PRACTICE AREAS
Bankruptcy, Creditors' Rights
Bankruptcy Reorganization
Mediation

ANDREW M. THALER

Andrew Thaler is founding Member of the Thaler Law Firm. With over 35 years of experience in the bankruptcy and insolvency field, his practice focuses on a wide spectrum of matters including representation of debtors, creditors, trustees and creditor committees in commercial Chapter 11 and 7 cases, consumers in Chapter 7 and 13 cases, and various situated parties in complex bankruptcy litigation and insolvency service businesses, manufacturing and retail companies, and financial institutions. As a federally appointed Panel 7 Bankruptcy Trustee for the United States Bankruptcy Court for the Eastern District of New York since 1990, Andrew has presided over twenty thousand bankruptcy cases. In addition to his bankruptcy practice, he also serves as a Mediator/Neutral for the United States Bankruptcy Court, Eastern District and the Mediation Panel of the Commercial Division of the Supreme Court, Nassau County. When businesses or individuals encounter financial difficulties, Andrew helps analyze the situation presented to determine the client's best course of action. His reputation for thoroughness, concern, resourcefulness, and fairness enables his clients to confidently make decisions throughout all stages of their legal issue.

Andrew is active in the Nassau County Bar Association, where he has served as a member of the Board of Directors, former Dean of the Nassau Academy of Law and Chair of the Bankruptcy Law and Alternative Dispute Resolution Committees. He has lectured on bankruptcy/insolvency topics for the Nassau Academy of Law, the National Business Institute, The New York State Society of Certified Public Accountants and First American Title Insurance Company of New York. In 2011 Andrew was appointed to the New York City Bar Association's Committee on Bankruptcy & Corporate Reorganization. He is Past President (2010) of The Theodore Roosevelt American Inn of Court.

Andrew is rated "AV Preeminent" by Martindale-Hubbell, the highest level in professional excellence. He has been selected to the Super Lawyers listing the category of bankruptcy & creditor rights in the New York Metro area since 2012. He has annually been recognized by L.I. Pulse Magazine as one of the region's "Top Legal Eagles" since 2010. He has an AVVO Rating of 10-Superb.

Attorneys > Ellen Tobin

Ellen Tobin

Ellen Tobin is a Partner in the Firm's Litigation Department, representing individuals and businesses in federal and state court actions and arbitrations. Ellen's practice focuses on complex commercial cases including contract and real estate matters, business and partnership disputes, accounting and securities fraud and bankruptcy litigation. Ellen is active in the legal community, serving as Vice Chair of the Federal Courts Committee of the Nassau County Bar Association. Ellen was recently named to *Long Island Business News'* "Who's Who of Women in Professional Services" (August 2016) and is a 2016 Super Lawyers "Rising Star" recognized for her securities and business litigation work. Also recognized in 2017 and 2018 Super Lawyers for Business Litigation.

Prior to joining the Firm, Ellen worked in the Manhattan office of a prominent international law firm, where she represented clients in federal and state courts, government investigations, arbitrations and matters before the Department of the Justice, the Securities and Exchange Commission and the Public Company Accounting Oversight Board, in complex commercial cases and in antitrust and maritime and intellectual property matters. For two years Ellen served as a Law Clerk for the Honorable A. Kathleen Tomlinson of the U.S. District Court for the Eastern District of New York.

Ellen is also committed to serving her community. She volunteers with Surf For All, an amazing not-for-profit that provides surfing programs for children with disabilities. She has done extensive pro bono work advocating for children and indigent parents in family court disputes on behalf of the Children's Law Center and the Brooklyn Family Defense Practice. She is a proud member of The Energeia Partnership at Molloy College.

Ellen received her Juris Doctor degree in 2005 from the University of Pennsylvania. In 2001 Ellen received a Bachelor of Arts degree from the University of Pennsylvania, from which she graduated *magna cum laude* and with Distinction in International Relations.

Ellen is admitted to practice law in New York State, the United States Court of Appeals for the Second Circuit, and the United District Courts for the Southern and Eastern Districts of New York and is an active member of the Nassau County Bar Association and Chair of the Federal Courts Committee.
Ellen has received the following honors:
Premiere Business Woman on Long Island
Long Island Business News Who's Who in Women in Professional Services

Emma Bausert
emma.bausert18@stjohns.edu

Emma Bausert is a second-year law student at St. John's University School of Law. She graduated *cum laude* from Fordham University in 2017 with her bachelor's degree in International Political Economy and International Humanitarian Studies. At St. John's School of Law, Emma is a staff member of the Journal of Civil Rights and Economic Development. She is also an advocate for the Polestino Trial Advocacy Institute. She received an award for "Best Cross Examination" in the Brian Peterson Memorial First-Year Mock Trial Competition. Emma was a semi-finalist in the Queens District Attorney's Office Mock Trial Competition this past fall. This spring, she will be competing in the American Association for Justice Student Trial Advocacy Competition. Emma was an intern at Morris, Duffy, Alonso & Faley last summer. She completed an externship with the Manhattan District Attorney's Special Victim's Bureau this past fall, and will be interning with the Bronx District Attorney's Office this upcoming summer. Emma is thrilled and honored to be a student representative at the Nassau County Bar Association's Theodore Roosevelt American Inn of Court.

KIMBERLY E. CAPUDER
125 Hampton Avenue, Albertson, NY 11507
516-508-1929 ▪ kimberly.capuder18@stjohns.edu

KIMBERLY E. CAPUDER

Kimberly Capuder is a second year law school student at St. John's University School of Law. She graduated *summa cum laude* from Fordham University in 2018 with her Bachelor's Degree in both English and Communications & Media Studies.

During her time at St. John's Law School, Kimberly has interned for the Honorable Joseph F. Bianco of the U.S. Court of Appeals for the Second Circuit and for the St. John's Law Consumer Justice for the Elderly: Litigation Clinic. She works as a Teaching Assistant and Research Assistant for various professors, is a staff member on *St. John's Law Review*, a member of the Moot Court Honor Society, and is the Secretary for the St. John's Student Division of the Federal Bar Association.

Kimberly is looking forward to working as a Summer Associate at Latham & Watkins, LLP this coming summer. She is excited and grateful to serve as a student representative at the Nassau County Bar Association's Theodore Roosevelt American Inn of Court.

Ron Eniclerico

Ron Eniclerico entered law school at St. John's in 2018 after many years in the publishing industry; a project that involved writing and editing material on Supreme Court decisions sparked his interest in the law and led him to pursue it as a career. At St. John’s, Ron is a member of the Moot Court Honor Society and the Journal of Civil Rights and Economic Development. He is looking forward to spending his 2L summer with the criminal law division of the Legal Aid Society in Brooklyn. He has also developed an interest in intellectual property and copyright law in particular. Ron is pleased and honored to be a part of the Nassau County Bar Association's Theodore Roosevelt American Inn of Court program.

NallyAnn Scaturro
37 Brixton Road, Garden City, NY 11530
516-306-0643 ▪ nally.scaturro11@stjohns.edu

NallyAnn Scaturro

NallyAnn Scaturro is a second year law school student at St. John's University School of Law. She graduated *magnum cum laude* from Providence College in 2016 with her Bachelor's Degree in both English and American Studies. She also studied Shakespeare in a one-on-one tutorial with Sir Jonathan Bate at Oxford University. Subsequently, she earned a Masters in History from Trinity College Dublin.

During her time at St. John's Law School, NallyAnn has interned for the Honorable Leonard Livote of the New York Supreme Court Civil Term in Queens County and for the St. John's Law Securities Arbitration Clinic. She is a staff member on *American Bankruptcy Institute Law Review*, a member of the Dispute Resolution Society, and is the Special Events Coordinator for the St. John's Children's Rights Society.

NallyAnn is looking forward to working as a Summer Intern with the Department of Justice, Criminal Division, Fraud Section this coming summer. She is excited and grateful to serve as a student representative at the Nassau County Bar Association's Theodore Roosevelt American Inn of Court.

The New York Times https://nyti.ms/33lqoKi

Your DNA Profile is Private? A Florida Judge Just Said Otherwise

Privacy experts say a warrant granted in Florida could set a precedent, opening up all consumer DNA sites to law enforcement agencies across the country.

By Kashmir Hill and Heather Murphy

Published Nov. 5, 2019 Updated Dec. 30, 2019

For police officers around the country, the genetic profiles that 20 million people have uploaded to consumer DNA sites represent a tantalizing resource that could be used to solve cases both new and cold. But for years, the vast majority of the data have been off limits to investigators. The two largest sites, Ancestry.com and 23andMe, have long pledged to keep their users' genetic information private, and a smaller one, GEDmatch, severely restricted police access to its records this year.

Last week, however, a Florida detective announced at a police convention that he had obtained a warrant to penetrate GEDmatch and search its full database of nearly one million users. Legal experts said that this appeared to be the first time a judge had approved such a warrant, and that the development could have profound implications for genetic privacy.

"That's a huge game-changer," said Erin Murphy, a law professor at New York University. "The company made a decision to keep law enforcement out, and that's been overridden by a court. It's a signal that no genetic information can be safe."

DNA policy experts said the development was likely to encourage other agencies to request similar search warrants from 23andMe, which has 10 million users, and Ancestry.com, which has 15 million. If that comes to pass, the Florida judge's decision will affect not only the users of these sites but huge swaths of the population, including those who have never taken a DNA test. That's because this emerging forensic technique makes it possible to identify a DNA profile even through distant family relationships.

Using public genealogy sites to crack cold cases had its breakthrough moment in April 2018 when the California police used GEDmatch to identify a man they believe is the Golden State Killer, Joseph James DeAngelo.

After his arrest, dozens of law enforcement agencies around the country rushed to apply the method to their own cases. Investigators have since used genetic genealogy to identify suspects and victims in more than 70 cases of murder, sexual assault and burglary, ranging from five decades to just a few months old.

Most users of genealogy services have uploaded their genetic information in order to find relatives, learn about ancestors and get insights into their health — not anticipating that the police might one day search for killers and rapists in their family trees. After a revolt by a group of prominent genealogists, GEDmatch changed its policies in May. It required law enforcement agents to identify themselves when searching its database, and it gave them access only to the profiles of users who had explicitly opted in to such queries. (As of last week, according to the GEDmatch co-founder Curtis Rogers, just 185,000 of the site's 1.3 million users had opted in.)

Like many others in law enforcement, Detective Michael Fields of the Orlando Police Department was disappointed by GEDmatch's policy shift. He had used the site last year to identify a suspect in the 2001 murder of a 25-year-old woman that he had spent six years trying to solve. Today, working with a forensic consulting firm, Parabon, Detective Fields is trying to solve the case of a serial rapist who assaulted a number of women decades ago.

In July, he asked a judge in the Ninth Judicial Circuit Court of Florida to approve a warrant that would let him override the privacy settings of GEDmatch's users and search the site's full database of 1.2 million users. After Judge Patricia Strowbridge agreed, Detective Fields said in an interview, the site complied within 24 hours. He said that some leads had emerged, but that he had yet to make an arrest. He declined to share the warrant or say how it was worded.

Detective Fields described his methods at the International Association of Chiefs of Police conference in Chicago last week. Logan Koepke, a policy analyst at Upturn, a nonprofit in Washington that studies how technology affects social issues, was in the audience. After the talk, "multiple other detectives and officers approached him asking for a copy of the warrant," Mr. Koepke said.

DNA policy experts said they would closely watch public response to news of the warrant, to see if law enforcement agencies will be emboldened to go after the much larger genetic databases.

"I have no question in my mind that if the public isn't outraged by this, they will go to the mother lode: the 15-million-person Ancestry database," Professor Murphy said. "Why play in the peanuts when you can go to the big show?"

Yaniv Erlich, the chief science officer at MyHeritage, a genealogy database of around 2.5 million people, agreed. "They won't stop here," he said.

Because of the nature of DNA, every criminal is likely to have multiple relatives in every major genealogy database. Without an outcry, Professor Murphy and others said, warrants like the one obtained by Detective Fields could become the new norm, turning all genetic databases into law enforcement databases.

Not all consumer genetics sites are alike. GEDmatch and FamilyTreeDNA make it possible for anyone to upload his or her DNA information and start looking for relatives. Law enforcement agents began conducting genetic genealogy investigations there not because these sites were the biggest but because they were the most open.

Ancestry.com and 23andMe are closed systems. Rather than upload an existing genetic profile, users send saliva to the companies' labs, and then receive information about their ancestry and health. For years, fearful of turning off customers, the companies have been adamant that they would resist giving law enforcement access to their databases.

Both sites publish transparency reports with information about subpoenas and search warrants they receive. 23andMe says it has received seven data requests relating to 10 customers and has not released any data. Ancestry.com said in its 2018 report that it had received 10 "valid law enforcement requests" that year and complied with seven, but that all the cases involved "credit card misuse, fraud and identity theft," not requests for genetic information.

Genetic genealogy experts said that until now, the law enforcement community had been deliberately cautious about approaching the consumer sites with court orders: If users get spooked and abandon the sites, they will become much less useful to investigators. Barbara Rae-Venter, a genetic genealogist who works with law enforcement, described the situation as "Don't rock the boat."

FamilyTreeDNA permits law enforcement searches of its database of two million users for certain types of crimes.

Ancestry.com did not respond to a request for comment on the Florida search warrant. A spokesman for 23andMe, Christine Pai, said in an emailed statement, "We never share customer data with law enforcement unless we receive a legally valid request such as a search warrant or written court order. Upon receipt of an inquiry from law enforcement, we use all practical legal measures to challenge such requests in order to protect our customers' privacy."

Detective Fields said he would welcome access to the Ancestry.com and 23andMe databases. "You would see hundreds and hundreds of unsolved crimes solved overnight," he said. "I hope I get a case where I get to try."

The New York Times | https://nyti.ms/2KNWrZd

Banks and Retailers Are Tracking How You Type, Swipe and Tap

By Stacy Cowley

Aug. 13, 2018

When you're browsing a website and the mouse cursor disappears, it might be a computer glitch — or it might be a deliberate test to find out who you are.

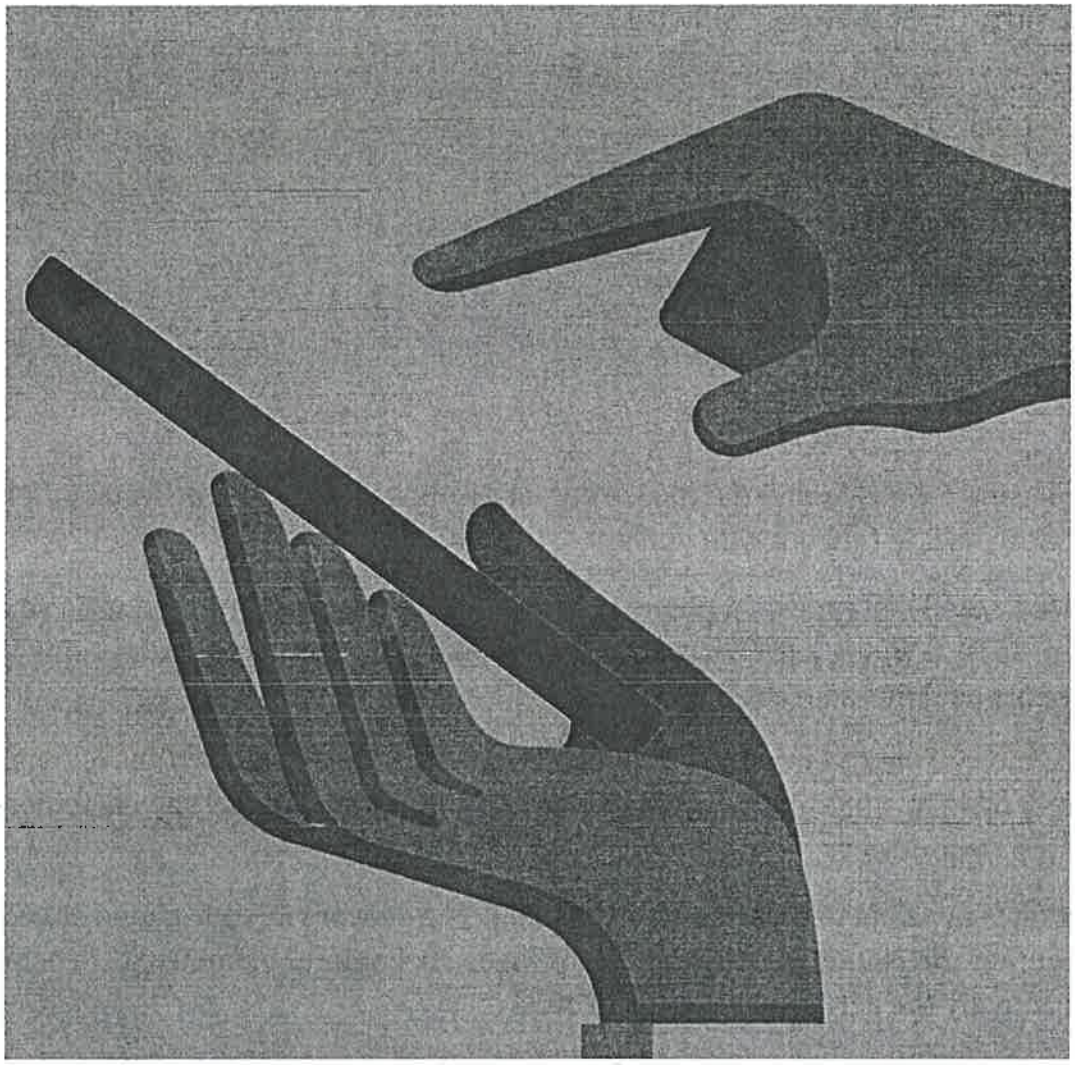
The way you press, scroll and type on a phone screen or keyboard can be as unique as your fingerprints or facial features. To fight fraud, a growing number of banks and merchants are tracking visitors' physical movements as they use websites and apps.

Some use the technology only to weed out automated attacks and suspicious transactions, but others are going significantly further, amassing tens of millions of profiles that can identify customers by how they touch, hold and tap their devices.

The data collection is invisible to those being watched. Using sensors in your phone or code on websites, companies can gather thousands of data points, known as "behavioral biometrics," to help prove whether a digital user is actually the person she claims to be.

To security officials, the technology is a powerful safeguard. Major data breaches are a near-daily occurrence. Cyberthieves have obtained billions of passwords and other sensitive personal information, which can be used to steal from customers' bank and shopping accounts and fraudulently open new ones.

"Identity is the ultimate digital currency, and it's being weaponized at an industrial scale," said Alisdair Faulkner, one of the founders of ThreatMetrix, which makes fraud detection software for large merchants and financial companies. Many of his company's customers are now using or testing behavioral biometric tools, he said.



The angle at which you hold your device is one of the many biometric markers that can be measured. Andrew Roberts

Privacy advocates view the biometric tools as potentially troubling, partly because few companies disclose to users when and how their taps and swipes are being tracked.

"What we have seen across the board with technology is that the more data that's collected by companies, the more they will try to find uses for that data," said Jennifer Lynch, a senior lawyer for the Electronic Frontier Foundation. "It's a very small leap from using this to detect fraud to using this to learn very private information about you."

The Royal Bank of Scotland, one of the few banks that will talk publicly about its collection of biometric behavioral data, started testing the technology two years ago on private banking accounts for wealthy customers. It is now expanding the system to all of its 18.7 million business and retail accounts, according to Kevin Hanley, the bank's director of innovation.

When clients log in to their Royal Bank of Scotland accounts, software begins recording more than 2,000 different interactive gestures. On phones, it measures the angle at which people hold their devices, the fingers they use to swipe and tap, the pressure they apply and how quickly they scroll. On a computer, the software records the rhythm of their keystrokes and the way they wiggle their mouse.

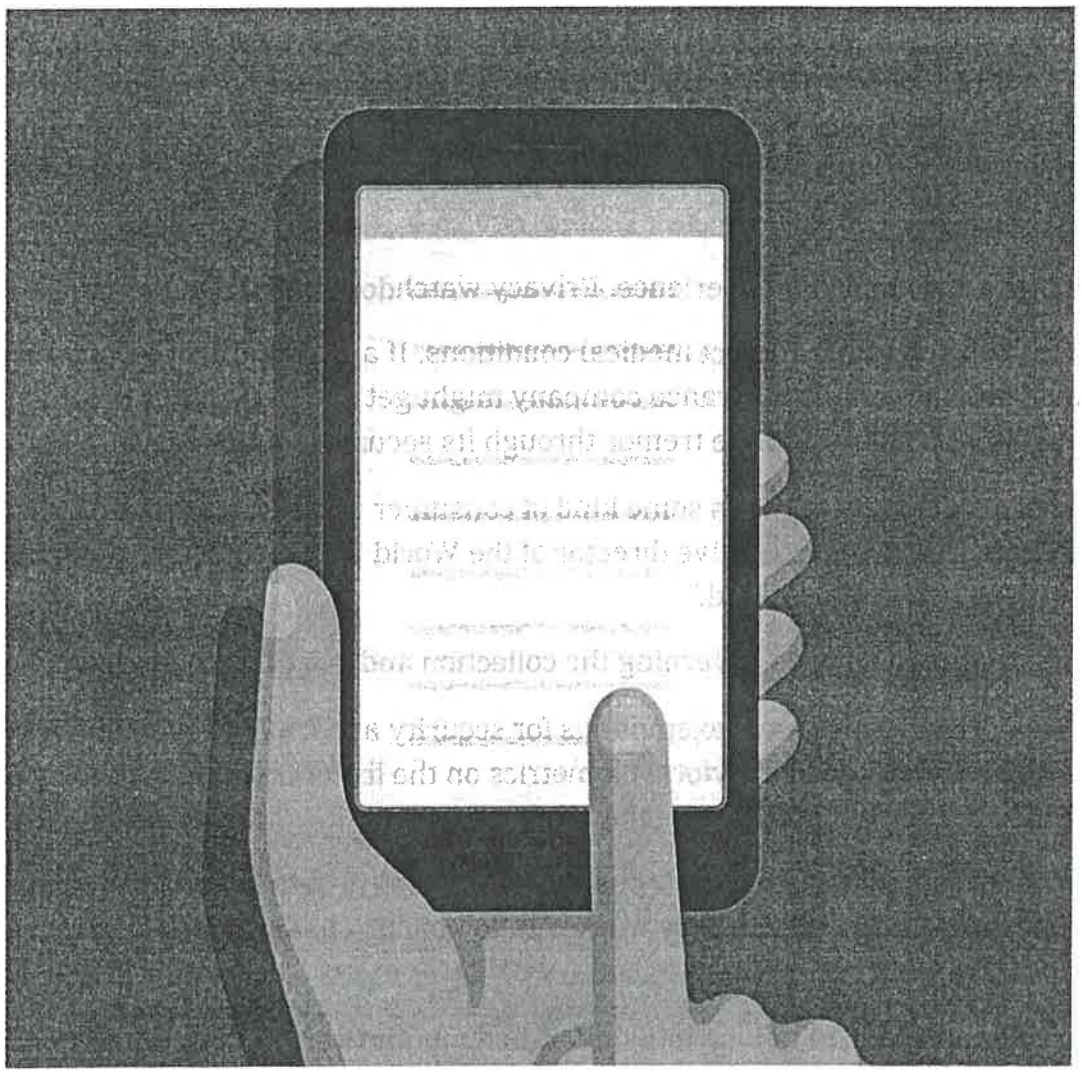
R.B.S. is using software designed by a small New York company called BioCatch. It builds a profile on each person's gestures, which is then compared against the customer's movements every time they return. The system can detect impostors with 99 percent accuracy, BioCatch says.

A few months ago, the software picked up unusual signals coming from one wealthy customer's account. After logging in, the visitor used the mouse's scroll wheel — something the customer had never done before. Then the visitor typed on the numerical strip at the top of a keyboard, not the side number pad the customer typically used.

Alarm bells went off. The R.B.S. system blocked any cash from leaving the customer's account. An investigation later found that the account had been hacked, Mr. Hanley said.

"Someone was trying to set up a new payee and transfer a seven-figure sum," he said. "We were able to intervene in real time and stop that from happening."

That case was unusually blatant. A user's behavior isn't constant; people act differently when they're tired, injured, drunk, distracted or in a hurry. The way people type at an office desk is distinct from when they're slumped on their sofa at home.



Biometric software can also determine the pressure you tend to apply to your phone when you tap and type. Andrew Roberts

Behavioral monitoring software churns through thousands of elements to calculate a probability-based guess about whether a person is who they claim. Two major advances have fed its growing use: the availability of cheap computing power and the sophisticated array of sensors now built into most smartphones.

The system's unobtrusiveness is part of its appeal, Mr. Hanley said. Traditional physical biometrics, like fingerprints or irises, require special scanning hardware for authentication. But behavioral traits can be captured in the background, without customers doing anything to sign up.

BioCatch occasionally tries to elicit a reaction. It can speed up the selection wheel you use to enter data like dates and times on your phone, or make your mouse cursor disappear for a fraction of a second.

"Everyone reacts a little differently to that," said Frances Zelazny, BioCatch's chief strategy and marketing officer. "Some people move the mouse side to side; some people move it up and down. Some bang on the keyboard."

Because your reaction is so individual, it's hard for a fraudulent user to fake. And because customers never know the monitoring technology is there, it doesn't impose the kind of visible, and irritating, roadblocks that typically accompany security tests. You don't need to press your thumb on your phone's fingerprint reader or type in an authentication code.

"We don't have to sit people down in a room and get them to type under perfect laboratory conditions," said Neil Costigan, the chief executive of BehavioSec, a Palo Alto, Calif., company that makes software used by many Nordic banks. "You just watch them, silently, while they go about their normal account activities."

Businesses call that a "frictionless" experience. Privacy watchdogs call it dangerous.

Biometric systems can sometimes detect medical conditions. If a customer with a once-steady hand develops a tremor, her automobile insurance company might get worried. That's potentially a problem if the customer's bank, which detected the tremor through its security software, is also her insurer.

"This is the kind of data that usually has some kind of consumer protections around it, but here there's none at all," said Pam Dixon, the executive director of the World Privacy Forum. "Companies are using these systems with no notice of any kind."

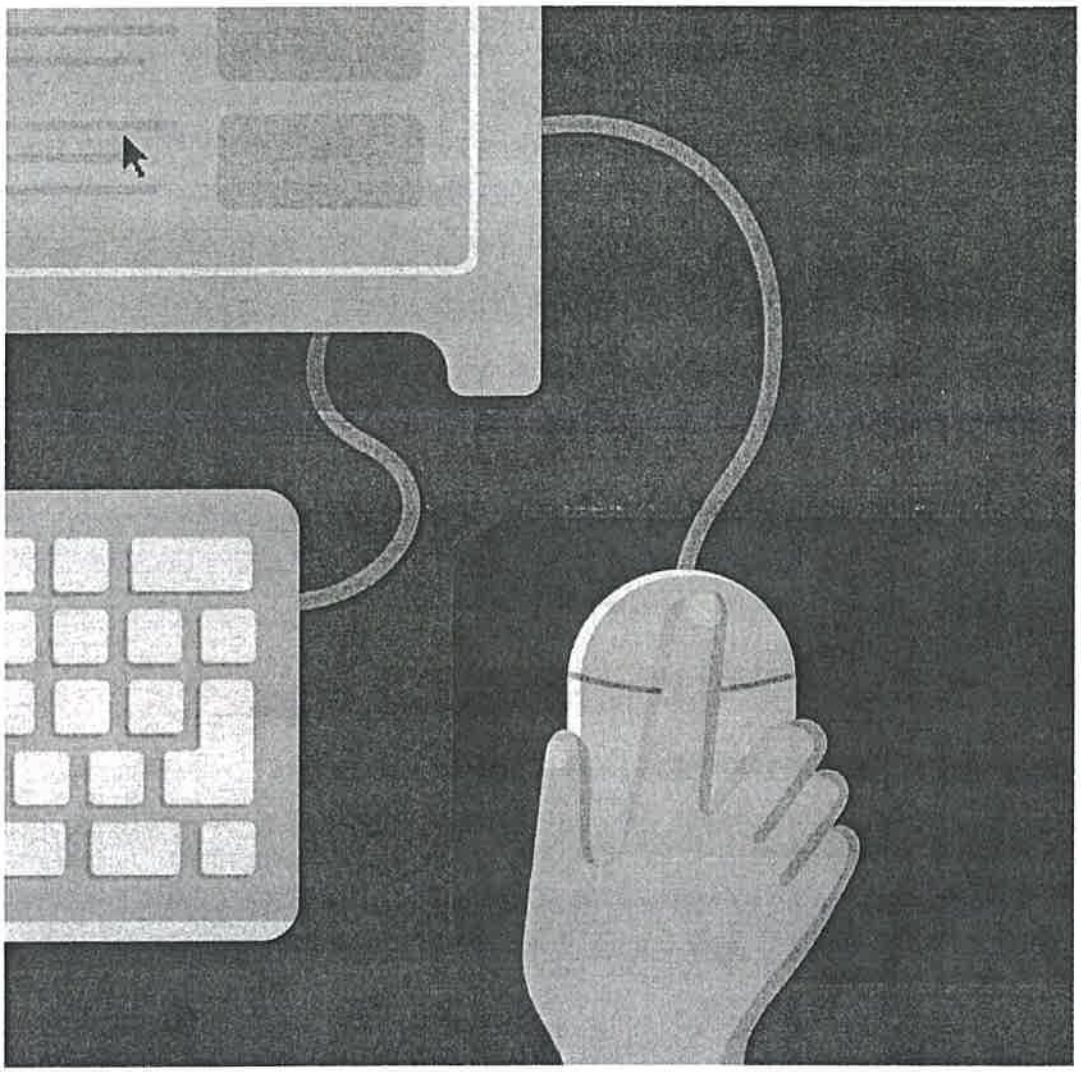
In most countries, there are no laws governing the collection and use of biometric behavioral data.

Even Europe's new privacy rules have exemptions for security and fraud prevention. A new digital privacy law in California includes behavioral biometrics on the list of tracking technologies companies must disclose if they collect, but it does not take effect until 2020.

Banks and merchants sometimes store their customers' biometric data internally. In many cases, though, they allow the outside vendors they work with to hold it. That magnifies the risks, Ms. Dixon said.

BioCatch has profiles on about 70 million individuals and monitors six billion transactions a month, according to Ms. Zelazny, the company's strategy executive. American Express, an investor in BioCatch, recently began using its technology on new account applications.

Some of BioCatch's rivals have even larger networks. Forter, a New York start-up that sells online fraud detection software incorporating behavioral biometrics to big retailers, said its database has records on 175 million people from more than 180 countries. Another competitor, NuData, was acquired last year by Mastercard.



On your computer, software can track your mouse habits, including the speed and rhythm of your cursor tracking. Andrew Roberts

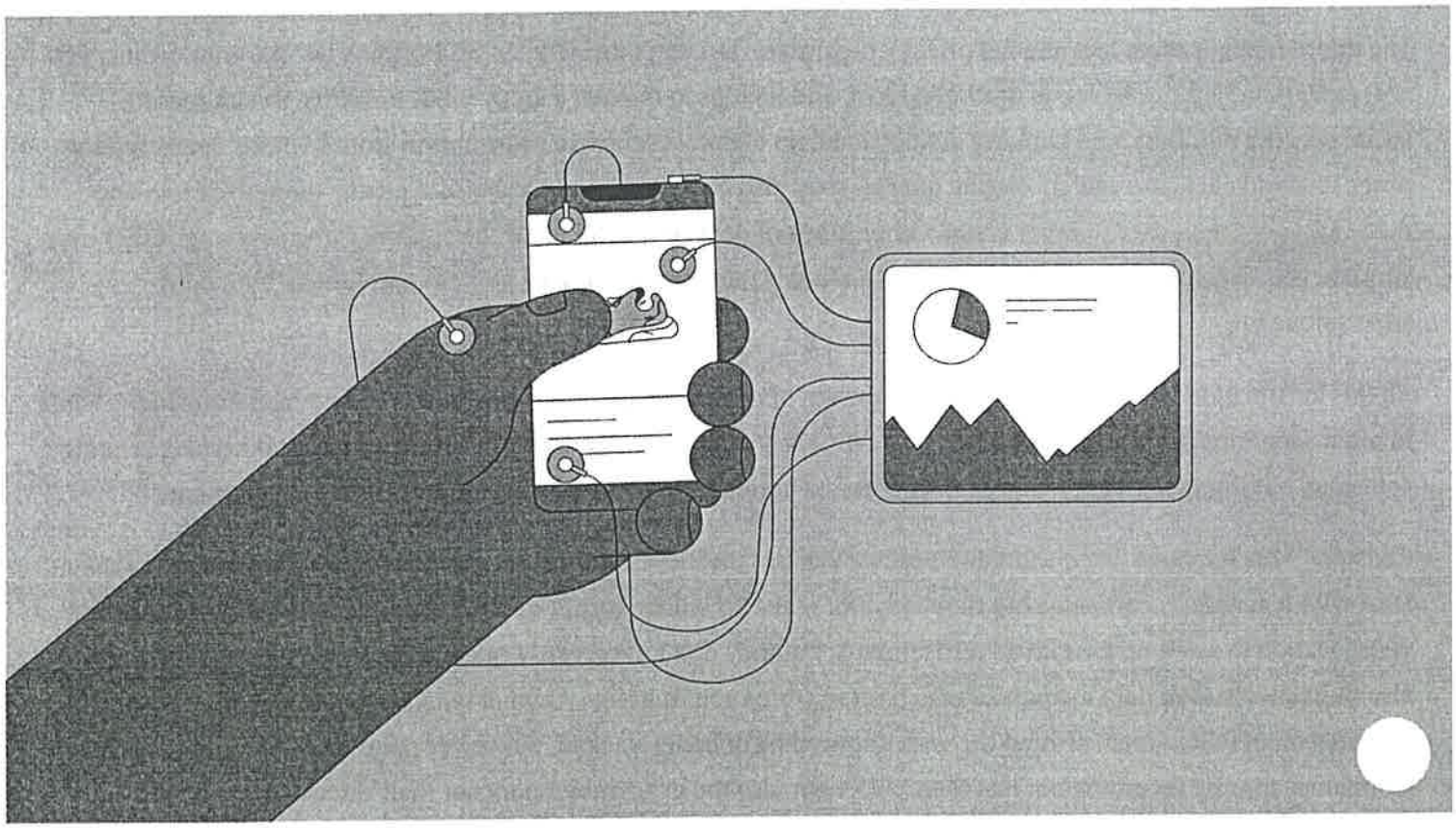
More than a dozen technology vendors, from under-the-radar start-ups to giants like I.B.M., have built behavioral biometrics into the security software they sell to retailers and banks.

The technology can be useful for rooting out fraud even without personal data on individual customers.

On new account applications, for example, behavioral biometric systems pay close attention to where and when applicants pause. A legitimate applicant typically types personal information — their name, their address, their Social Security number — fluidly, with few breaks. A scammer will often either cut and paste or take breaks to consult their notes.

"This used to be like science fiction," said Ryan Wilk, a NuData employee who is now a Mastercard vice president. "When we described what we did, people would give us looks like, 'Is this real?' Now, it's become not just a gimmick but a major technology in the financial industry. Lots of big companies are

using it."



RADIO

LOUISE MATSAKIS BUSINESS 02.15.2019 07:00 AM

The WIRED Guide to Your Personal Data (and Who Is Using It)

Information about you, what you buy, where you go, even where you *look* is the oil that fuels the digital economy.

On the internet, the personal data users give away for free is transformed into a precious commodity. The puppy photos people upload train machines to be smarter. The questions they ask Google uncover humanity's deepest prejudices. And their location histories tell investors which stores attract the most shoppers. Even seemingly benign activities, like staying in and watching a movie, generate mountains of information, treasure to be scooped up later by businesses of all kinds.

Personal data is often compared to oil—it powers today's most profitable corporations, just like fossil fuels energized those of the past. But the consumers it's extracted from often know little about how much of their

academic researchers, hackers, law enforcement, and foreign nations—as well as plenty of companies trying to sell you stuff.

What Constitutes "Personal Data"?

The internet might seem like one big privacy nightmare, but don't throw your smartphone out the window just yet. "Personal data" is a pretty vague umbrella term, and it helps to unpack exactly what it means. Health records, social security numbers, and banking details make up the most sensitive information stored online. Social media posts, location data, and search-engine queries may also be revealing but are also typically monetized in a way that, say, your credit card number is not. Other kinds of data collection fall into separate categories—ones that may surprise you. Did you know some companies are analyzing the unique way you tap and fumble with your smartphone?

All this information is collected on a wide spectrum of consent: Sometimes the data is forked over knowingly, while in other scenarios users might not understand they're giving up anything at all. Often, it's clear *something* is being collected, but the specifics are hidden from view or buried in hard-to-parse terms-of-service agreements.

Consider what happens when someone sends a vial of saliva to 23andme. The person knows they're sharing their DNA with a genomics company, but they may not realize it will be resold to pharmaceutical firms. Many apps use your location to serve up custom advertisements, but they don't necessarily make it clear that a hedge fund may also buy that location data to analyze which retail stores you frequent. Anyone who has witnessed the same shoe advertisement follow them around the web knows they're being tracked, but fewer people likely understand that companies may be recording not just their clicks but also the exact movements of their mouse.

In each of these scenarios, the user received something in return for allowing a corporation to monetize their data. They got to learn about their genetic ancestry, use a mobile app, or browse the latest footwear trends from the comfort of their computer. This is the same sort of bargain Facebook and Google offer. Their core products, including Instagram, Messenger, Gmail, and Google Maps, don't cost money. You pay with your personal data, which is used to target you with ads.

Who Buys, Sells, and Barters My Personal Data?

The trade-off between the data you give and the services you get may or may not be worth it, but another breed of business amasses, analyzes, and sells your information without giving you anything at all: data brokers. These firms compile info from publicly available sources like property records, marriage licenses, and court cases. They may also gather your medical records, browsing history, social media connections, and online purchases. Depending on where you live, data brokers might even purchase your information from the Department of Motor Vehicles. Don't have a driver's license? Retail stores sell info to data brokers, too.

over $16 billion in data acquiring and analyzing consumer data, according to the Interactive Advertising Bureau.

Data brokers are also valuable resources for abusers and stalkers. Doxing, the practice of publicly releasing someone's personal information without their consent, is often made possible because of data brokers. While you can delete your Facebook account relatively easily, getting these firms to remove your information is time-consuming, complicated, and sometimes impossible. In fact, the process is so burdensome that you can pay a service to do it on your behalf.

Amassing and selling your data like this is perfectly legal. While some states, including California and Vermont, have recently moved to put more restrictions on data brokers, they remain largely unregulated. The Fair Credit Reporting Act dictates how information collected for credit, employment, and insurance reasons may be used, but some data brokers have been caught skirting the law. In 2012 the "person lookup" site Spokeo settled with the FTC for $800,000 over charges that it violated the FCRA by advertising its products for purposes like job background checks. And data brokers that market themselves as being more akin to digital phone books don't have to abide by the regulation in the first place.

There are also few laws governing how social media companies may collect data about their users. In the United States, no modern federal privacy regulation exists, and the government can even legally request digital data held by companies without a warrant in many circumstances (though the Supreme Court recently expanded Fourth Amendment protections to a narrow type of location data).

The good news is, the information you share online does contribute to the global store of useful knowledge: Researchers from a number of academic disciplines study social media posts and other user-generated data to learn more about humanity. In his book, *Everybody Lies: Big Data, New Data, and What the Internet Can Tell Us About Who We Really Are*, Seth Stephens-Davidowitz argues there are many scenarios where humans are more honest with sites like Google than they are on traditional surveys. For example, he says, fewer than 20 percent of people admit they watch porn, but there are more Google searches for "porn" than "weather."

Personal data is also used by artificial intelligence researchers to train their automated programs. Every day, users around the globe upload billions of photos, videos, text posts, and audio clips to sites like YouTube, Facebook, Instagram, and Twitter. That media is then fed to machine learning algorithms, so they can learn to "see" what's in a photograph or automatically determine whether a post violates Facebook's hate-speech policy. Your selfies are literally making the robots smarter. Congratulations.

The History of Personal Data Collection

astrological patterns as far back as 150 BC. Two millennia later, in the late 1880s, Herman Hollerith invented the tabulating machine, a punch card device that helped process data from the 1890 United States Census. Hollerith created a company to market his invention that later merged into what is now IBM.

By the 1960s, the US government was using powerful mainframe computers to store and process an enormous amount of data on nearly every American. Corporations also used the machines to analyze sensitive information including consumer purchasing habits. There were no laws dictating what kind of data they could collect. Worries over supercharged surveillance soon emerged, especially after the publication of Vance Packard's 1964 book, *The Naked Society*, which argued that technological change was causing the unprecedented erosion of privacy.

The Trackers Tracking You

Online trackers can be divided into two main categories: same-site and cross-site. The former are mostly benign, while the latter are more invasive. A quick taxonomy:

- **Traditional Cookies**
  Facebook, Google, and other companies use these extremely popular cross-site trackers to follow users from website to website. They work by depositing a piece of code into the browser, which users then unwittingly carry with them as they surf the web.
- **Super Cookies**
  Supercharged cookies can be difficult or impossible to clear from your browser. They were most famously used by Verizon, which had to pay a $1.35 million fine to the FCC as a result of the practice.
- **Fingerprinters**
  These cross-site trackers follow users by creating a unique profile of their device. They collect things like the person's IP address, their screen resolution, and what type of computer they have.
- **Identity trackers**
  Instead of using a cookie, these rare trackers follow people using personally identifiable information, such as their email address. They collect this data by hiding on login pages where people enter their credentials.
- **Session cookies**
  Some trackers are good! These helpful same-site scripts keep you logged in to websites and remember what's in your shopping cart—often even if you close your browser window.
- **Session replay scripts**
  Some same-site scripts can be incredibly invasive. These record everything you do on a website, such as which products you clicked on and sometimes even the password you entered.

The next year, President Lyndon Johnson's administration proposed merging hundreds of federal databases into one centralized National Data Bank. Congress, concerned about possible surveillance, pushed back and organized a Special Subcommittee on the Invasion of Privacy. Lawmakers worried the data bank, which would "pool statistics

the Fair Credit Reporting Act in 1970 and the Privacy Act in 1974. The regulations mandated transparency, but did nothing to prevent the government and corporations from collecting information in the *first* place, argues technology historian Margaret O'Mara.

Toward the end of the 1960s, some scholars, including MIT political scientist Ithiel de Sola Pool, predicted that new computer technologies would continue to facilitate even more invasive personal data collection. The reality they envisioned began to take shape in the mid-1990s, when many Americans started using the internet. By the time most everyone was online, though, one of the first privacy battles over digital data brokers had already been fought: In 1990, Lotus Corporation and the credit bureau Equifax teamed up to create Lotus MarketPlace: Households, a CD-ROM marketing product that was advertised to contain names, income ranges, addresses, and other information about more than 120 million Americans. It quickly caused an uproar among privacy advocates on digital forums like Usenet; over 30,000 people contacted Lotus to opt out of the database. It was ultimately canceled before it was even released. But the scandal didn't stop other companies from creating massive data sets of consumer information in the future.

Several years later, ads began permeating the web. In the beginning, online advertising remained largely anonymous. While you may have seen ads for skiing if you looked up winter sports, websites couldn't connect you to your real identity. (HotWired.com, the online version of WIRED, was the first website to run a banner ad in 1994, as part of a campaign for AT&T.) Then, in 1999, digital ad giant DoubleClick ignited a privacy scandal when it tried to de-anonymize its ads by merging with the enormous data broker Abacus Direct.

Privacy groups argued that DoubleClick could have used personal information collected by the data broker to target ads based on people's real names. They petitioned the Federal Trade Commission, arguing that the practice would amount to unlawful tracking. As a result, DoubleClick sold the firm at a loss in 2006, and the Network Advertising Initiative was created, a trade group that developed standards for online advertising, including requiring companies to notify users when their personal data is being collected.

But privacy advocates' concerns eventually came true. In 2008, Google officially acquired DoubleClick, and in 2016 it revised its privacy policy to permit personally-identifiable web tracking. Before then, Google kept its DoubleClick browsing data separate from personal information it collected from services like Gmail. Today, Google and Facebook can target ads based on your name—exactly what people feared DoubleClick would do two decades ago. And that's not all: Because most people carry tracking devices in their pockets in the form of smartphones, these companies, and many others, can also follow us wherever we go.

Personal information is currently collected primarily through screens, when people use computers and smartphones. The coming years will bring the widespread adoption of new data-guzzling devices, like smart speakers, censor-embedded clothing, and wearable health monitors. Even those who refrain from using these devices will likely have their data gathered, by things like facial recognition-enabled surveillance cameras installed on street corners. In many ways, this future has already begun: Taylor Swift fans have had their face data collected, and Amazon Echos are listening in on millions of homes.

We haven't decided, though, how to navigate this new data-filled reality. Should colleges be permitted to digitally track their teenage applicants? Do we really want health insurance companies monitoring our Instagram posts? Governments, artists, academics, and citizens will think about these questions and plenty more.

And as scientists push the boundaries of what's possible with artificial intelligence, we will also need to learn to make sense of personal data that isn't even *real*, at least in that it didn't come from humans. For example, algorithms are already generating "fake" data for other algorithms to train on. So-called deepfake technology allows propagandists and hoaxers to leverage social media photos to make videos depicting events that never happened. AI can now create millions of synthetic faces that don't belong to anyone, altering the meaning of stolen identity. This fraudulent data could further distort social media and other parts of the internet. Imagine trying to discern whether a Tinder match or the person you followed on Instagram actually exists.

Whether data is fabricated by computers or created by real people, one of the biggest concerns will be how it is analyzed. It matters not just what information is collected but also what inferences and predictions are made based upon it. Personal data is used by algorithms to make incredibly important decisions, like whether someone should maintain their health care benefits, or be released on bail. Those decisions can easily be biased, and researchers and companies like Google are now working to make algorithms more transparent and fair.

Tech companies are also beginning to acknowledge that personal data collection needs to be regulated. Microsoft has called for the federal regulation of facial recognition, while Apple CEO Tim Cook has argued that the FTC should step in and create a clearinghouse where all data brokers need to register. But not all of Big Tech's declarations may be in good faith. In the summer of 2018, California passed a strict privacy law that will go into effect on January 1, 2020, unless a federal law supersedes it. Companies like Amazon, Apple, Facebook, and Google are now pushing for Congress to pass new, less stringent privacy legislation in 2019 before the California law kicks in. Even in a divided Congress, lawmakers could come together around privacy—scrutinizing Big Tech has become an important issue for both sides.

Some companies and researchers argue it's not enough for the government to simply protect personal data; consumers need to own their information and be compensated when it's used. Social networks like Minds and Steemit have experimented with rewarding users with cryptocurrency when they share content or spend time

by personal data collection. It might also be the wrong way to frame the issue. Instead, perhaps, less collection should be permitted in the first place, forcing companies to move away from the targeted-advertising business model altogether.

Before we can figure out the future of personal data collection, we need to learn more about its present. The cascade of privacy scandals that have come to light in recent years—from Cambridge Analytica to Google's shady location tracking practices—have demonstrated that users still don't know all the ways their information is being sold, traded, and shared. Until consumers actually understand the ecosystem they've unwittingly become a part of, we won't be able to grapple with it in the first place.

Learn More

- **The Privacy Battle to Save Google From Itself**
  Google's sprawling privacy apparatus includes thousands of employees and billions of dollars in cumulative investment. But the company is still an advertising behemoth and fundamentally makes money by monetizing the personal data it collects from users. Yet Google has also played a leadership role in creating industry standards for transparency and data protection. More than a dozen privacy employees at Google spoke to WIRED about how they make sense of the paradox of their work, insisting that there's no internal pressure to compromise privacy protections to make a larger profit.

- **Few Rules Govern Police Use of Facial-Recognition Technology**
  One of the most sensitive pieces of personal data you possess isn't hidden at all: It's your face. The issue has become contentious for civil rights activists, and Amazon in particular has faced backlash—even from its own employees—over use of the technology, especially for law enforcement purposes. With the exception of two states however, few laws regulating the use of facial recognition exist.

- **Carriers Swore They'd Stop Selling Location Data. Will They Ever?**
  In 2018, US phone carriers promised to stop selling customer location data after journalists discovered it had ended up in the hands of questionable third parties. Not even a year later, the same carriers were caught doing it again. The question now is how the Federal Communications Commission will handle the issue. The agency has the authority to make it illegal for carriers to sell this kind of information, but so far it hasn't said whether the law should apply to location data. In the meantime, consumers are left to take Verizon, Sprint, T-Mobile, and AT&T's promises at face value.

- **I Sold My Data for Crypto. Here's How Much I Made**
  A new wave of companies is peddling an alluring message: Users should own their own data and get a cut of its value, instead of allowing it to be monetized by advertising companies and data brokers for free. Sign up for one of these apps and the brokers will contact users directly, offering crypto currency as a bonus in exchange for

Companies like Amazon, Apple, Facebook, and Google are pushing hard for federal digital privacy legislation in 2019, and not quite out of the goodness of their hearts. Last summer, California's state legislature passed a groundbreaking privacy bill that is set to go into effect on January 1, 2020. Tech giants are now racing to supersede the law with more industry-friendly federal legislation. Even though Congress is divided politically, it looks like a deal could be reached. Reigning in Big Tech has become a bipartisan issue.

- **Your Smartphone Choice Could Determine Whether You Get a Loan**
  In Europe, some lenders are using passive signals, like what kind of phone you have, to determine whether you should qualify for a loan. Research from the National Bureau of Economic Research suggests those indicators can predict consumer behavior as accurately as traditional credit scores. But these factors aren't necessarily ones consumers are aware of or know to change.

- **The Wired Guide to Data Breaches**
  There's no such thing as perfect security, and it's impossible to safeguard against every potential data breach. But how worried should users be when they find out their personal information was leaked or stolen? To answer that question, it helps to know a little about the history of data breaches. Armed with context, consumers can determine whether they need to take extra precautions after a security incident happens.

- **What Does a Fair Algorithm Actually Look Like?**
  Lawmakers largely haven't decided what rights citizens should have when it comes to transparency in algorithmic decision-making. There isn't a "right to explanation" for how a machine came to a conclusion about your life. Some researchers are conceptualizing what such a right should might look like in the future.

Thanks to Ghostery, Mozilla, the Electronic Frontier Foundation, and Seth Stephens-Davidowitz for their help in creating this guide.

Last updated February 13, 2019.

Enjoyed this deep dive? Check out more WIRED Guides.

Louise Matsakis is a Staff Writer at WIRED covering Amazon, security, and online platforms. She was formerly an editor at Motherboard, VICE's science and technology site. She is based in New York. Send tips to louise_matsakis@wired.com or via Signal at 347-966-3806.

STAFF WRITER

All Tech Considered

PRIVACY & SECURITY

Facebook's Facial Recognition Software Is Different From The FBI's. Here's Why

May 18, 2016 · 9:30 AM ET

NAOMI LACHANCE

Facebook's Moments app uses facial recognition technology to group photos based on the friends who are in them. Amid privacy concerns in Europe and Canada, the versions launched in those regions excluded the facial recognition feature.
Facebook

When someone tags you in a photo on Facebook, it's often a nice reminder of a shared memory. It lets your whole social network see what you've been up to or where you've been.

ALL TECH CONSIDERED

A Look Into Facebook's Potential To Recognize Anybody's Face

Well, to three men from Illinois, this feature takes on a much more sinister capacity. They argue that when someone tags you in a photo on Facebook without your consent, Facebook is breaking the law — and a federal judge has allowed the case to proceed.

Facebook is hardly the only facial recognition technology that exists, but this company in particular is being challenged because its capabilities are so powerful. In Europe and Canada this month, privacy advocates won a victory when Facebook launched its photo app, Moments, without facial recognition scanning.

02:38

Learn More About Facebook AI Research from Facebook on Vimeo.

"There are more [facial recognition] algorithms and techniques than there are companies," says Jonathan Frankle, staff technologist at the Georgetown Center on Privacy and Technology. But with its huge database of images, Facebook's algorithm has a leg up on most others in that it is constantly being taught how to improve. Every

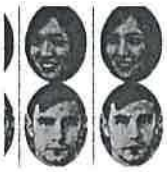
time you tag a photo, you're adding to an enormous, user-driven wealth of knowledge and data.

ALL TECH CONSIDERED

Can Computer Programs Be Racist And Sexist?

Every time one of its 1.65 billion users uploads a photo to Facebook and tags someone, that person is helping the facial recognition algorithm. The tag shows the algorithm what someone looks like from different angles and in different lights, Frankle says. If you give Facebook a face to identify, it has fewer photos to parse through, because it's only looking at photos of you and your friends.

Facebook, according to the company, is able to accurately identify a person 98 percent of the time. Compare that with the FBI's facial recognition technology, Next Generation Identification, which according to the FBI, identifies the correct person in the list of the top 50 people only 85 percent of the time. Facial recognition in the Google Photos app is prone to error as well — the company came under fire last year when its system tagged two African-Americans as gorillas.



ALL TECH CONSIDERED

How To Make Your Face (Digitally) Unforgettable

Part of why the FBI's technology has such a large margin of error is that its database usually only has a photo taken straight on — a mug shot, or in several states, a driver's license photo. The software has to look through a huge database to find a match, and each photo is often of a different person. Grainy security footage can be problematic.

"It's much harder for face recognition to work when you're trying to identify one person from a very large database versus one from a very small database, which is what Facebook is doing," says Jennifer Lynch, staff attorney at the Electronic Frontier Foundation.

Another reason Facebook is a target for privacy advocates is that its database — so carefully updated and tended — is tempting to the FBI. Law enforcement officials can issue a warrant for any information available on Facebook, including tagged photos.

TECHNOLOGY

Photo Identification: The 'Best And Worst Way' To ID People

"The FBI has said publicly that they do not put these photographs in the facial recognition database, but there is nothing in the law to prevent them from doing that," Lynch says.

Be careful about conspiracy theory rabbit holes, though. "People don't have a good intuition for what is and isn't possible," Frankle says. "And a lot of times until you've written code and tried to do this yourself it's hard to have a real visceral sense for just how hard some of this stuff is."

So next time you tag a friend on Facebook, go ahead — just remember that you're helping to train one of the most powerful facial recognition systems in the world.

photos facial recognition algorithms facebook fbi

Facial Recognition Technology: Where Will It Take Us?

Kristine Hamann and Rachel Smith

Share this:

–

Technology is expanding, evolving, and improving at an explosive rate. Society, including law enforcement, is struggling to keep pace with these seemingly daily developments. This paper addresses facial recognition technology used by law enforcement to enhance surveillance capabilities and the associated legal issues it raises. Facial recognition technology provides a sophisticated surveillance technique that can be more accurate than the human eye. The use of this technology to enhance public safety will only increase and improve. Nevertheless, the criminal justice system must grapple with the many novel legal issues it poses. The legal landscape is far from settled. This article is not intended to be an in-depth legal analysis; rather, the goal is to provide an overview of the technology and an explanation of the evolving legal issues that law enforcement and the legal community may confront.

How It Works

Generally, facial recognition technology (FRT) creates a "template" of the target's facial image and compares the template to photographs of preexisting images of a face(s) (known). The known photographs are found in a variety of places, including driver's license databases, government identification records, mugshots, or social media accounts, such as Facebook.

Facial recognition technology uses a software application to create a template by analyzing images of human faces in order to identify or verify a person's identity. (Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOW STUFF WORKS (last visited Nov. 30, 2018).) FRT has the potential to be a useful tool in crime fighting by identifying criminals who are captured on surveillance footage, locating wanted fugitives in a crowd, or spotting terrorists as they enter the country. (*Id.*) FRT also can be used in other ways, such as to identify problem gamblers in casinos, greet hotel guests, connect people on matchmaking websites, help take attendance in schools, and identify drinkers who are underage (*7 Surprising Ways Facial Recognition Is Used*, CBS NEWS (last visited Apr. 14, 2018).) FRT has effectively identified individuals in controlled environments with relatively small populations, for example, where an individual's face is matched to a preexisting image on an internal file. (State v. Alvarez, No. A-5587-13T2, 2015 N.J. Super. LEXIS 1024, at *2 (N.J. Super. Ct. App. Div. May 4, 2015); Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues,* CTR. FOR CATASTROPHE PREPAREDNESS & RESPONSE, NYU (July 22, 2009).) On the other hand, FRT has not worked as well in more complex situations, such as finding an unknown face on a crowded street. (*Id.* at 3.) Nevertheless, while not yet being used as the sole basis for an arrest, FRT does aid police investigations and can be used to develop

leads. (Alexander J. Martin & Tom Cheshire, *Legal Questions Surround Use of Police Facial Recognition Tech*, SKY NEWS (Aug. 23, 2017).)

Measuring the Face

A template for FRT is created by use of measurements. The face is measured through specific characteristics, such as the distance between the eyes, the width of the nose, and the length of the jaw line. (Bonsor & Johnson, *supra*.) The facial landmarks, known as nodal points (*id.*), are measured and translated into a template with a unique code. New technologies are emerging that are improving recognition rates, such as 3-D facial recognition and biometric facial recognition that uses the uniqueness of skin texture for more accurate results. (*Id.*) Once the face in question is analyzed, the software will compare the template of the target face with known images in a database in order to find a possible match. (*Id.*; Jenni Bergal, *States Use Facial Recognition Technology to Address License Fraud*, GOVERNING MAG. (July 15, 2015).)

Social Media and Technology Companies

Social media and technology companies have developed their own facial recognition software to use for "photo-tagging," a system where a photograph is automatically associated with a known person. For example, Facebook and Shutterfly rely on FRT to identify individuals in uploaded photographs. (*In re* Facebook Biometric Info. Privacy Litig., No. 15-cv-03747-JD, 2016 WL 2593853, at *1 (N.D. Cal. May 5, 2016); Norberg v. Shutterfly, Inc., 152 F. Supp. 3d 1103, 1106 (N.D. Ill. 2015).) Their facial recognition algorithm performs well as it is assisted and improved by its own users who tag themselves and fellow users in photos, many of which are taken at different angles and in different lighting. (Naomi Lachance, *Facebook's Facial Recognition Software Is Different from the FBI's. Here's Why*, NPR (May 18, 2016); Yaniv Taigman et al., *DeepFace: Closing the Gap to Human-Level Performance in Face Verification*, FACEBOOK AI RESEARCH (June 24, 2014).)

Technological Limitations

FRT is an evolving scientific and diagnostic tool with enormous potential for law enforcement, but it does have limitations. When these images meet certain professional scientific standards, the accuracy rate when comparing each to one another is high. (*See* Introna & Nissenbaum, *supra*, at 3.) However, the accuracy of FRT decreases when there is no standardized photo for comparison or when the comparison comes from a photo from an uncontrolled environment. (*Id.*) Additionally, FRT works best when the picture is head-on and has no movement. (Lachance, *supra*. *See* David Nicklaus, *Cops' Start-Up Uses Facial Recognition to Improve Security*, ST. LOUIS POST-DISPATCH (Mar. 17, 2017).) Because faces change over time, unlike fingerprints or DNA (Richard Raysman & Peter Brown, *How Has Facial Recognition Impacted the Law?*, N.Y.L.J. (Feb. 9, 2016)), software can trigger incorrect results by changes in hairstyle, facial hair, body weight, and the effects of aging. (*Id.*) There is also some research indicating that FRT algorithms may not be as accurate in reading the faces of certain demographics, in particular African Americans. (Clare Garvie & Jonathan Frankel, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATL. (Apr. 7, 2016).)

Investigative Uses

General Surveillance

FRT has been used for general surveillance, yet, so far its results have been mixed. For example, FRT was used at the 2001 Super Bowl in Tampa, Florida, to screen for potential criminals and terrorists from the event. (Bonsor & Johnson, *supra*; Raysman & Brown, *supra*.) Law enforcement was able to identify 19 people with minor criminal records, although it was later admitted that the software only flagged petty criminals and resulted in some false positives. (*Id.*) More recently, facial recognition was used by Baltimore police to monitor protesters during the unrest and rioting after the death of Freddie Gray, leading to the apprehension and arrest of protestors that had outstanding warrants. (Benjamin Powers, *Eyes over Baltimore: How Police Use Military Technology to Secretly Track You*, ROLLING STONE MAG. (Jan. 6, 2017). *See also* Kevin Rector & Alison Knezevich, *Maryland's Use of Facial Recognition Software Questioned by Researchers, Civil Liberties Advocates*, BALT. SUN (Oct. 18, 2016 12:01 AM).)

Targeted Photo Comparisons

Unlike the challenges with using FRT for general surveillance, FRT has been used effectively to identify thousands of suspects relating to identification fraud, with particular success in cases of driver's license fraud. (Bergal, *supra*.) For example, New York has identified over 10,000 people with more than one driver's license with the help of FRT. (*Id.*) Similarly, New Jersey Department of Motor Vehicle officials have referred about 2,500 fraud cases to law enforcement since 2011. (*Id.*) Additionally, airports are using FRT to assist airlines by having passengers board planes based on photographic images they take instead of boarding passes. These photos are compared to previously stored photographs from passports and visas on file with the U.S. Customs and Border Patrol. (*See* Adam Vaccaro, *At Logan, Your Face Could Be Your Next Boarding Pass,* BOS. GLOBE (May 31, 2017).)

Active Criminal Case Investigations

The software also has been useful in investigations—not for conclusive identification of an individual, but in conjunction with other evidence. FRT has contributed to establishing probable cause for the arrest of suspected activity of assailants in videos of fights posted on YouTube (*In re* K.M., No. 2721 EDA 2014, 2015 WL 7354644, at *1 (Penn. Sup. Ct. Nov. 20, 2015)), for passport fraud (United States v. Roberts-Rahim, No. 15-CR-243 (DLI), 2015 WL 6438674, at *3 (E.D.N.Y. Oct. 22, 2015)), and in identity theft cases (United States v. Green, No. 08-44, 2011 WL 1877299, at *2 (E.D. Penn. May 16, 2011)). Facial recognition software also was used in an attempt to find the suspects of the Boston Marathon Bombings in 2013, though the use of the software was ultimately unhelpful, due in part to the uncontrolled environment in which the surveillance images were taken. (Brian Ross, *Boston Bombing Day 3: Dead-End Rumors Run Wild and a $1B System Fails*, ABC NEWS (Apr. 20, 2016); Sean Gallagher, *Why Facial Recognition Tech Failed in the Boston Bombing Manhunt*, ARSTECHNICA (May 7, 2013).) Recently, the NYPD arrested an individual related to a shooting after taking a surveillance image from a nightclub of the shooter and creating a full 3-D image of him, then running it through a

facial recognition software program that revealed 200 likely matches. (Greg B. Smith, *Behind the Smoking Guns: Inside the NYPD's 21st Century Arsenal*, N.Y. DAILY NEWS (Aug. 20, 2017).) Officers then compared the images looking for similar physical characteristics between them, which enabled officers to narrow it down to a single image that was utilized in a photo array that was then shown to witnesses. (*Id.*)

Trial Evidence

With increasing reliability and use of FRT, at some point soon, prosecutors will seek to introduce the technology into evidence in court, either to establish probable cause or as evidence of an identification. At that time, the scientific reliability of FRT algorithms may have to be established by prosecutors under either the *Frye* or *Daubert* standard in court before the evidence is ultimately accepted. (*See* Daubert v. Merrell Dow Pharms., 509 U.S. 579, 580 (1993).)

Future Use

Progress and improvements in facial recognition are made daily and increased accuracy is foreseeable. (*See* Smith, *supra*.) Ultimately, it is expected that law enforcement will seek to use FRT for real-time analysis of faces and immediate identification. For example, it soon may be possible for an officer's body-worn camera to use FRT to identify a person he or she observes on the street. (*See* Barak Ariel, *Technology in Policing: The Case for Body-Worn Cameras and Digital Evidence,* POLICECHIEF; Ava Kofman, *Real-Time Face Recognition Threatens to Turn Cops' Body Cameras into Surveillance Machines*, THE INTERCEPT (Mar. 22, 2017).). Also, state and local governments are investing tremendous resources and increasingly relying on biometric and pattern recognition technologies to help thwart domestic terrorism and other crime, representing a shift in how such investigations are conducted. (Introna & Nissenbaum, *supra*, at 47.)

The federal government has invested approximately $1 billion in the FBI's Next Generation Identification system (NGI) database. (Jose Pagliery, *FBI Lauches a Face Recognition System*, CNNTECH (Sept. 16, 2014).) A component of the database, the Interstate Photo System, incorporates facial recognition and search capabilities into a photo database, consisting of photographs of different sources, including both criminal mugshots and noncriminal sources, such as employment records and background check databases. (Christopher De Lillo, *Open Face: Striking the Balance Between Privacy and Security with the FBI's Next Generation Identification System*, 41 J. LEGIS. 264, 265 (2014–15).) However, when it released NGI, the FBI issued a caveat that the system was to be used for investigatory purposes only, and it could not serve as the sole basis for an arrest. (*See* Pagliery, *supra*.) Nevertheless, as the technology improves, FRT's role in law enforcement investigations will undoubtedly continue to grow.

Legal Issues

Fourth Amendment Concerns Generally

The Fourth Amendment prohibits an unlawful search of a place where a person has a reasonable expectation of privacy. In *Katz v. United States*, the Supreme Court announced a two-part test to determine whether a person has a reasonable expectation of privacy, which assesses (1) whether the person exhibited an actual, subjective expectation of privacy and (2) whether that expectation is one that society recognizes as reasonable. (389 U.S. 347 (1967).) The *Katz* test provides a framework for analyzing Fourth Amendment issues.

On June 22, 2018, the US Supreme Court decided *Carpenter v. United States.* (138 S. Ct. 2206 (2018).) In *Carpenter*, the Court ruled on whether a person's expectation of privacy covered the records of historical cell phone data (historical CSLI), which could reveal the person's physical location or movements. Relying on *Katz*, *Carpenter* held that a person's Fourth Amendment rights were violated when the government received historical CSLI from cell phone companies without first obtaining a search warrant. (*Id.*)

Before the *Carpenter* opinion, government agencies could obtain historical cell phone location records with only a court order by explaining to a judge that the information was necessary to an investigation and that the information was in the possession of a third party.
However, *Carpenter* ruled that the government must be put to a higher standard and must obtain a judicial search warrant based on sworn facts that probable cause exists to search for the requested items. Thus, law enforcement agencies must now seek a search warrant for individual, personal historical CSLI from phone companies in these specific situations: where no exigent circumstances exist and for date ranges of more than six days.

The *Carpenter* decision was quite narrow, so many questions remain regarding how the Court will address the government's access to other forms of technology that can track an individual's physical location or movement. The Court, however, clearly outlined that as forms of technology develop and enhance the government's ability to encroach on private areas, the courts will be required to work to preserve an individual's privacy from the government intrusion.
The *Carpenter* Court has found that an individual has an expectation of privacy in his or her personal information acquired in large quantities over an extended period of time even when possessed by third parties. This ruling will shape how courts view other forms of technology.

Possible Legal Issues Raised by FRT Specifically

In light of *Katz* and *Carpenter*, FRT that is used on a limited, short-term basis with strictly public systems should not implicate the Fourth Amendment because an individual's face is open to the public. (*Katz*, 389 U.S. at 351–52; United States v. Dionisio, 410 U.S. 1, 14 (1973). *See, e.g.*, De Lillo, *supra*, at 282.) Nevertheless, legal arguments against the warrantless use of FRT can be made on a variety of issues, including that the technology can be used to track an individual's movement over an extended period of time, First Amendment rights may be chilled, and the technology is not available for public use and may implicate the Fourth Amendment.

Data Aggregation Issues

When a suspect has been identified and law enforcement wishes to track the suspect's movement, the use of FRT together with other technologies could also raise a Fourth

Amendment issue. (*Carpenter,* 138 S. Ct. at 2212–21. *See* United States v. Jones, 564 U.S. 400 (2012) (Sotomayor, J., concurring).) As discussed, in *Carpenter,* the Court held that the government's warrantless access to an extensive compilation of cell phone user data violated the Fourth Amendment. (138 S. Ct. at 2219.) The Supreme Court declined to address whether short-term, limited, or real-time access had equal concerns under the Fourth Amendment. (*Id.* at 2220.) As for FRT, *Carpenter* suggests that an individual's public movements captured by FRT in an isolated incident do not implicate the Fourth Amendment. However, the same individual's public movements viewed using FRT over an extended timeframe could reveal intimate details about the individual's personal life that may be found to amount to a Fourth Amendment search, even though everything took place in public. (*See, e.g.,* Riley v. California, 134 S. Ct. 2473 (2014); *Jones,* 565 U.S. 400; United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).) Furthermore, compiling data across various databases (whether public or private), throughout multiple locations over a long period, may also implicate the Fourth Amendment.

First Amendment Issues

Critics also have argued that FRT may implicate the First Amendment right to freedom of association and right to privacy. (*The Perpetual Line-Up: Unregulated Police Face Recognition in America,* GEO. L. CTR. ON PRIVACY & TECH. 42–44 (Oct. 18, 2016); Rector & Knezevich, *supra.*) Courts have upheld the right to anonymous speech and association. (NAACP v. Alabama, 357 U.S. 449, 466 (1958); *see also M*cIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995); Talley v. California, 362 U.S. 60, 64 (1960).) These rights protect an individual's ability to associate freely and advocate for minority positions. Without these protections, the use of FRT could have a chilling effect on individuals' behaviors and lead to self-censorship. (*See The Perpetual Line-Up, supra.*) Nevertheless, some courts have considered law enforcement's use of photography at public demonstrations as not violating the First Amendment right to freedom of association. (Laird v. Tatum, 408 U.S. 1 (1972); Phila. Yearly Meeting of Religious Soc'y of Friends v. Tate, 519 F.2d 1335, 1337–38 (3d Cir. 1974); Donohoe v. Duling, 465 F.2d 196, 202 (4th Cir. 1972).) On the other hand, specific, targeted surveillance of a group may cross the line and violate First Amendment association protections. For example, the Second Circuit in *Hassan v. City of New York* determined that the NYPD's targeted use of pervasive video, photographic, and undercover surveillance of Muslim Americans may have caused those individuals "direct, ongoing, and immediate harm," and it may have created a chilling effect. (*See* 804 F.3d 277, 292 (2d Cir. 2015).) Privacy advocates have been particularly critical of the use of FRT in widespread surveillance. The FRT program that was used to monitor the protestors in Baltimore during the Freddie Gray protests were widely criticized for many reasons, including a fear that African Americans were overrepresented in the facial recognition repository. (Stephen Babcock, *Report Raises Troubling Questions About Facial Recognition Technology in Maryland,* TECHNICAL.LY (Oct. 19, 2016); Rector & Knezevich, *supra*; *ACLU Letter to Principal Deputy Assistant Attorney General Vanita Gupta,* LEADERSHIP CONFERENCE (Oct. 18, 2016).)

Use of Technology That Is Not in the General Public Use

Under the *Katz* test, an individual would not have an automatic expectation of privacy with respect to his or her face because it is exposed to the public. (Carpenter v. United States, 138 S.

Ct. 2206, 2217 (2018) (quoting Katz v. United States, 389 U.S. 347, 351–352 (1967)), and United States v. Jones, 565 U.S. 400, 430 (2012)).) In some instances, however, law enforcement's use of FRT that is not yet available for use generally has been deemed a search. The theory is that such technology is "sense-enhancing" and enables law enforcement to do more than ordinary surveillance by a police officer. For example, in *Kyllo v. United States*, the Supreme Court determined that law enforcement's use of thermal imaging technology to obtain information from the inside of a home constituted a search. (533 U.S. 27, 33 (2001).) Even though law enforcement was on a public street at the time, the use of the thermal imaging to obtain information that would otherwise have required law enforcement to enter the home concerned the Court. (*Id.* at 34.) In part because law enforcement in *Kyllo* relied on technology that was not in the general public use, the use of that technology constituted a search. (*Id.*) Though *Kyllo* addressed a technology that could reach into someone's home, which (unlike FRT) is clearly a private area, some scholars have considered the application of *Kyllo* in terms of the limited availability of the technology to FRT. (*See* NAT'L RESEARCH COUNCIL, BIOMETRIC RECOGNITION: CHALLENGES AND OPPORTUNITIES 106–107 (Nat'l Acads. Press, 2010); *Kyllo*, 533 U.S. at 34.) How the courts will interpret privacy interests in light of FRT technology has yet to be seen and will turn on how the technology is used, how much data are sought, how many locations are requested, how long the tracking of the face continues, the exigency of the need, and the actual method used to "capture" the image. (*Dep't of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, Sept. 3, 2015, at 5.)

Conclusion

Technology permeates almost every aspect of our daily lives. For law enforcement, technology comes with many benefits, but also drawbacks and questions. On the positive side, technology has benefited law enforcement in innumerable ways, such as creating reliable evidence, enabling efficient investigations, and helping to accumulate data that allow law enforcement to react quickly and effectively. On the other hand, this technology impacts peoples' privacy in many ways and will trigger many debates on the parameters of privacy.

It will be up to the courts and policymakers to strike the right balance between the need for information and the right to privacy. The debate about the proper balance between privacy and public safety will continue to play out in the courts, as well as in public discourse, for many years to come. Federal, state, and local law enforcement officials will have to be mindful of this debate when developing the rules and regulations that must ensure citizens' privacy protections, while still enabling law enforcement to make use of surveillance's tremendous investigatory and crime-fighting tools. In the meantime, technology will advance and evolve in ways that cannot be anticipated.

The Major Concerns Around Facial Recognition Technology

Nicole Martin Former Contributor
AI & Big Data
I write about digital marketing, data and privacy concerns.

Deep fake or deepfake technology as AI or artificial intelligence as a biometrics fake visual... [+]
GETTY

Facial recognition software has become increasingly popular in the past several years. It is used everywhere from **airports, venues, shopping centers and even by law enforcement**. While there are a few potential benefits to using the technology to prevent and solve crimes, there are many **concerns about the privacy, safety and legislation regarding the use of the technology.**

Facial recognition technology uses a database of photos, such as mugshots and driver's license photos to identify people in security photos and videos. It uses biometrics to map facial features and help verify identity through key features of the face. The most key feature is the geometry of a face such as the distance between a person's eyes and the distance from their forehead to their chin. This then creates what is called a **"facial signature."** It is a **mathematical formula** that is then compared to a database of known faces.

The market for this technology is growing exponentially. According to a research report "Facial Recognition Market" by Component, the facial recognition industry is expected to grow $3.2 billion in 2019 to $7.0 billion by 2024 in the U.S. The most significant uses for the technology being for surveillance and marketing. This, however, raises concerns for many people.

The main reason for concerns amongst citizens is the lack of federal regulations surrounding the use of facial recognition technology. Many are worried about how accurate the technology is and if there are biases and misinformation in these technologies. One issue, for example, is that the technology has been proven in multiple studies to be inaccurate at identifying people of color, especially black women.

Another major concern is the use of facial recognition for law enforcement purposes. Today, many police departments in the U.S., including New York City, Chicago, Detroit and Orlando, have begun utilizing the technology. According to a May 2018 report, the FBI has access to 412 million facial images for searches.

Not only is this a concern with the possibility of misidentifying someone and leading to wrongful convictions, it can also be very damaging to our society by being abused by law enforcement for things like constant surveillance of the public. Currently, the Chinese government is already

using facial recognition to arrest jaywalkers and other petty crimes that cause debate amongst what is considered basic civil rights and privacy issues versus protecting the public. Accuracy and accountability are necessary when it comes to the use of technology, especially regarding the justice system.

The concerns have not gone unnoticed by politicians and many cities have started to create legislation around these issues. Oregon and New Hampshire have banned the use of facial recognition in body cameras for police officers. California cities, such as San Francisco and Oakland, and some cities in Massachusetts have outlawed certain uses of facial recognition technology for city officials including law enforcement.

The Utah Department of Public Safety has also put forth some bans on the use of facial recognition for active criminal cases. Law enforcement in Utah claim that the use of facial recognition software helps keep dangerous criminals off the streets, but advocates say that there is no checks and balances when it comes to the system. Recent pushes from Portland, Oregon show that they are soon to follow suit.

The latest legislation push to put limitations on facial recognition technology is a California bill, AB 1215, also referred to as the Body Camera Accountability Act. This bill will temporarily stop California law enforcement from adding face and other biometric surveillance technology to officer-worn body cameras for use against the public in California.

According to the ACLU of Southern California, "AB 1215 is a common-sense bill that rightly concludes that keeping our communities safe doesn't have to come at the expense of our fundamental freedoms. We should all be able to safely live our lives without being watched and targeted by the government."

Governor Gavin Newsom must decide whether or not to sign it into law by October 13. If he does, it will go into effect in January.

Law enforcement isn't the only issue with the technology that is of concern. U.S. Customs and Border Protection in partnership with Delta have added facial scanning to the Atlanta airport's Concourse E, its Detroit hub, boarding gates in Minneapolis and Salt Lake City, and this month to Los Angeles International Airport. The use of this technology causes concerns about how much people are being watched and if hackers can access this data causing more harm than good.

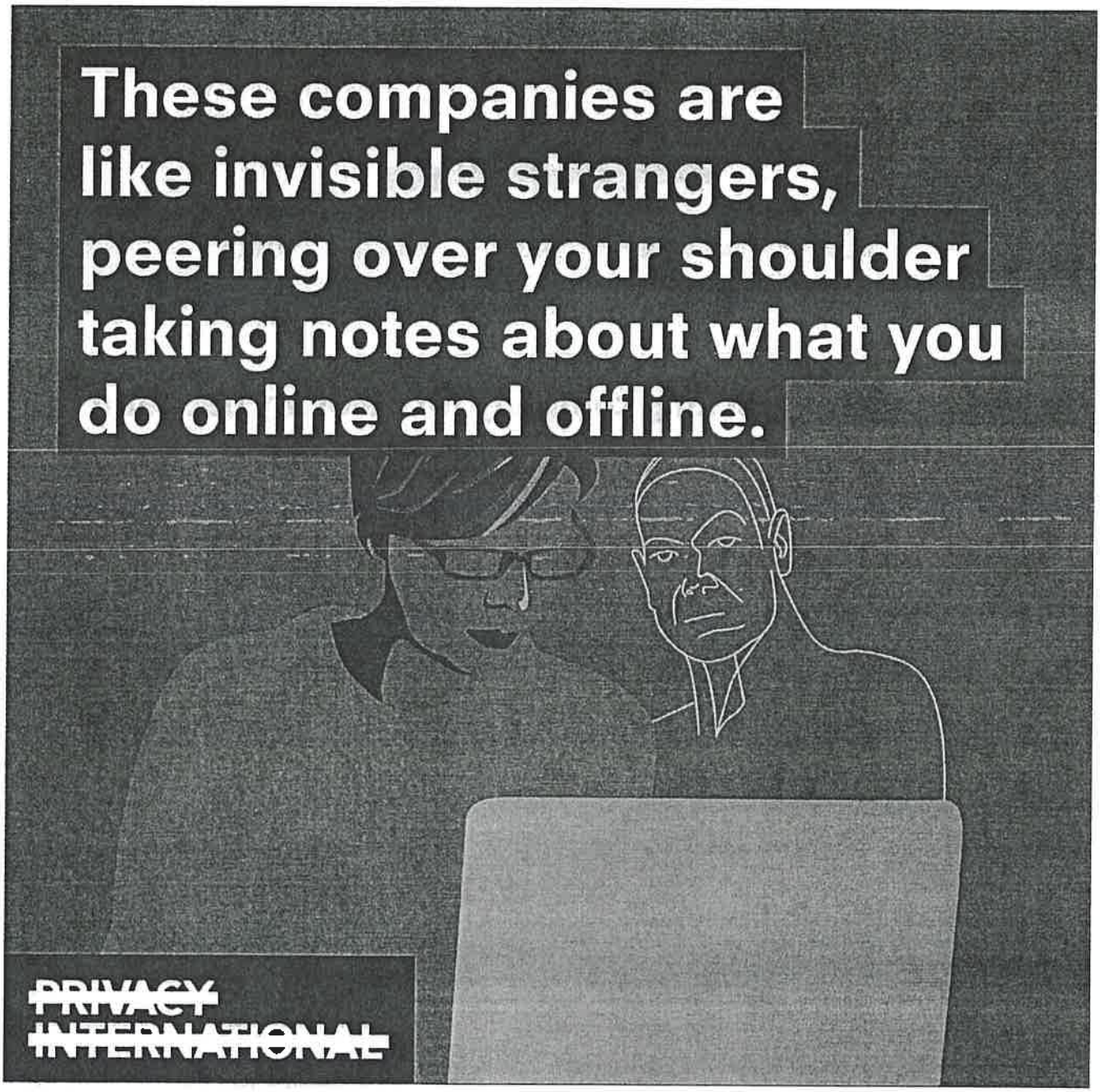
An activist group called Fight for the Future said facial recognition is an invasive technology that can be used for surveillance.

"Facial recognition really doesn't have a place in society," said Evan Greer, deputy director of Fight for the Future. "It's deeply invasive, and from our perspective, the potential harm to society and human liberties far outweigh the potential benefits."

With the vast number of concerns and privacy issues surrounding facial recognition software and its use, cities around the U.S. will face more dilemmas as they attempt to tackle these issues. AI and facial recognition technology are only growing and they can be powerful and helpful tools

when used correctly, but can also cause harm with privacy and security issues. Lawmakers will have to balance this and determine when and how facial technology will be utilized and monitor the use, or in some cases abuse, of the technology.

Follow me on LinkedIn. Check out my website.



Wednesday, November 7, 2018

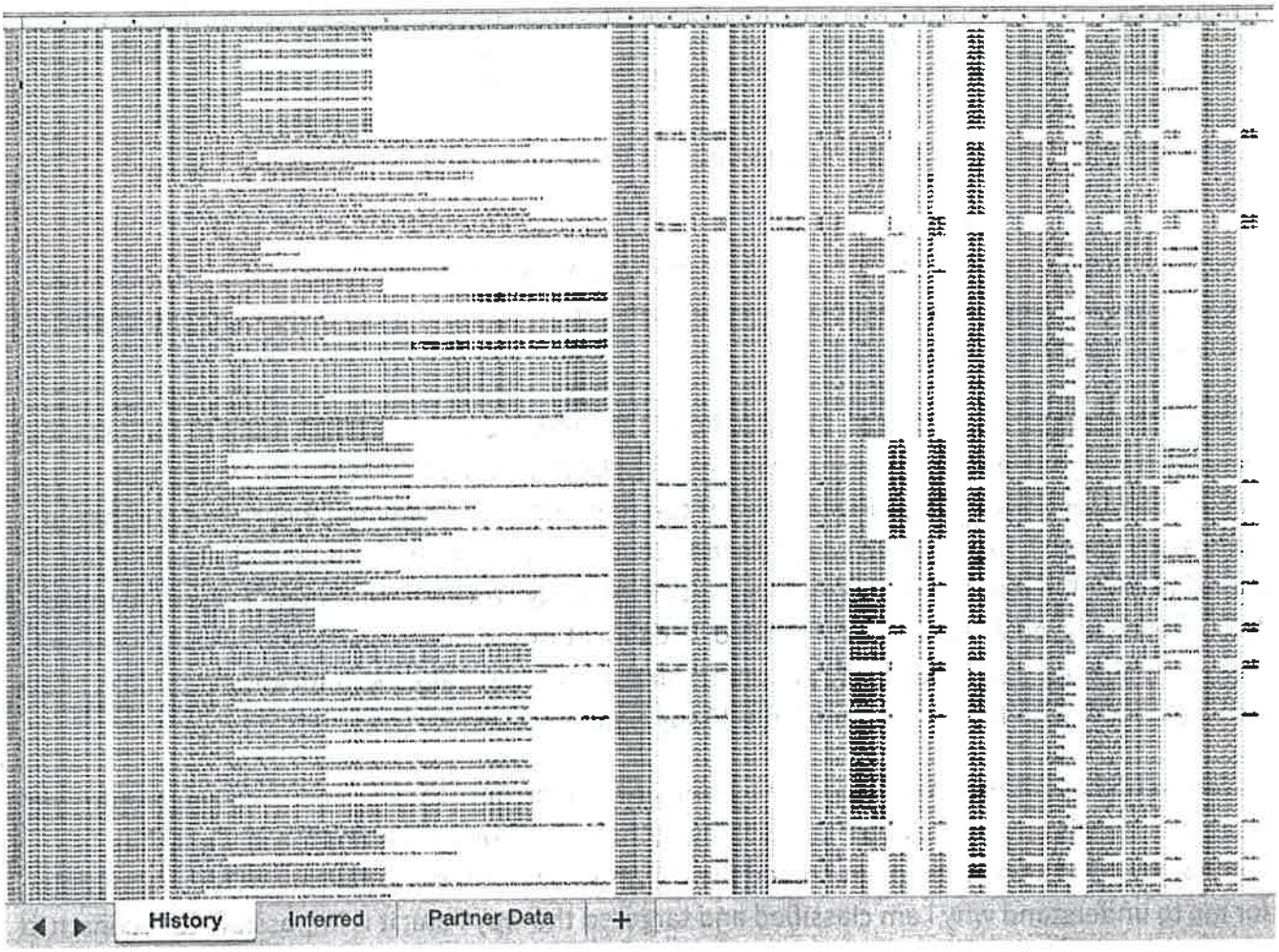
It's 15:10 pm on April 18, 2018. I'm in the Privacy International office, reading a news story on the use of facial recognition in Thailand. On April 20, at 21:10, I clicked on a CNN Money Exclusive on my phone. At 11:45 on May 11, 2018, I read a story on USA Today about Facebook knowing when teen users are feeling insecure.

How do I know all of this? Because I asked an advertising company called Quantcast for all of the data they have about me.

Most people will have never heard of Quantcast, but Quantcast will certainly have heard about them. The San Francisco-based company collects real-time insights on audience characteristics across the internet and claims that it can do so on over 100 million websites.

Quantcast is just one of many companies that form part of a complex back-end systems used to direct advertising to individuals and specific target audiences.

The (deliberately) blurred screenshot below shows what this looks like for a single person: over the course of a single week, Quantcast has amassed over 5300 rows and more than 46 columns worth of data including URLs, time stamps, IP addresses, cookies IDs, browser information and much more.



[A screengrab of the Data Subject Access Request PI obtained from Quantcast]

Seeing that the company has such granular insight into my online habits feels quite unnerving. Yet the websites, where Quantcast has tracked my visit, are just a small fraction of what the company knows about me. Quantcast has also predicted my gender, my age, the presence of children in my household (in number of children and their ages), my education level, and my gross yearly household income in US Dollars and in British Pounds.

a_unit	value
GenderVisits;GB	[0.9995629009618636 4.370990381364389E-4]
InetHHAgeAndGenderVisits;GB	[0.16963163563535782 0.18513675831813 07 0.1257233779170356 0.3538862968105453 4 0.06144096703915405 4 0.10374386524
InetHHAgeVisits;GB	[0.1697058138833724 0.18521771680399154 0.1257783555152497 0.3540410478120047 4 0.06146783457052116 0.10378923141
InetHHChildrenV2Visits;GB	[0.5145015966768377 1.0530208287461875E-4 0.0049111484312639 59 0.0875618093476440 2 0.0038107317722292887 0.3891094
InetHHEducationVisits;GB	[0.03904572745494902 0.6540257453949422 0.3069285271501087]
InetHHIncomeVisits;GB	[0.2664956273083136 0.0629016098818328 0.0722023682149928 0.5984003945948608]
GenderVisits;GB	[0.999830749461473 1.6925053852702787E-4]
InetHHAgeAndGenderVisits;GB	[0.21469208759269612 0.19940725420905558 0.1418112512367487 0.2920525468783964 4 0.04761961398810414 0.10424799555
InetHHAgeVisits;GB	[0.2147284304951945 0.19944100970735293 0.1418352569303662 8 0.2921019852967127 0.0476276749977463 0.10426564257 26
InetHHChildrenV2Visits;GB	[0.5506935498169285 1.1219017142199964E-4 0.0030622065531428627 0.0247059613149716 93 0.0065438140767976 97 0.414882
InetHHEducationVisits;GB	[0.03298286903380676 0.6663213365517425 0.30069579441445077]
InetHHIncomeVisits;GB	[0.34208517996066146 0.03563795182697384 0.0853527356865378 8 0.5369241325258268]
GenderVisits;GB	[0.9999056163347138 9.438366528628081E-5]
InetHHAgeAndGenderVisits;GB	[0.19660969859225438 0.16747187896307 41 0.1744350585812582 7 0.2547427421082612 6 0.03901343076057947 0.16763280732
InetHHAgeVisits;GB	[0.1966282570878572 0.16748768706486 96 0.1744515239555039 5 0.2547667879314994 0.03901711333874527 0.16764863062 15
InetHHChildrenV2Visits;GB	[0.5044999754302371 5.679890668526 68E-4 0.0021387712218162414 0.1950899754500293 8.3737197310194 16E-4 0.2968659168
InetHHEducationVisits;GB	[0.04567057386281842 0.3577744161262463 3 0.5965550100109352]

[A screengrab of the Data Subject Access Request PI obtained from Quantcast]

Quantcast has also placed me in much more fine-grained categories whose names suggest that the data was obtained by data brokers like Acxiom and Oracle, but also MasterCard and credit referencing agencies like Experian.

Some of the categories are uncannily specific. My MasterCard UK shopping interests, for instance, includes travel and leisure to Canada (I have in fact been to Canada recently for work) and frequent transactions in Bagel Restaurants (I can remember one night out where I've purchased quite a few bagels). Experian UK classifies me according to my assumed financial situation (for some inexplicable reason I'm classified as" City Prosperity:World-Class Wealth"), the data broker Acxiom even placed me in a category called "Alcohol at Home Heavy Spenders" (was it because I went shopping for a birthday party at home?), and a company called Affinity Answers thinks I have a social affinity with the consumer profile "Baby Nappies & Wipes" (very, very wrong).

Ads *seem* trivial, but the sheer scope and granularity of the data that is used to target people ever more precisely is anything but trivial. Looking at these categories reminds me of what the technology critic Sara Watson has coined the uncanny 'valley of personalisation'. It is impossible for me to understand why I am classified and targeted the way I am; it is impossible to reconstruct which data any of these segmentations are based on and - most worryingly - it is impossible for me to know whether this data can (and is) being used against me.

DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Retail:In Market:Toy Stores
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Hobbies & Interests:Beauty & Style:Jewellery
DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Travel & Leisure:Destinations:Asia
DATA_SEGMENT:Acxiom UK:Shopping Interests:Psychographics & Lifestyles:Lifestyle:Interest in Cultural Pursuits
DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Travel & Leisure:Destinations:Africa
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Media Interests:TV:Genres:News
DATA_SEGMENT:Acxiom UK:Shopping Interests:Finance:Investment Services:High Investment Activity
DATA_SEGMENT:Oracle Data Cloud - Affinity Answers (UK):Shopping Interests:Social Affinity:Food & Beverage:Cow & Gate
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Consumer Electronics:Brand Affinity:Toshiba
DATA_SEGMENT:Oracle Data Cloud - Experian UK:Shopping Interests:Psychographics & Lifestyles:Mosaic UK:Rural Reality
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Finance:Financial Services:Investing Seekers:College Savings
DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Travel & Leisure:Destinations:Northern Europe
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Hobbies & Interests:Internet & Online Activities:Social Influencers
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Automotive:In Market Make:BMW
DATA_SEGMENT:Acxiom UK:Shopping Interests:Psychographics & Lifestyles:Lifestyle:Interest in Gym/Classes
DATA_SEGMENT:Acxiom UK:Shopping Interests:Travel & Leisure:Travel Activities:World Travel as a regular hobby
DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Services:In Market:Hair Care & Beauty Salons
DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Retail:In Market:Jewellery & Giftware
DATA_SEGMENT:Oracle Data Cloud - Datalogix UK:Shopping Interests:Psychographics & Lifestyles:Personas:Avid Readers
DATA_SEGMENT:Oracle Data Cloud - Affinity Answers (UK):Shopping Interests:Social Affinity:Consumer Products:Aveeno
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Business & Occupation:Occupation:Occupation:IT/Technology
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Automotive:In Market Make:Acura
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Automotive:In Market Make:Cadillac
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Hobbies & Interests:Home & Garden:Housewares & Furnishings
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Fast Moving Consumer Goods:Categories:Beverages:Juice
DATA_SEGMENT:Oracle Data Cloud - Datalogix UK:Shopping Interests:Fast Moving Consumer Goods:Beverage Buyers:Tea
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Fast Moving Consumer Goods:Spend Profile:Top Grocery Spenders
DATA_SEGMENT:Oracle Data Cloud - MasterCard UK:Shopping Interests:Retail:In Market:Luggage & Leather Stores
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Hobbies & Interests:Shopping:Coupons
DATA_SEGMENT:Oracle Data Cloud - Oracle UK:Shopping Interests:Automotive:In Market Make:Mini

[A screengrab of the Data Subject Access Request PI obtained from Quantcast]

The murky world of third-party tracking

Quantcast is one of countless of so-called "third-parties" that monitor people's behaviour online. Because companies like Quantcast (just like Google, and Facebook) have trackers on so many websites and apps, they are able to piece together your activity on several different websites throughout your day.

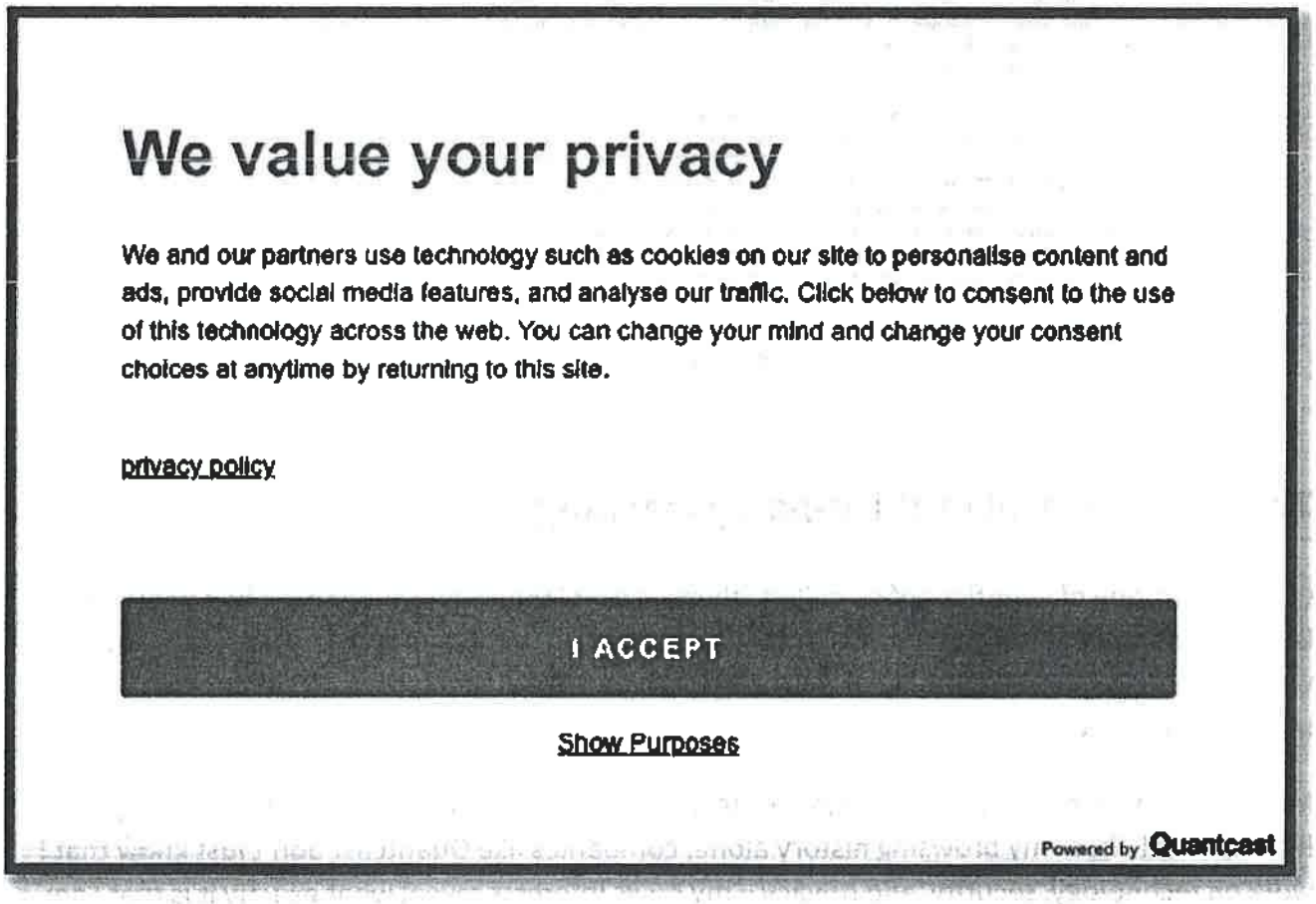
My Quantcast data, for instance, gives an eerily specific insight into my work life at Privacy International. From my browsing history alone, companies like Quantcast don't just know that I work on technology, security, and privacy – my news interests reveal what exactly it is that I am working on at any point in time. My Quantcast data even reveals that I have a personal blog on Tumblr.

For each and every single one of these links, Quantcast claims that it has obtained my consent to be tracked – but that is only part of the story. Quantcast has no direct relationship with the people whose data they collect. Therefore, most people have never heard of the company's name, do not know that they process their data and profile them, whether this data is accurate, for what purposes they are using it, or with whom it is being shared and the consequences of this processing.

Quantcast claims that it has obtained my (and likely your) consent because somewhere, on some website, I must have mindlessly clicked "I ACCEPT". The reason that I did this is because so-called "consent forms" are specifically designed to make you to click "I ACCEPT", simply because it is incredibly tedious and unnecessarily time-consuming to not accept tracking. Privacy International believes that this is in violation of the EU's General Data Protection Regulation (GDPR) which

requires that consent is freely given, unambiguous, and specific. The UK Information Commissioners Office argues that "genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation."

Quantcast sells such a "consent solution" to websites and publishers like news websites. Its design in a perfect example of such 'dark patterns' that incentivise people to "agree" to highly-invasive privacy practices – a widespread practice that our friends at the Norwegian Consumer Council have outlined in this excellent report.



Only after I clicked on the incredibly small "Show Purposes" and "See full vendor list" in the next window am I able to fully grasp what clicking "I ACCEPT" really entails: namely that I "consent" to hundreds of companies to use my data in ways that most people would find surprising. If I clicked "I ACCEPT" on the window above, I would have agreed to a company called Criteo to match my online data to offline sources and to link different devices I use.

< Back

We value your privacy

REJECT ALL ACCEPT ALL

You can set your consent preferences and determine how you want your data to be used based on the purposes below. You may set your preferences for us independently from those of third-party partners. Each purpose has a description so that you know how we and partners use your data.

Ad selection, delivery, reporting

The collection of information, and combination with previously collected information, to select and deliver advertisements for you, and to measure the delivery and effectiveness of such advertisements. This includes using previously collected information about your interests to select ads, processing data about what advertisements were shown, how often they were shown, when and where they were shown, and whether you took any action related to the advertisement, including for example clicking an ad or making a purchase. This does not

Required

See full vendor list

SAVE & EXIT

In fact, Quantcast's deceptive design is so effective, that the company proudly declares that it achieves a 90 percent consent rate on websites that use its framework.

Data brokers and the hidden data ecosystem

The fact that countless companies are tracking millions of people around the web and on their phones is disturbing enough, but what is even more disturbing about my Quantcast data is the extent to which the company relies on data brokers, credit referencing agencies, and even credit card companies in ways that are impossible for the average consumer to know about or escape.

Advertising companies and data brokers have been quietly collecting, analysing, trading, and selling data on people for decades. What has changed is the granularity and invasiveness at which this is possible.

Data brokers buy your personal data from companies you do business with; collect data such as web browsing histories from a range of sources; combine it with other information about you (such as magazine subscriptions, public government records, or purchasing histories); and sell their insights to anyone that wants to know more about you.

Even though these companies are on the whole non-consumer facing and hardly household names, the size of their data operations is astounding. **Acxiom's Annual report of 2017**, for instance, states that they offer data "on approximately 700 million consumers worldwide, and our data products contain over 5,000 data elements from hundreds of sources."

Part of the problem is that this data can be used to target, influence, and manipulate each and every one of us ever more precisely. How precisely? A few years ago, an advertising company from Massachusetts in the US targeted "abortion-minded women" with anti-abortion messages while there were in hospital. Laws in the US are very different from what is legal in the EU, yet the example shows what it technically possible: to target very precise groups of people, at particular times and particular places. This is the reality of what targeted advertisement looks like today.

While uncannily accurate data can be used against us, inaccurate data is no less harmful, especially when data that most of us don't even know exists and have very little control over is used to make decisions about us. **An investigation by Big Brother Watch in the UK**, for instance, showed how Durham Police in the UK were feeding Experian's Mosaic marketing data into their 'Harm Assessment Risk Tool', to predict whether a suspect might be at low, medium or high risk of reoffending in order to guide decisions as to whether a suspect should be charged or released onto a rehabilitation program. Durham Police is not the only police force in England and Wales that uses Mosaic service. Cambridgeshire Constabulary, and Lancashire Police are listed as having contracts with Experian for Mosaic.

How Privacy International is challenging the hidden data industry

If you have been following the Cambridge Analytics and Facebook scandals over the past few months, you might get the impression that privacy scandals are about bad actors misusing well-intended platforms during major elections, who are guilt of responding too slowly. Our interpretation has always been that we are faced with a much more systemic problem that lies at the very core of the current ways in which advertisers, marketers, and many other exploit people's data.

The European General Data Protection Regulation, which entered into force on May 25, 2018 strengthens rights of individuals with regard to the protection of their data, imposes more stringent obligations on those processing personal data, and provides for stronger regulatory enforcement powers.

That's why Privacy International has filed **complaints** against seven data brokers (Acxiom, Oracle), ad-tech companies (Criteo, Quantcast, Tapad), and credit referencing agencies (Equifax, Experian) with data protection authorities in France, Ireland, and the UK.

These companies do not comply with the Data Protection Principles, namely the principles of transparency, fairness, lawfulness, purpose limitation, data minimisation, and accuracy. They also do not have a legal basis for the way they use people's data, in breach of GDPR.

The world is being rebuilt by companies and governments so that they can exploit data. Without urgent and continuous action, data will be used in ways that people cannot now even imagine, to

define and manipulate our lives without us being to understand why or being able to effectively fight back. We urge the data protection authorities to investigate these companies and to protect individuals from the mass exploitation of their data, and we encourage journalists, academics, consumer organisations, and civil society more broadly, to further hold these industries to account.

This piece was written by PI's Data Exploitation Programme Lead Frederike Kaltheuner

---

What PI is Campaigning on: Tell companies to stop exploiting your data!

Learn more: AdTech Data Exploitation Data Protection Metadata

Legal Action: Challenge to Hidden Data Ecosystem

Contact Us

62 Britton Street,
London, EC1M 5UY
UK

MOTHERBOARD
TECH BY VICE

What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?

These sites you haven't heard of are sharing boatloads of data about you.

By Yael Grauer

Mar 27 2018, 10:00am

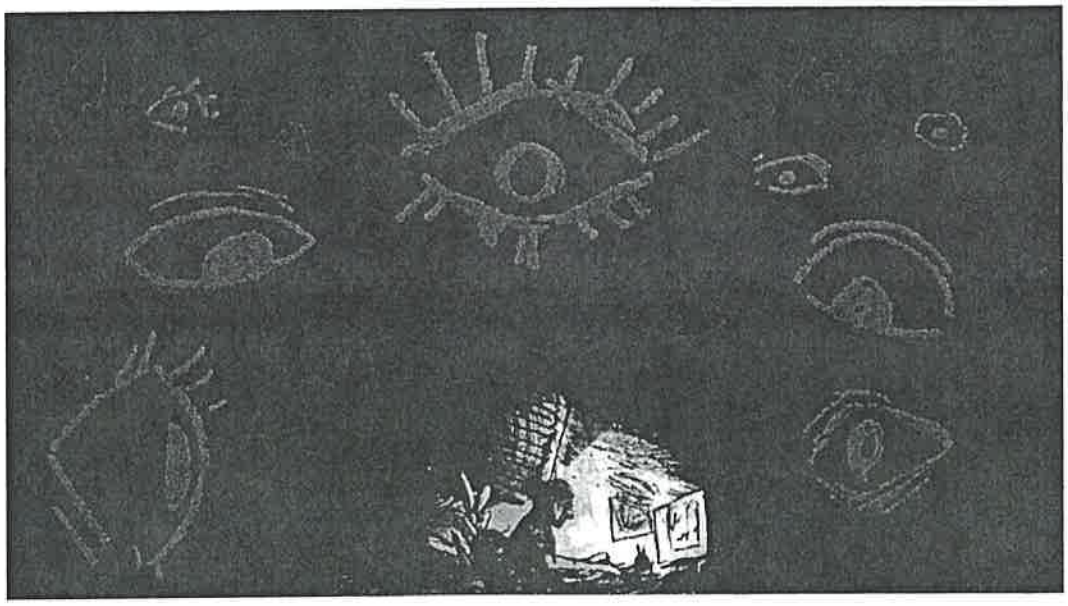
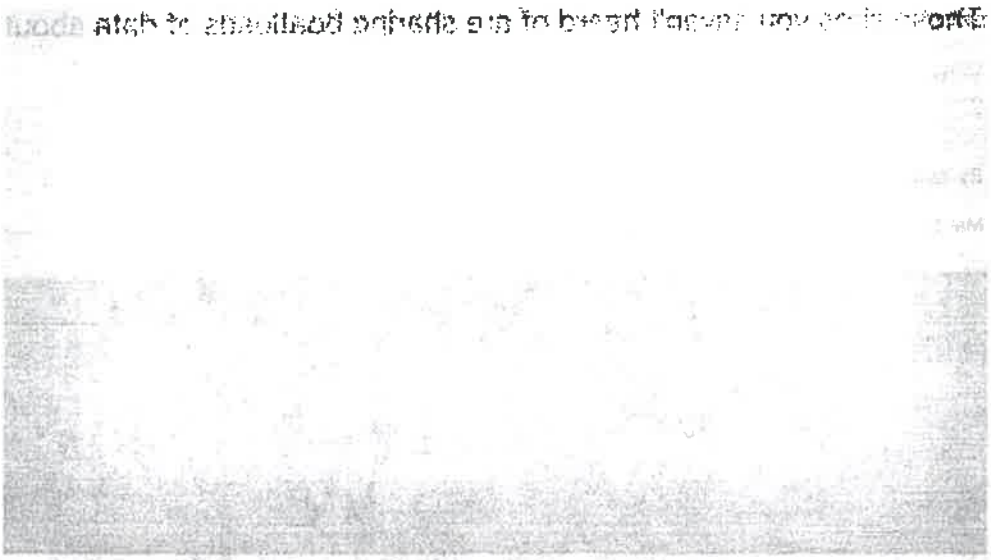


IMAGE: CHRIS KINDRED

Going about your daily business—shopping online, buying a home, getting married, using a search engine, liking a Facebook page, registering to vote—leaves an enormous paper trail, and data brokers are scooping it up.

Data brokers are entities that collect information about consumers, and then sell that data (or analytic scores, or classifications made based on that data) to other data brokers, companies, and/or individuals. These data brokers do not have a direct relationship with the people they're collecting data on, so most people aren't even aware that the data is even being collected.



"Most have no idea who these companies are and how they got their data on them, and they would be very surprised to know the intimate details that these companies have collected on people," said Amul Kalia, an analyst and intake coordinator at the Electronic Frontier Foundation (an organization I've written for in the past).

Even when consumers are aware of both the existence of data brokers and the extent of data collected, it's difficult to determine which data they can control. For example, some data brokers might allow users to remove raw data, but not the inferences derived from it, making it difficult for consumers to know how they have been categorized. Some data brokers store all data indefinitely, even if it is later amended. The industry is

incredibly opaque, and data brokers have no real incentive to interact with the people whose data they are collecting, analyzing, and sharing.

Let's take a deep dive into the shadowy world of data brokers, what kind of information they collect, and some options you have for minimizing the dissemination of that information. If you want to skip to the part where you can do something about this, check out our **Big Ass Data Broker Opt-Out List**.

Types of data brokers and the threats they pose to users

The data broker industry is generally divided into three categories. There are people search sites, where users can input a piece of data, such as a person's name (or a phone number, city/state, email address, social security number, etc.) and get personal information on that person either for free or for a small fee. Information can include aliases, birthdates, interests and affiliations, addresses and address history, education information, employment details, information on marriage, divorce, bankruptcy, etc., social media profiles, property records, and details on relatives. These people search sites include places like Spokeo, PeekYou, PeopleSmart, Pipl, and many more. These sites can be used to research people and find old friends to send them postcards. Because they give access to addresses, court records, and other information people would rather keep private, they can also be used for doxing.

There are data brokers that focus on marketing, such as Datalogix (owned by Oracle), or divisions or subsidiaries of companies like Experian and Equifax. They develop dossiers on individuals which can be used to tailor marketing. Data brokers typically place consumers in categories based on their age, ethnicity, education level, income, number of children, and interests. Companies purchase lists of names, email addresses, interests and offline activity to assist in soliciting or marketing to those individuals. These

sites can be used to better tailor marketing, offering consumers great deals or personally tailored discounts or coupons.

But the information can also be used to put people in high-risk classifications based on their search history or to advertise high-interest loans to them rather than low-interest ones for which they'd qualify. For example, searching specific medical conditions such as heart disease or diabetes could be added to your digital biography. Even seemingly innocuous information, like looking at motorcycles or researching diabetes for oneself or a friend—might mean that insurance companies would consider you more likely to engage in risky behavior, according to the FTC. In some cases, these classifications may be based on inaccurate information—and there's no easy process for consumers to access information, correct it, or remove it.

Lastly, there are data brokers such as ID Analytics that offer risk mitigation products to verify identities and help detect fraud. These are typically the least troublesome to consumers, unless, of course, the information is inaccurate—in which case, it may be difficult to correct. For example, a lender might use a risk mitigation product to determine whether a Social Security number is associated with a deceased person, or whether a mailing address used has been associated with fraud. This can be useful for detecting fraud, but can also stop consumers who happen to have a matching address but are not committing fraud from being able to complete a transaction.

Other threats

In addition to the threats listed above, the information collected on individuals can be used in various other nefarious ways, such as to facilitate identity theft.

"If you can get information on someone online, you might be able to impersonate them or use their credit history, or perhaps get into a password protected website if you can answer security questions about people," said Paul Stephens, Director of Policy and Advocacy at Privacy Rights Clearinghouse.

Then, of course, information on people search sites can be used nefariously. "It certainly can be used by stalkers to find out the address of someone; it can be used by someone who wants to harass you by phone if they're able to get your phone number."

Additionally, companies scooping up tons of data on individuals are vulnerable to security breaches, so the information they're collecting has ended up in the wrong hands. In addition to the Equifax breach, which affected more than 145 million people, **Acxiom was hacked** in 2003, and over 1.6 billion records (including names, addresses, and email addresses) were stolen, and some were sold to spammers. **Epsilon was hacked in 2011**, exposing names and email addresses of millions of people on email marketing lists who were then subject to spam as well as **spear phishing attempts**. LexisNexis' parent company RELX has been **breached multiple times**, exposing social security numbers, mailing addresses, and driver's license data. In 2015, 15 million records belonging to T-Mobile but stored on Experian's servers were accessed.

Where do data brokers get your data?

Data brokers collect information from public records, such as property records, court records, driver's license and motor vehicle records, Census data, birth certificates, marriage licenses, divorce records, state professional and recreational license records, voter registration information, bankruptcy records, etc.

They also collect or buy information from commercial sources, scooping up people's purchase histories (along with the dates, dollar amounts, payment used, loyalty cards, coupons used, etc.) as well as warranty registration information, etc. from retailers and catalog companies.

Data brokers also collect information from social media sites, web browsing activity, **quiz apps**, media reports, websites, and other publicly available sources. And, of course, they also exchange or purchase information from one another, and then merge the data with their own records.

Is this even legal?

"There's nothing unlawful about posting this information online," said Stephens. "You have to draw a distinction between the data broker and a credit reporting or consumer reporting agency, and that really depends on how the information is used." The use of consumer reports for credit, insurance, or employment purposes (including background checks) are regulated under the Fair Credit Reporting Act (FCRA), which was passed in 1970, is the law that allows you to access and correct errors in your credit report. It also means that users of consumer reports can only access that information in certain circumstances. For example, employers using consumer reports to screen employees or job applicants must get written permission and explain how they plan to use the report.

> ***Read more:*** *The Motherboard Guide to Not Getting Hacked*

But data brokers that aren't considered consumer reporting agencies aren't regulated in the same way. People search sites often instruct users to not use the data as a proxy for a traditional credit check (for decisions about credit, housing, employment, insurance, etc.), though whether or not users of sites not regulated by FCRA actually utilize those sites for those purposes, and how often that happens, is difficult to determine.

Griffin Boyce, a system administrator at Berkman Klein Center for Internet & Society at Harvard University, received several hundred dollars in a **class action lawsuit** settlement from LexisNexis, a corporation that provides business research and risk management services, after trying and failing to fix false information in its records. In 2012, people search site Spokeo **paid $800,000 to settle FTC charges** that it sold information to human resources, recruiting, and background screening companies without complying with the FCRA.

Meanwhile, another **lawsuit against Spokeo** is playing out in court. In 2011, a Virginia resident named Thomas Robins accused Spokeo of selling inaccurate information about him, which incorrectly stated he was in his 50s, married, employed in a professional or technical field, and that he had children, none of which was true. Robbins alleged that Spokeo was in violation of federal law by not making reasonable attempts to confirm the information before selling it to third parties. He said that he may have lost job opportunities as a result.

The initial complaint was tossed out by a district judge because Robins didn't show he'd experienced harm, but he appealed to the 9th Circuit Court of Appeals, and the lawsuit was reinstated. The US Supreme Court ruled 6-2 that Robins must show real harm for the lawsuit to proceed. The 9th Circuit ruled that his alleged injuries were sufficient to merit a lawsuit. Robins' attorney is seeking class-action status for the lawsuit.

In addition to FCRA regulations, there's **Section 5 of the Federal Trade Commission Act**, which prohibits unfair or deceptive acts or practices. "The mere existence of the site is not necessarily a violation," explains Tiffany George, a senior staff attorney in the FTC's Division of Privacy and Identity Protection. The site needs to make misleading statements or commit an act that causes injury to consumers.

In May 2014, the Federal Trade Commission **released a 110-page report on data brokers**, which included the results of its in-depth study on nine of them in order to shed light on the industry and its practices. "Congress has

not passed comprehensive data broker legislation since then," confirmed Kalia. "The report was good. It had a lot of great recommendations, but unfortunately, our legislature didn't actually follow them." Among other things, the recommendations including legislation requiring consumer-facing entities to disclose that they share data with brokers, and allow them to opt out. It also recommended data brokers to create a centralized mechanism, such as a portal, to provide consumers access to their data and the ability to opt out of that data being shared for marketing purposes. It also recommended that Congress consider requiring data brokers to clearly disclose the names and categories of sources of their data, and that data brokers disclose that they not only use raw data but also make inferences based on some of the elements of data collected.

"In a lot of ways there are parallels with the 2017 Equifax data breach because Equifax also aggregates consumer data and you would have thought that would have provided sufficient incentive for Congress to do something about it, but they have actually not done that either," Kalia adds.

Kalia points out that election campaigns, especially at the federal level, use information from data broker companies to determine to whom to target ads. "We rely on our politicians to think of a way to regulate this industry, but at the same time our politicians are some of the customers of this data broker industry and stand to benefit from their deregulated nature," he said.

That said, Kalia believes that approaching the issue locally may be fruitful. For example, he testified **in front of a committee** put together by the Vermont Attorney General, since the legislature is looking at **regulating the data broker industry**.

For now, it is possible for some consumers to opt out of some sites, but the process is time-consuming, difficult, and needs to be regularly repeated because data brokers will just add you again. Some pull data from other sites and update automatically. And then there are data brokers who don't remove information even when asked.

"One of the reasons that we recommended legislation in our data broker report and one of the things that we note in our data broker report is that there's a proliferation of these data brokers, and there's no central source or mechanism for consumers to be able to find out about them or find out what they can do to protect themselves or remove their information, so we recommended that Congress enact legislation for such centralized mechanism for consumers to find out that information," said George.

She found that sites allowing consumers to opt out may require them to submit identifying information, but variations of her name continued to proliferate, requiring multiple opt-out requests. "A part of our legislative recommendations, we recommended that Congress enact legislation that would require data brokers to be transparent about any limitations of the opt-outs that they may provide to consumers," she said.

What you can do about it?

Experts agree that opting out might be a good use of time to remove information from people search sites. Some, but not all, of these sites do allow people the opportunity to opt out. But you can't opt out just once. "A lot of the time these processes are automated, so even if you opt out of the system now they get data again from another source and then your information will be back up on the system," said Kalia.

Not only does opting out not always work, it can be difficult and complicated, too. Some sites offer a simple and transparent opt-out process, but others don't allow removal at all. In between those two extremes, some sites require users to jump through many hoops by making phone calls, sending information by mail or fax, or opting out twice on the same page.

Some require users to provide additional information to let them opt out. "For example, a site like Radaris won't let you remove the information but will give you the chance to 'control' the information. But what controlling really means is that you can hide some of the information but not all of it, and you sign up on this website and give them more information than they

had previously," said Joe Sutton, head of DeleteMe at Abine. (Radaris did not respond to request for comment.) **DeleteMe** is a paid subscription service that removes user's information from people search sites. It's a good option for people wanting to remove their information from data broker sites, but still isn't a catch-all because it is not comprehensive.

If a consumer submits identifying information in an opt-out request that varies from the identifying information in the data broker's records, the opt-out may not capture all of those records. As a result, consumers may find themselves having to submit many opt-out requests to the same data broker again and again.

So, opting out is best done early and often. "Waiting until you're targeted by creeps is a bad idea. There are lots of proactive steps people can take to protect themselves, and it only takes two hours a year to maintain," said Boyce. "The first time I did this, it took about two to four hours. I used to check the most common sites every quarter, but now I do it every six to 12 months. For someone in the public eye, like a celebrity, doing a quick search once a month is not a bad idea. These companies merge and spin off on a regular basis."

You can subscribe to services such as DeleteMe that offer this type of protection. However, information automatically added from other sites can re-proliferate, and some data brokers only respond to removal requests from the affected person directly, so even if you go with a paid option, you'll want to hit the sites for which DeleteMe and other removal services don't do data removal.

Opting out of marketing sites

If your primary concern is making sure that data brokers don't share intimate information about your financial problems, pregnancy, and obsession with Elvis memorabilia, that can be even trickier, explains Kalia.

"A lot of the times the outputs that the data broker industry offers are not actually very effective," he said. "They will still hold onto that data and contain that data on you. It might be suppressed, which varies from data broker to data broker, and it's not actually the equivalent of, 'Okay now we'll stop collecting data on you because you opted out of our system.'"

There are some strategies to safeguard personal information. Web developer and online security researcher Tony Webster points out that

some state motor vehicle departments offer privacy options (though in some states they are limited to victims of identity theft or violent crimes) and that home or cell phone companies may allow users to opt out of directory information sharing and remove numbers from outbound caller ID. He also recommends opting out of pre-shared offers of credit and looking into adding a security freeze to credit reports.

"Companies can give credit bureaus a profile of consumers they're looking for—such as a credit score in a certain range, consumers who live in a certain area, or consumers with student loans—and the credit bureaus will happily sell the personal information of anyone matching that profile, as long as the company said they desire to offer them credit," he said. "It's why you receive credit card offers in the mail. But credit bureaus don't do a good enough job of ensuring the companies obtaining this information are legitimate financial institutions."

Griffin echoes the recommendation to opt out of pre-approved credit offers. Doing so can help prevent people from stealing your mail and activating credit cards, and it also limits sharing and selling of data to some extent.

"People who've opted-out are typically removed from an entire marketing campaign. When the personal data for that campaign is shared or sold, the opted-out individuals wouldn't be in that data set," he said. "A rogue dataset replicates like a virus. A company builds it, expands upon it, and tries to make a marketable profile from it. Then they sell it to someone else. And in the case of a corporate bankruptcy, the business itself typically doesn't have a say in whether this data is sold. Because in the eyes of the law, your personal data is a sellable asset."

Freezing credit

A credit freeze restricts access to your credit report, primarily to existing creditors or debt collectors acting on their behalf, and to government agencies responding to subpoenas, warrants, or court/administrative orders. Restricted access makes it difficult for identity thieves to open accounts in your name, because most creditors will want to see this credit report before opening a new account.

"People that are concerned about their privacy should exercise every option that they have. Everyone has to make that determination for themselves as to how far they want to go but certainly in this day and age with all the data breaches, freezing credit is a very good thing to do because it's probably the most effective way to prevent you from becoming a victim of identity theft," said Stephens.

The downside of freezing your credit is that it can be a bit of a hassle to temporarily lift the freeze if, for example, you need your credit checked to rent a new apartment (or for any other reason). You'll need to figure out which credit bureau its using, remember a pin number, and possibly pay a fee. "There is that nuisance factor, but certainly it's a very effective way to prevent identity theft," Stephens said.

Stop giving out information

Making your social media information public makes it vulnerable to collection from data brokers, so it can be useful to make accounts accessible only to friends and family. Locking down social media sites and avoiding online quiz apps are good ways to keep data brokers from scooping up data.

Webster further recommends exercising common sense online. "Your date of birth is frequently used as an identifier or security question, so consider not posting a photo of your birthday night celebration on Twitter," he says. But while making locking down accounts and not putting your data of birth on social media or making can prevent some of these problems, ultimately the only way to prevent your social media information getting scooped up is not to have social media.

Even if you do that, data brokers still collect data from other sources. It's not only locking down your social media, but also not giving your information out in the first place. Once your information is out there, you can't get it

back, because once one data broker gets your information because you've inadvertently disclosed it, there's really no way to get it back," said Stephens.

For those willing to go through the effort, the best thing is to be proactive and not give out your information to anybody unless you know that the business is committed to their privacy policy to not selling it to anybody. If you move, that's your perfect opportunity—you now have a new address that might not appear in the data broker index, and you can opt for a P.O. Box or a mail forwarding service. "Before you give your information to anybody, think to yourself, do they really need this information and what are they going to do with this information," said Stephens.

File a complaint

Finally, if you come across data broker sites that are behaving unscrupulously, consider **filing a complaint with the FTC**, as Abine did about BeenVerified **in 2012**.

"Consumers can file a complaint with the FTC for any practices that a company is engaged in that they feel are unfair or harming them. It goes into our complaint database which is available not only to us but to other law enforcement, and we use that information to inform our investigations as well as our policy work or other work," said George.

If you want to remove yourself from people search sites, check out our Big Ass Data Broker Opt-Out List.

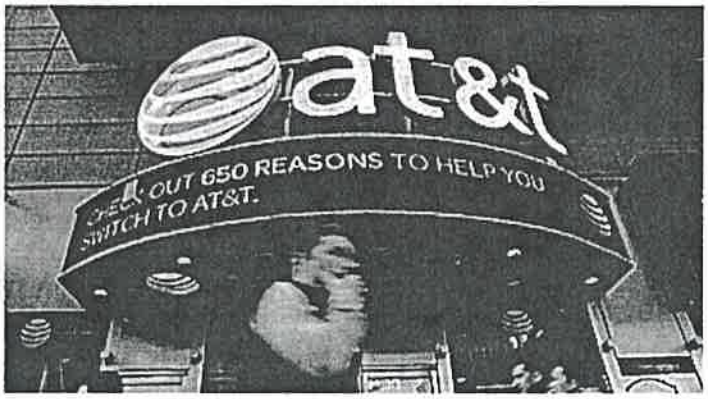
TAGGED: TECH, MOTHERBOARD, PRIVACY, SOCIAL MEDIA, FTC, DATA BROKERS

The California DMV Is Making $50M a Year Selling Drivers' Personal Information

JOSEPH COX

What Are Third-Party Internet Cookies, and Why Is Google Killing Them?

KARL BODE

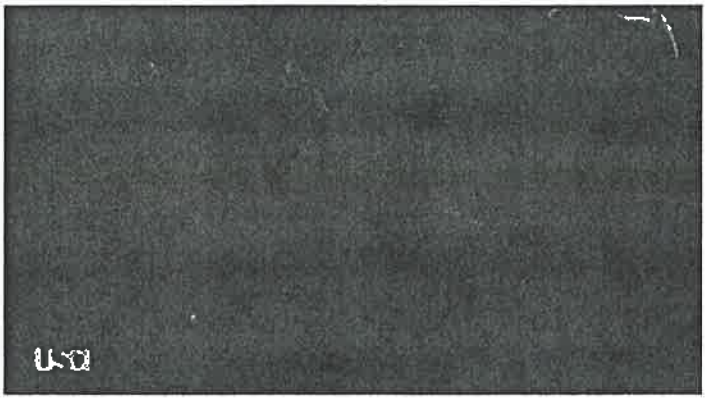


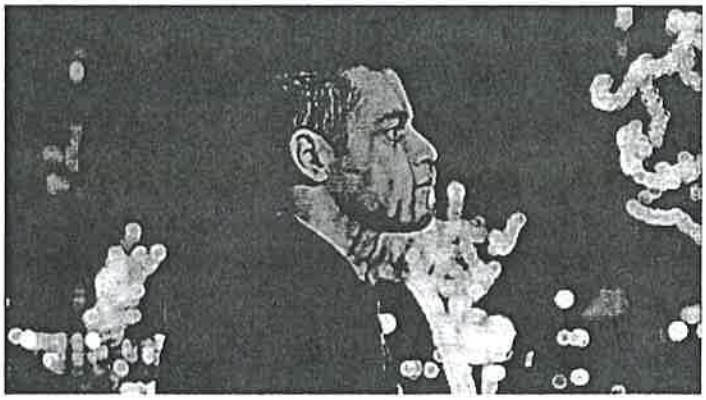
A Roundtable of Hackers Dissects 'Mr. Robot' Season 4 Episode 1: 'Unauthorized'

YAEL GRAUER

AT&T Says Customers Can't Sue the Company for Selling Location Data to Bounty Hunters

JOSEPH COX





Hackers Dissect 'Mr. Robot' Season 4 Episode 9: 'Conflict'

YAEL GRAUER

Hackers Dissect 'Mr. Robot' Season 4 Episode 8: 'Request Timeout'

YAEL GRAUER

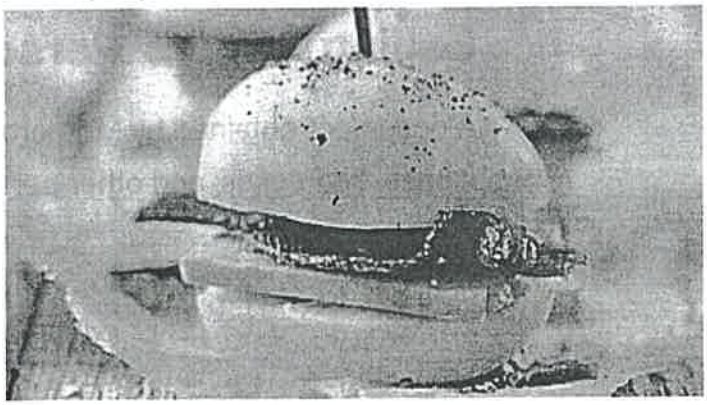
Why a Steak in California Comes With a Privacy Notice

KARL BODE

Hackers Dissect 'Mr. Robot' Season 4 Episode 6: 'Not Acceptable'

YAEL GRAUER

Most read

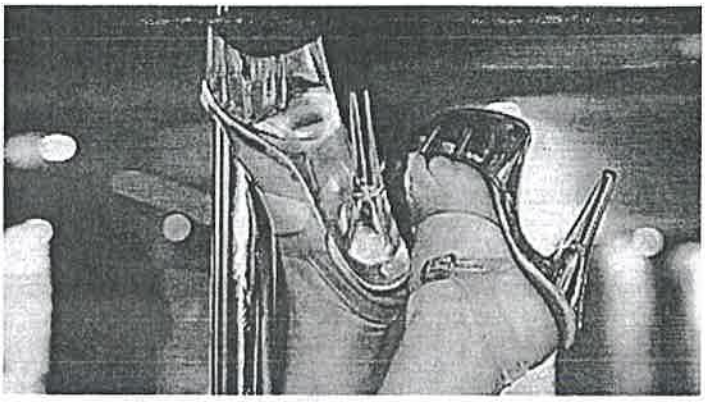


We're Working Nurses to Death

JASON SILVERSTEIN IN HEALTH

Experts Condemn Keto. Will People Finally Stop?

HANNAH SMOTHERS IN HEALTH



'This Is a Show of Force': Gun Rights Advocates and Far-Right Extremists Descend on Richmond

TESS OWEN IN NEWS

Ohio Strip Club Loses License After Accepting Food Stamps for Lap Dances, Hard Drugs

JELISA CASTRODALE IN FOOD

MOTHERBOARD
TECH BY VICE

The California DMV Is Making $50M a Year Selling Drivers' Personal Information

A document obtained by Motherboard shows how DMVs sell people's names, addresses, and other personal information to generate revenue.

By Joseph Cox

Nov 25 2019, 11:05am

IMAGE: MARK BOSTER/LOS ANGELES TIMES VIA GETTY IMAGES

The California Department of Motor Vehicles is generating revenue of

Keep Reading

MOTHERBOARD
TECH BY VICE

How to Cancel Your Amazon Prime Membership (and Why You Should)

Here's how to stop financially supporting a monopoly.

By Izzie Ramirez

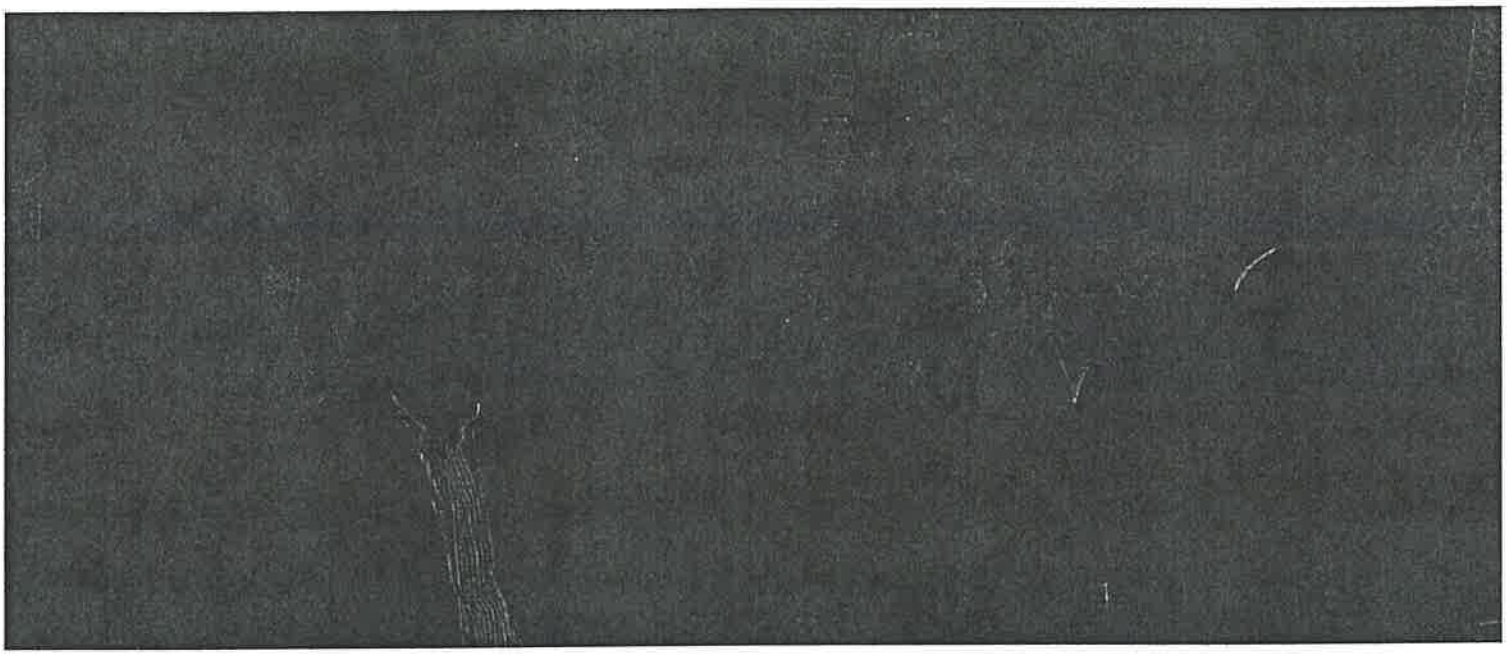
Aug 14 2019, 12:15pm

IMAGE: HUNTER FRENCH/MOTHERBOARD

Welcome to CANCELED, Motherboard's series of helpful guides on how to stop

Keep Reading

JURY LAB



Measure the True Impact of Your Arguments

Lawsuits that go to trial can be tremendously expensive — more so when perceptions of the case's strength don't match reality.

Jury Lab™ Emotion Response technology was created to mitigate that risk, improving the chance of successful outcomes by testing jury responses before the case goes to trial.

"New" Jury Lab Emotive Response Technology for ...

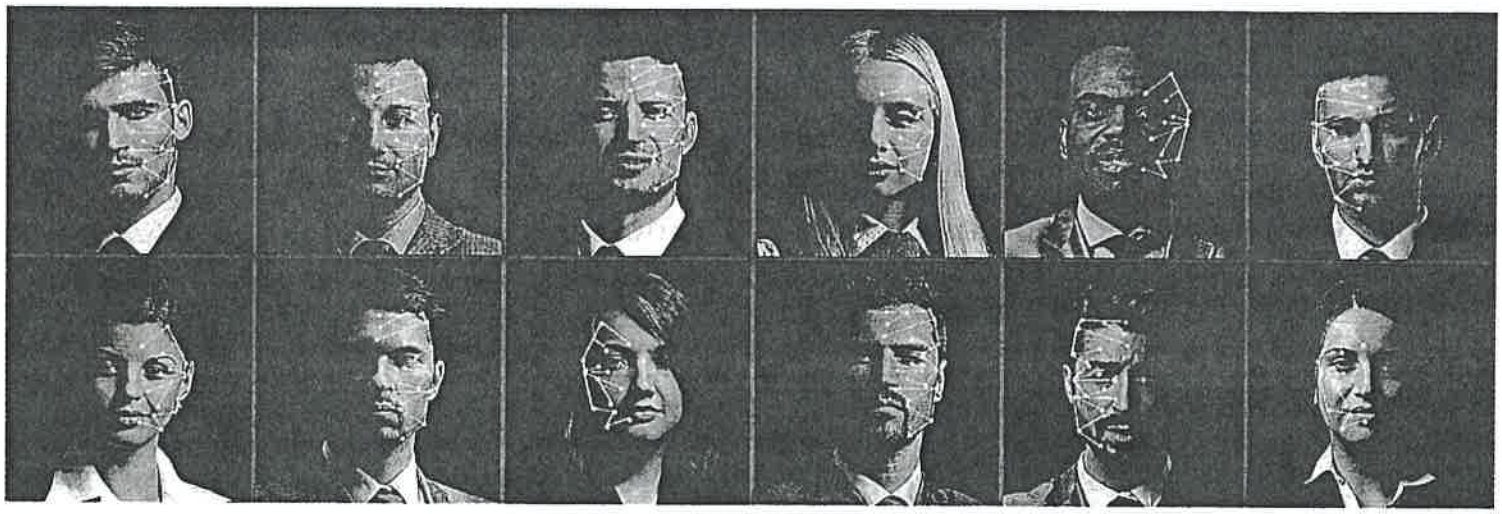
JURY LAB

"In many cases, wins and losses are decided in the opening statement."

- Susan Constantine MPsy, Founder of Silent Messages and Creator of Jury Lab

LESS RISK. MORE REWARD

THE POWER OF SCIENCE



Jury Lab is a patented emotion response software designed specifically for legal professionals.

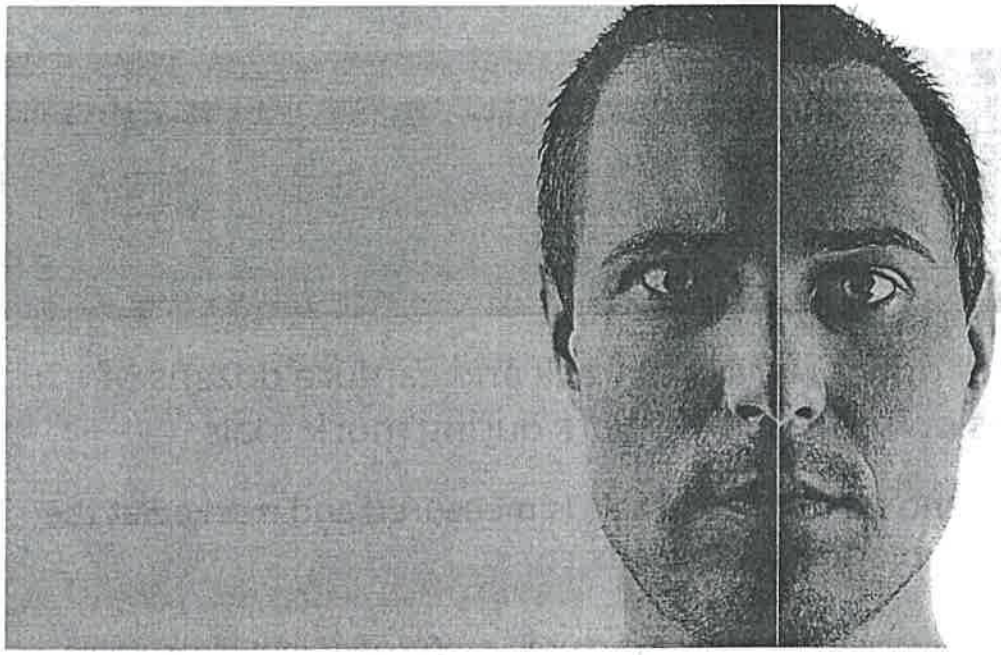
Through analysis of the facial expressions of up to 12 mock jurors, legal teams using Jury Lab are able to test arguments, key points, opening and closing arguments, photographic and video evidence, witnesses, and more, to pre-determine how a real jury might perceive their trial strategy.

profession.

So rather than the risk of assumptions, Jury Lab delivers greater clarity and certainty — which can translate into smarter settlements, adjustments in case strategy and improved chances of victory.

https://www.clickorlando.com/news/investigators/this-technology-can-tell-how-youre-feeling-by-reading-your-face

WHY JURY LAB?



Emotions may be difficult to read, but are essential to understanding.

Created by trial consultant and human behavior expert Susan Constantine , Jury Lab is premised upon the idea that the way in which people respond to an online survey, or answer a question in a group environment, may mask their true feelings.

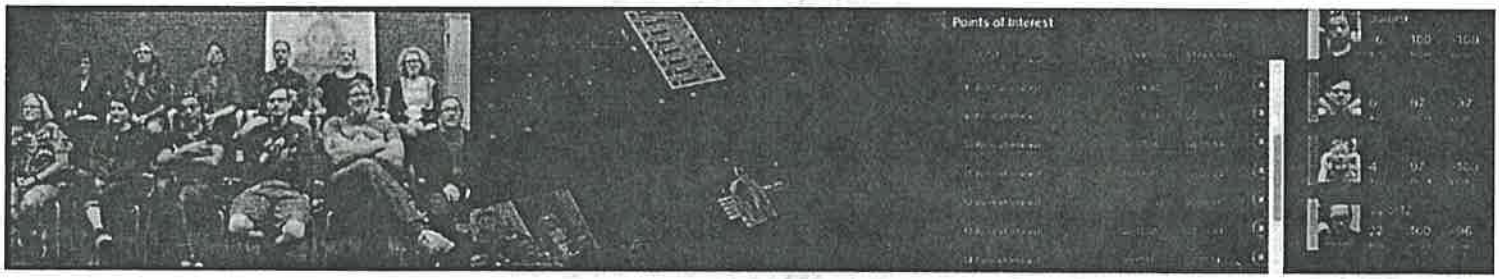
According to recent research , even the observations of the most astute federal judges, clinical psychologists and law enforcement professionals are right only about half the time when it comes to accurately gauging people's emotions.

With Jury Lab in play at mock trial settings, however, attorneys can increase that accuracy by 95%.

JURY LAB

Academia | Government agencies | Corporations

HOW IT WORKS



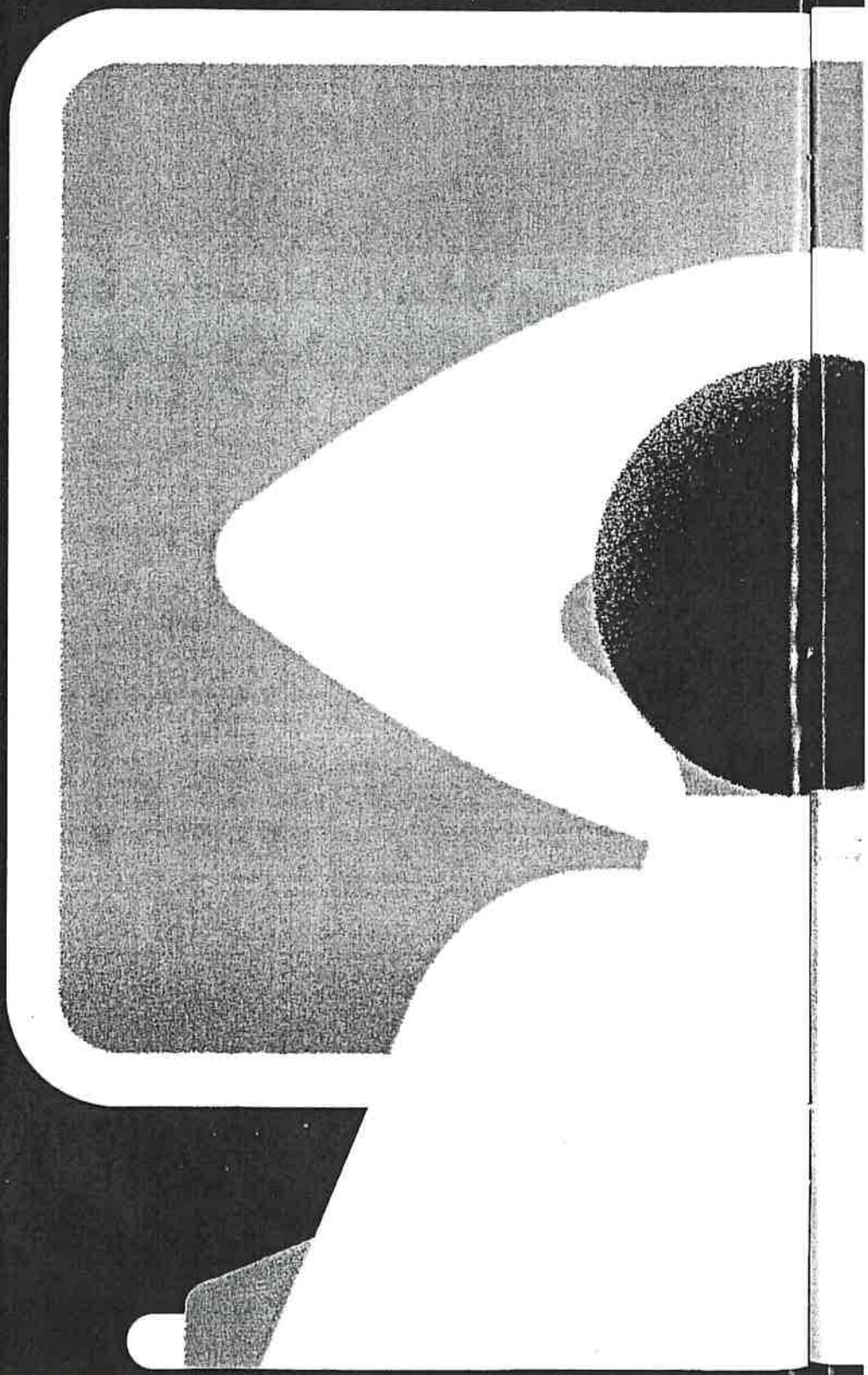
Jury Lab uses a series of optical arrays to track and capture dozens of separate locations on the faces of jurors during mock trials.

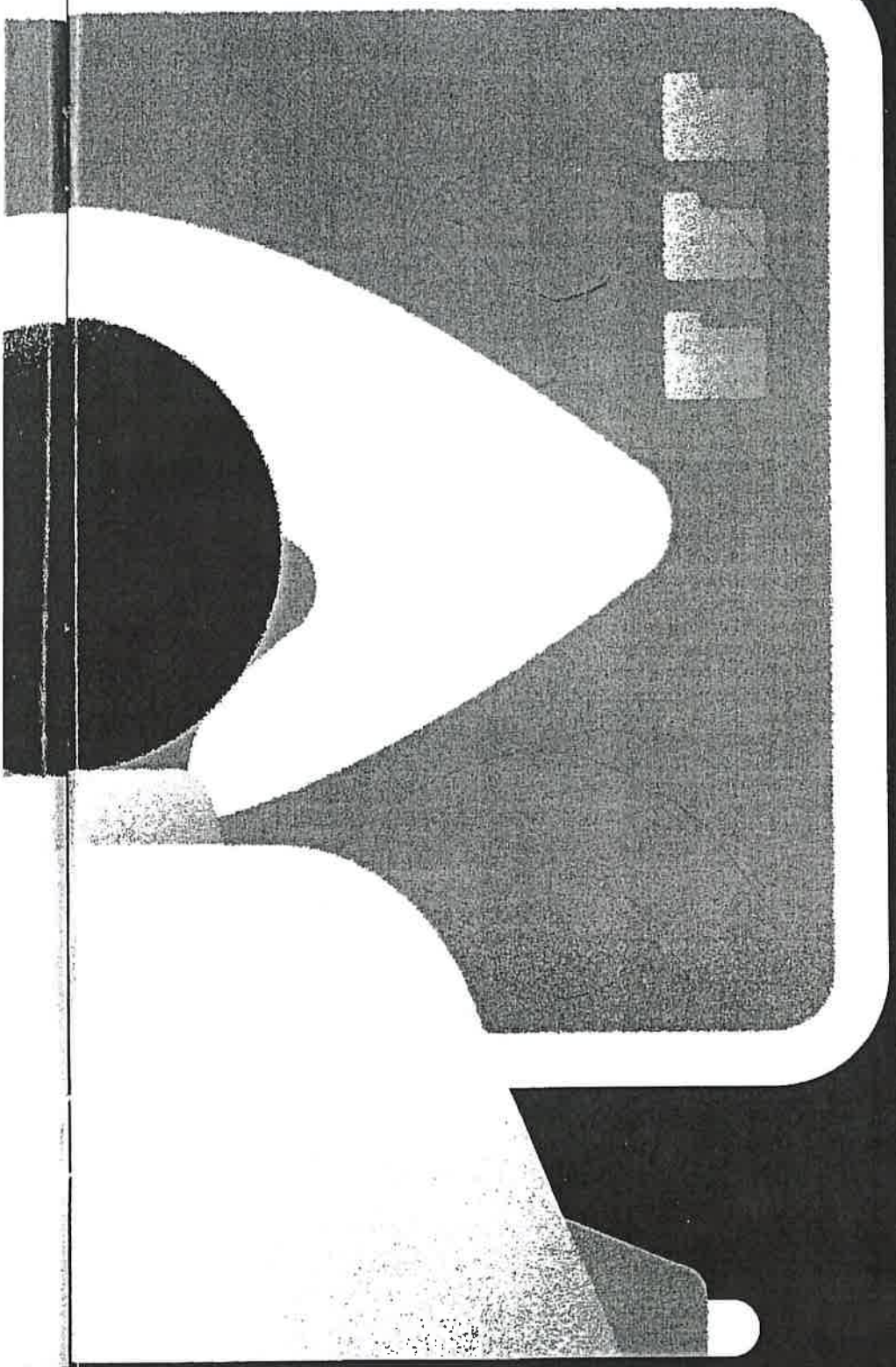
Every subtle facial expression, no matter how small, is measured and marked at the moment it happens.

Once gathered, digital algorithms convert all of these captured expressions into measurable, quantified inputs.

From these inputs are generated customized, easily understood reports legal teams can use to improve their arguments and strengthen their legal strategies.

Your Guide to Digital Privacy





Welcome to the age of ordinary objects that stealthily spy on us—from inside our cars, our homes, and our offices. That smartphone game you play in a waiting room, the mobile app that gives you a weather forecast, the photo you share with online friends—all have the ability to reveal intimate details about your life. Our increasingly digital world has created mountains of data, and there are precious few laws to safeguard the information. But that doesn't mean you can't protect yourself. According to one of three nationally representative Consumer Reports surveys that guided this special report, 60 percent of Americans now bar mobile apps from accessing the camera, GPS data, and contact list on their phones. And half protect their online accounts with two-factor authentication.* In the pages ahead, we'll provide you with more ways to protect your personal data and we'll answer key privacy questions about technologies from smart speakers to fitness trackers. Here's how to take charge of your digital domain.

ILLUSTRATIONS BY GIACOMO BAGNARA

***Source:** June 2019 Consumer Reports nationally representative survey of 1,004 U.S. adults. These questions were answered by those for whom each method was applicable.

SNEAKY GADGET

Smart Speakers That Listen When They Shouldn't

If you own a smart speaker, you should be mindful about the internet-connected microphone that lives inside it, according to David Choffnes, Ph.D., an associate professor of computer science at Northeastern University in Boston. How does he know? Well, he and Daniel Dubois, Ph.D., are conducting a privacy study on smart speakers in consultation with CR, and they have some interesting early results.

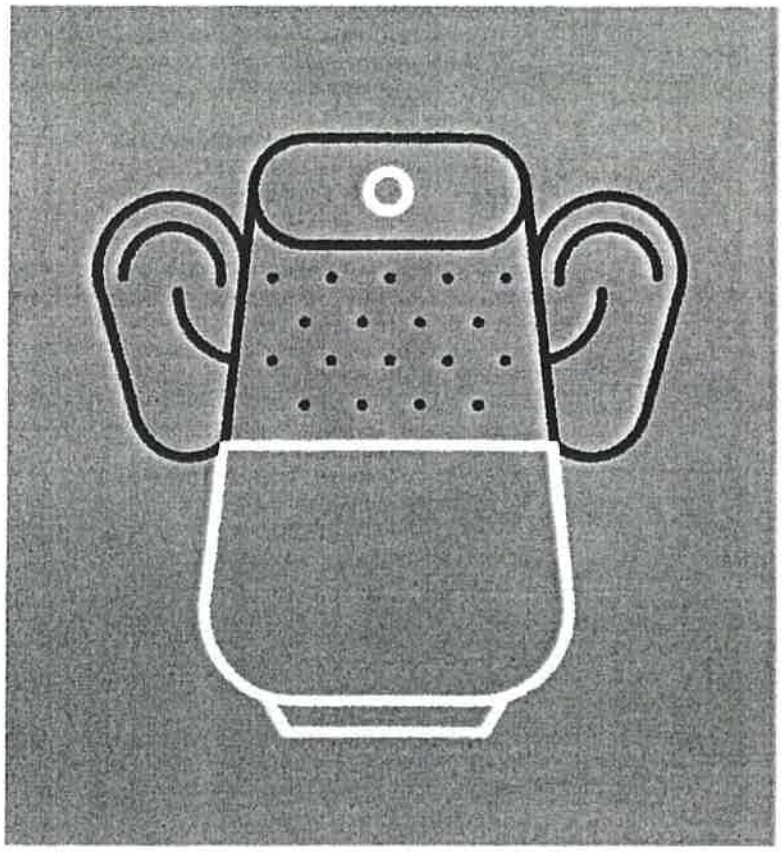
The team started with the leading brand, setting up four identical Amazon Echo speakers, each programmed to respond to a different wake word: **Alexa, Amazon, Computer,** or **Echo.** Then they exposed the devices to lots of conversation by playing three audiobooks and nine episodes of the super-talky turn-of-the-millennium TV show "Gilmore Girls."

The results? During the "Gilmore Girls" marathon, the speakers started recording snippets of dialogue 10 times without hearing the correct wake word.

During the audiobook test, the team recorded 63 false positives in 21 hours.

Some of the false positives sounded a lot like an official wake word. (See examples at right.) Others? Not so much. There was some good news: When a speaker was fooled into responding to a false wake word, it stopped recording within seconds, Choffnes reports.

We called Amazon for an explanation. "In rare cases," a spokeswoman said, "Echo devices will wake up due to a word in background conversation sounding like Alexa or one of the other available wake words." The company continues to work hard to improve the speakers' performance, she said.



Here are bits of dialogue that appeared to trigger the speakers in Choffnes' lab:

MISTAKEN FOR ALEXA
I need medical assistance • It's actually • I like [plus any word that begins with "S"] • A later [plus another word]

MISTAKEN FOR AMAZON
This is on • It was • There were none • As soon as • Last night • There was also • Eyes were wide

MISTAKEN FOR COMPUTER
Confident • Kiro

MISTAKEN FOR ECHO
Marco • Echoing • That's also

We also asked CR staffers and members of our Facebook groups for examples of accidental wake words:

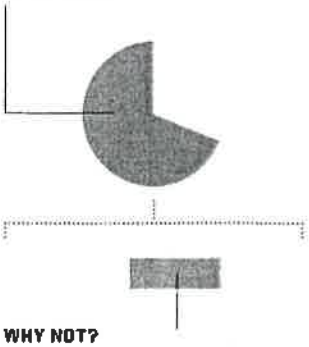
MISTAKEN FOR ALEXA
Election • I like some

MISTAKEN FOR ECHO
Petco • Pickles

MISTAKEN FOR GOOGLE
Good girl • Goofball

MISTAKEN FOR SIRI
Seriously • Hey, sir

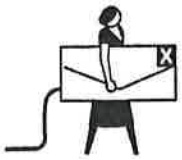
DO YOU WATCH WHAT YOU SAY AROUND YOUR SMART SPEAKER?*
69% SAY NO.



WHY NOT?
32% OF THOSE RESPONDENTS say they don't worry because the speaker listens only if you use a wake-up word.

ILLUSTRATIONS: JASON SCHNEIDER

*Source: May 2019 Consumer Reports nationally representative phone survey of 1,006 U.S. adults. These questions were answered by owners of smart speakers.



ENCRYPTED EMAIL

PROTONMAIL

Free email services, such as Gmail and Yahoo Mail, may scan your communications for anything from ad targeting to integrating mail with other apps. If that turns you off, consider shifting to ProtonMail. The service offers end-to-end encryption, which makes the contents off-limits to anyone but you and the recipient. Better yet, ProtonMail doesn't collect data on its users. In fact, you don't need to provide any personal info to register for an account. Drawbacks? The encryption hinders inbox searches. The 500-megabyte storage limit for the free service is low. And if you forget your password, you're in trouble: ProtonMail is so hands-off, it can't help you reaccess your emails.

PRESSING QUESTION

What's the Best Way to Sign In?

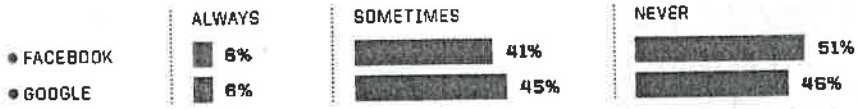
When you sign up for an app or a web account, it's very tempting to use those log-in tools provided by Facebook and Google that enroll you with a single click. But you're better off **creating your own username and password.**

"That way, you don't have to give Facebook or Google yet another way to monitor what you do online," says Justin Brookman, director of consumer privacy and technology policy at CR. Be sure the password you create is strong, Brookman adds. (Don't use Password123, and don't recycle one from another account.)

One argument for counting on the tech giants for your log-ins is their world-class security expertise. But "there's no such thing as perfect security," says Casey Oppenheim, founder of the security firm Disconnect. Early this year, for example, Facebook discovered that the passwords of hundreds of millions of users had been stored unencrypted on its servers.

When Apple releases its new log-in feature this fall, though, Oppenheim says it may be worth reconsidering his advice—at least from a security point of view. The feature, Sign In with Apple—which, much like Google Login, operates independently of the company's password manager—protects your email address by using your Apple ID instead. It uses Face ID or Touch ID for two-factor authentication. And it can generate random email addresses for new accounts that you simply delete if the accounts flood your inbox with spam. "The idea is frankly awesome," Oppenheim says, but much depends on the real-world details. "The jury's still out."

DO YOU USE FACEBOOK OR GOOGLE TO SIGN IN TO OTHER ACCOUNTS?*
Americans who have accounts on those platforms are almost evenly split on the question. Privacy and security experts say it's better to create individual log-ins for each account you create.



30-SECOND FIX

HOW TO DELETE ALEXA RECORDINGS

Amazon, Apple, and Google have at times had humans review bits of dialogue recorded by their smart speakers to improve their voice computing technology. To delete select recordings and place limits on the use of such data, you have to dip into the settings on the device's mobile app. But Amazon recently made things slightly easier with two new voice commands: **"Alexa, delete what I just said"** and **"Alexa, delete everything I said today."** Before you can use the feature, you have to activate it.

ON THE ALEXA APP:
Tap the three bars in the upper left and choose **Settings > Alexa Privacy > Review Voice History** > and flip the toggle switch to enable deletion by voice.

ILLUSTRATIONS: JASON SCHNEIDER

*Source: May 2019 Consumer Reports survey. These questions were answered by those who have an account on each platform. Data excludes those who answered "don't know" or who skipped the question.

PRESSING QUESTION

Is Public WiFi Still Dangerous?

You've probably read the advice countless times (we've given it ourselves): Don't use the WIFI in coffee shops, airports, and other public places, especially for sensitive activities, such as checking a bank balance. But are those worries outdated?

These days most websites use encryption to protect information as it travels back and forth between your device and the web. Whenever you check email, shop on Amazon, or read an article on the Consumer Reports website, you see a little lock symbol and "HTTPS" in the address bar of your browser, indicating that encryption is at work scrambling the data in transit. Even if hackers intercept, say, an email, they will be hard-pressed to decipher what it says.

Does that make WiFi a danger-free zone?

Not quite, says Gary Davis, chief consumer security evangelist for the antivirus software maker McAfee. "Things are much safer now," he explains, "but that doesn't mean all the threats have gone away."

First, PDFs—of medical records, bank statements, and so on—are transmitted in an unscrambled format. Second, there's no way to see whether most mobile apps employ HTTPS. And, finally, encryption isn't always deployed correctly. One study conducted by researchers in Europe concluded that the security of a significant number of websites had been severely harmed by "cryptographic weaknesses."

How to stay safe? Many tech-savvy folks connect to the Internet using a secure VPN (virtual private network) app. But you also might try using a cellular connection, because cellular signals are less likely than WiFi to get hacked. That's easy to do on a phone—just don't join the public WiFi network. If you're using a laptop or tablet, you can set up your phone as a WiFi hotspot—although access to that feature depends on your cellular plan.

This will burn through some data. It might also leave you with a slow connection. Or you could just use the WiFi and stay off sensitive sites. "Will I log on to my bank account on the Starbucks WiFi?" asks Chester Wisniewski of the cybersecurity firm Sophos. "No. But will I log on to Twitter? Sure."

30-SECOND FIX

LIMIT GPS TRACKING

The apps on your smartphone don't need to know where you are at all times, especially when you're not looking for a traffic report, weather forecast, or dining hotspot. Here's how to limit access to your phone's GPS data. (Apps may still use WiFi signals and other clues to infer your location, but the data is typically less precise.) While you're at it, you can use these settings to control access to your contacts and photo library, too.

ON AN IPHONE: Go to Settings > Privacy > Location Services. Then toggle the control off to stop GPS data from being transmitted. Or tap on each app individually to control which ones get access "always," "never," or "while [you're] using" the app.

ON AN ANDROID PHONE: Go to Settings > Google > Location and flip the toggle switch or scroll down to App-Level Permissions.

DATA BLACK MARKET

WHAT YOUR INFO SELLS FOR ON THE DARK WEB

Data stolen by hackers is often sold through online forums on the dark web. Here's what that personal info is worth, according to Emily Wilson, vice president of research at the security firm Terbium Labs.

Log-In Credentials

PRICE: A FEW DOLLARS

Username and password combinations for email, music streaming, and retail accounts aren't worth as much as you might expect, Wilson says. Criminals will often dump lists with tens of thousands of entries onto the Internet, driving prices down.

Credit Card Info

PRICE: UP TO $250

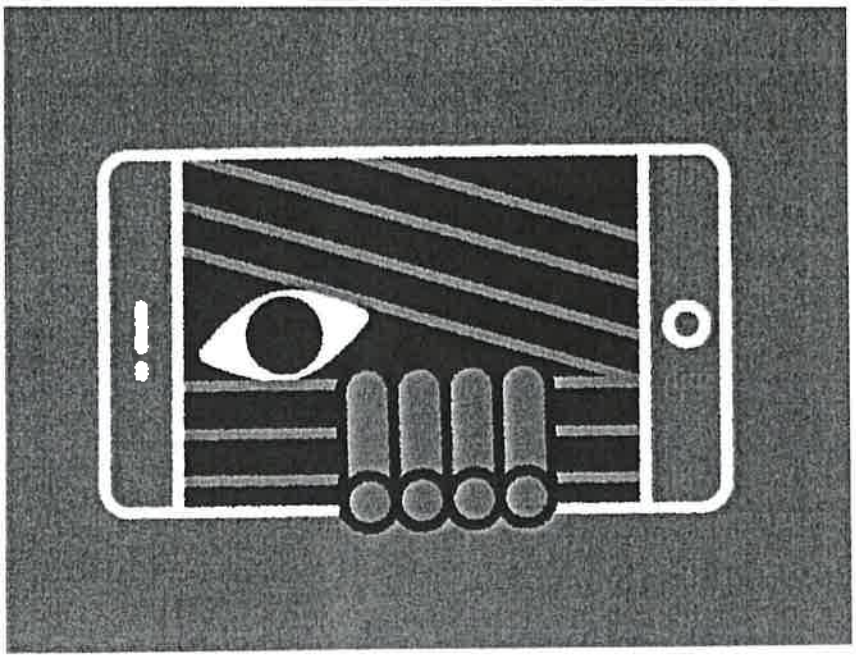
Tens of millions of credit card numbers are for sale online, Wilson says. The vast supply—plus the fact that numbers from old data breaches might no longer be valid—can limit the price to 50 cents apiece. But the price for a card with a high credit limit—think American Express Centurion card—can stretch into the hundreds.

'Fullz' Data

PRICE: UP TO $300

A complete digital profile—name, date of birth, billing address, Social Security number—opens the door for identity theft. A standard kit can cost anywhere from 50 cents to $50, Wilson says. But an infant's profile can claim $300 because the fraud it enables can go undetected for decades.

ILLUSTRATION (TWO MEN): JASON SCHNEIDER



SNEAKY GADGET

The Spy in Your Pocket

You're sitting in the kitchen with your spouse, chatting about island getaways, and minutes later an ad for a Bahamas cruise pops up on Facebook.

If such incidents have you convinced your phone is listening to you, you're not alone. (See statistic below.) But, surprise: Security experts say you're not entirely correct. You're right to think the technology industry is keeping close tabs on you—just not with your phone's mic.

Researchers led by Northeastern University associate professor David Choffnes, Ph.D., analyzed more than 17,000 widely used apps on the Android operating system and didn't find a single instance where an app activated a phone's microphone and leaked audio data without permission.

Wandera, a mobile security company, performed a similar study, focusing on high-profile apps such as Amazon, Chrome, Facebook, Instagram, and YouTube. And, just like Choffnes' team, it found no evidence of secret recordings.

The researchers weren't surprised.

Choffnes says the speech-to-text translation required to mine that audio data is relatively poor in quality. "It's just not an effective way to spy on people, compared to the extensive web and mobile app tracking ecosystem put in place by the major tech platforms, advertisers, and data brokers."

So what's really going on? People underestimate just how much data companies such as Google collect through methods having nothing to do with microphones, says Clay Miller, chief technology officer for the mobile security firm SyncDog. The sites you visit; the products you buy or simply read about; the places you live, work, and travel; and other personal details can help marketers decide precisely which ads to show you—especially when they can compare the data with the information on tens of millions of other people. At times, the process can seem like magic.

Not that apps don't do some dodgy things. For instance, the Northeastern study found about 9,000 apps with the potential to take and transmit screenshots of the app in use on a person's phone—potentially recording information as it's being entered and sharing it with third parties.

For what it's worth, mobile apps often suck up GPS and contact list data, too. To reduce such privacy intrusions, take a moment to read the permissions before installing an app, review those permissions on your phone every now and then (see the facing page), and avoid using Facebook and Google log-in features (page 29).

THINK YOUR PHONE SECRETLY LISTENS?*

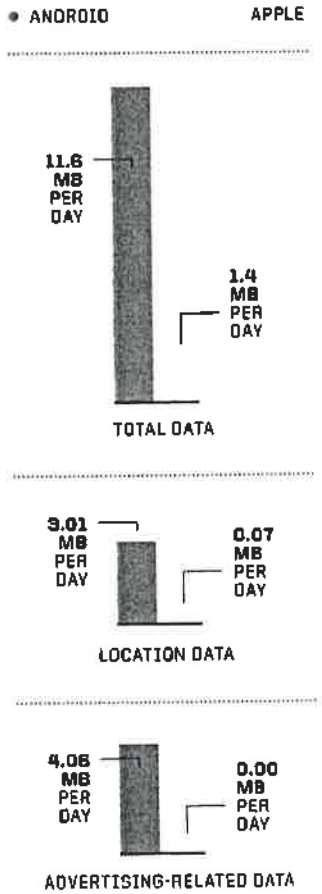
43% SAY YES. But security experts who study the question say no. Your phone does snoop on you—just not with its microphone.

A TALE OF TWO PHONES

ANDROID VS. APPLE

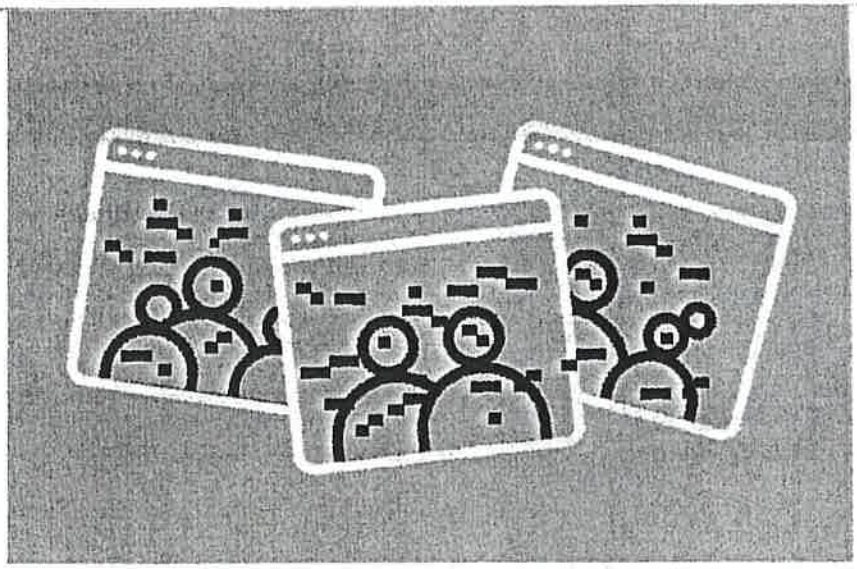
Smartphones collect all sorts of info about us—even when we're not using them. In 2018, Douglas C. Schmidt, a computer science professor at Vanderbilt University in Nashville, Tenn., set out to see how often Android phones and iPhones quietly send data back to the servers of their respective mother ships (Google and Apple). The results may surprise you.

In a typical day, Google's servers requested info from an Android phone 90.3 times per hour. Apple's servers? A less frequent 17.9 times per hour. Charted below is the volume of data relayed by each phone in that 24-hour stretch, including the approximate amounts used for location tracking and interaction with ad servers.



*Source: May 2019 CR survey. This question was answered by smartphone owners, who were asked whether they think their phone records what they say without permission.

ILLUSTRATION (TWO MEN): JASON SCHNEIDER



SNEAKY GADGET

The Oversharing Camera

When you take a snapshot with a digital camera, including the one on your smartphone, the device captures data about where, when, and how the image was recorded.

And when you share that picture with someone else, that information, called Exif data, typically goes along for the ride.

That's how mobile apps and storage services, such as Google Photos and iCloud Photos, know how to sort your Springsteen summer tour pictures by place and date.

Facebook, Instagram, Twitter, and other sites hide the data from the public, but they reserve the right to use it themselves to enhance their services.

"People should be aware that when they upload a photo, there is more to it than just the pixels they see," says University of California, Berkeley, computer science professor Hany Farid, a leading researcher on digital forensics.

Imagine, for instance, what a private investigator, savvy thief, or stalker could learn about your weekly routine simply by using the Exif data in your photo archives.

Most smartphones don't have built-in tools for removing the data, but free apps for Android and Apple phones can help you do it.

"If you are really worried, just take a screenshot of the photo and share that instead," says Bobby Richter, who oversees privacy and security testing at CR. "Screenshots typically don't include the same sensitive metadata as photos from a camera."

For some people, though, the only bit of Exif data that feels too personal is the info on where the photo was taken. "That's a pretty serious privacy issue," Farid says. "You know where [those in the picture] are at a given time of day."

If you want to keep that location information out of your images, simply revoke the camera app's access to the GPS function on your device.

In iOS, go to **Settings > Privacy > Location Services > Camera > Never.**

Instructions for Android devices vary by model, but typically you need to open **Settings > Lock Screen & Security > Location > App-Level Permissions** and switch the toggle off for **Camera.** On certain Android devices, camera apps have their own GPS setting.

To strip out the location data from photos stored on your computer, do the following.

In Windows, right-click on the image file, then **Properties > Remove Properties and Personal Information.**

In MacOS, open the photo in Preview, then **Tools > Show Inspector > Remove Location Info.**

BETTER MESSAGING

SIGNAL

This isn't the only messaging app to provide end-to-end encryption, scrambling data so that only the sender and recipient can read the contents. But Signal—available on Android phones, iPhones, and desktops—stands out for several reasons. It lets you send messages that self-delete from both parties' phones (though the recipient could preserve the contents in a screenshot). And according to its creators, the service does not store your user name, location, or data related to your contact list—info that others, such as Facebook's WhatsApp, can use for marketing. Signal has even tested a feature that lets you encrypt other metadata, so would-be snoops can't identify who wrote the texts.

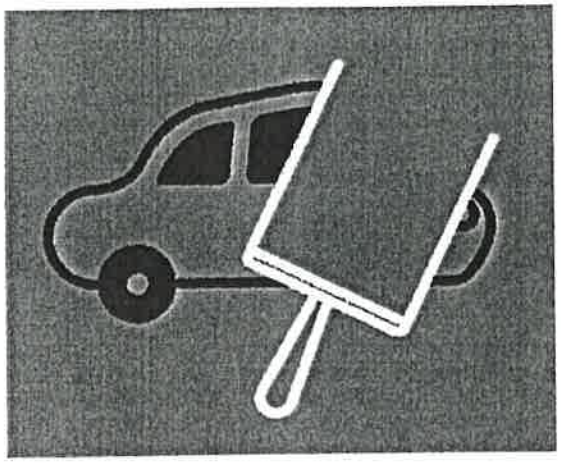
ILLUSTRATION (MAN PULLING SHADE DOWN): JASON SCHNEIDER

Reporting by Bree Fowler, Thomas Germain, Ian McClure, Chris Raymond, and Allen St. John

THE DEEP CLEAN

Wipe Data From Your Car Before Selling It

These days, vehicles collect and store all kinds of personal data—everything from the songs on your playlist to the locations you frequent to how firmly you apply the brakes. And if you're not careful, the data can travel on to your car's next owner. "That's why it's important to know your car," says CR auto analyst Mel Yu, who offers these tips for seeking and destroying the data. For more detailed instructions, consult the owner's manual for your particular vehicle.



UNPAIR ALL BLUETOOTH DEVICES
By deleting the connection to your smartphone, you protect info routinely shared for contacting friends, listening to music, and using GPS directions.

RESET THE GARAGE-DOOR OPENER
If you use a universal application, such as HomeLink, for example, you don't want it to be sharing codes that grant access to your home. To erase them, press and hold the two outer HomeLink control buttons until the red light flashes.

RESET TELEMATICS SERVICES
Blue Link, FordPass, and OnStar can all send data from a car to the cloud, even if you don't have a current subscription, Yu says. Look for an SOS or call button on the rearview mirror or overhead console. Press it and you will be connected to a live operator, who can help you change the account owner information.

LOG OUT OF CLOUD ACCOUNTS
Exclusive to certain automakers, they store driver data, including preset radio stations, favorite temperature settings, navigation destinations, and driving history.

REMOVE TRACKING DEVICES
Auto dealers, banks, and insurance companies may attach such devices to vehicles when setting up financing and coverage deals. If buyers don't read the fine print, they might not realize they're there. Once the car is paid off, check with your lender or dealer about disabling them.

ILLUSTRATION (MAN PULLING SHADE DOWN): JASON SCHNEIDER

DIGITAL WATCHDOG

CONSUMER REPORTS DOUBLES DOWN ON PRIVACY

When it comes to helping people protect their private lives from snoopy corporations and hackers alike, nothing beats a team of engineers, data experts, journalists, and advocates assigned to work on the problem full-time.

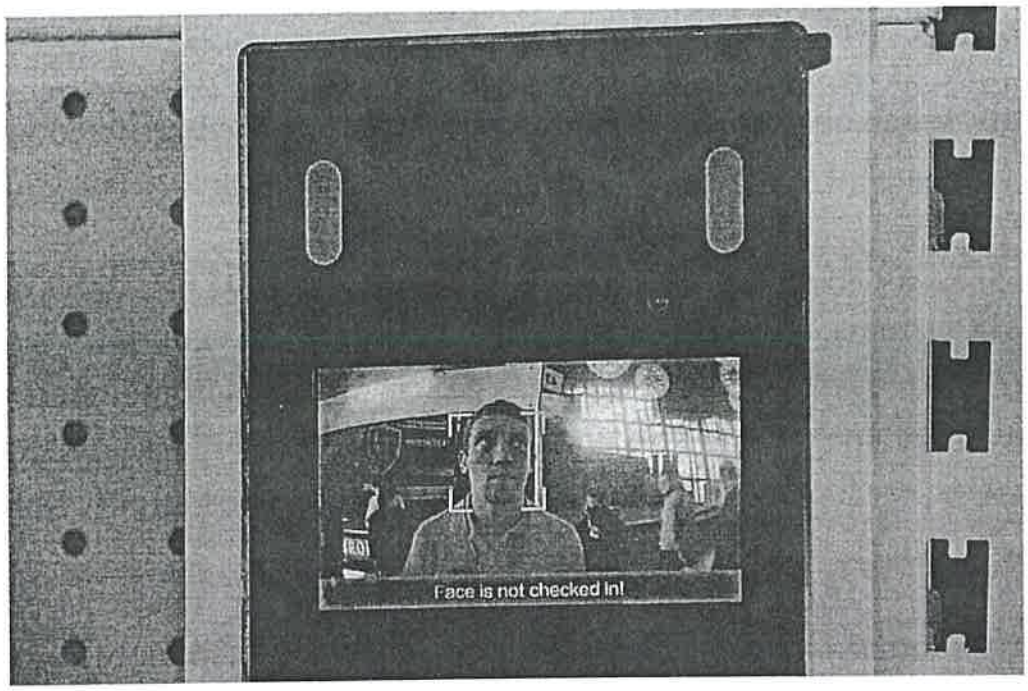
That's what CR has been creating over the past few years, and in 2019, we're taking a big step forward with a new project funded in part by a $6 million investment from Craig Newmark Philanthropies: The Digital Lab will develop new ways to empower consumers by testing and reporting on everything from online platforms such as Amazon and Google to connected thermostats to cars that collect data on their drivers.

"Our digital testing has already shown how products and services we use every day can expose us to many new and potential harms," says Marta L. Tellado, CR's CEO and president. "Consumer Reports' new Digital Lab will reveal precisely how and where our rights are undermined by the unchecked influence of technology. Armed with that knowledge, consumers can make more secure choices that protect our privacy and hold these digital giants to account." Stay tuned.

Tenants sounded the alarm on facial recognition in their buildings. Lawmakers are listening.

Imagine being locked out of your home because software selected by your landlord can't identify your face.

By Rebecca Heilweil | Dec 26, 2019, 4:00pm EST



A facial recognition-based check-in system on display in Yalta, Crimea. | Sergei Malgavko/TASS via Getty Images

OPEN SOURCED

Lawmakers want to press pause on deploying facial recognition and other biometric technology in public housing. Though it's not clear the extent to which the technology is

already being used in public housing (or other categories of government-supported and -regulated housing), lawmakers say facial recognition raises privacy concerns, and point to its known inaccuracies, especially when applied to people of color and women (among other minority groups).

There's no law regulating facial recognition at the federal level yet. But complementary legislation introduced in the House and the Senate — the "No Biometric Barriers to Housing Act" — would put a hold on the use of biometric-based recognition systems in most housing supported by the Department of Housing and Urban Development (HUD). The bill also directs the department to conduct research into the technology and its potential impact on residents of public housing.

HUD says on its website that about 1.2 million people live in public housing units, which are run by more than 3,000 housing agencies.

"[W]hen public housing and federally assisted property owners install facial recognition security camera systems, they could be used to enable invasive, unnecessary, and harmful government surveillance of their residents," wrote eight members of Congress, including Sens. Cory Booker and Ron Wyden and Reps. Yvette Clarke and Rashida Tlaib, in a letter to HUD Secretary Ben Carson last week. "Those who cannot afford more do not deserve less in basic privacy and protections."

Among other questions, lawmakers want to know how many federally assisted public housing properties have already used facial recognition.

"The goal of what this bill does is getting ahead of [facial recognition] before it becomes an issue," said Sarah Sinovic, a spokesperson for Rep. Clarke, who first proposed the House legislation alongside Reps. Tlaib and Ayanna Pressley in July. "We don't want to get into a situation where individuals are subjected to this and there hasn't been anything to pump the brakes."

An online petition in support of the bill has already attracted at least 44,000 signatures, though the legislation does have at least one critic: the Information Technology and Innovation Foundation. The think tank said in an online statement that "[r]ather than lock out low-income Americans from the latest innovations, Congress should welcome

the availability of technology that prevents them from getting locked out of their homes."

It's not clear how widespread the technology actually is. In Detroit, surveillance cameras installed in public housing could be used in conjunction with facial recognition technology, according to the New York Times. In New York City, facial recognition has also been used for years at a Lower East Side affordable housing complex called Knickerbocker Village, as reported by the Gothamist, that's overseen by New York State's Division of Housing and Community Renewal (DHCR).

In a statement to Recode, a HUD spokesperson said that no housing authorities have asked to fund facial recognition software through its emergency safety and security fund (that's the same thing HUD told the New York Times in September). The spokesperson did not clarify whether this fund was the only way in which HUD could become aware of facial recognition used in federally assisted housing.

Barbara Brancaccio, a spokesperson for the New York City Housing Authority, which oversees low- and moderate-income housing, says facial recognition is not used at any of its developments.

The case of Atlantic Plaza Towers

The proposed federal legislation was inspired by the organizing efforts of New York residents of Atlantic Plaza Towers, a rent-stabilized building complex in Brownsville, Brooklyn.

Residents there successfully pushed their landlord, Nelson Management, to withdraw plans for a facial recognition system. The proposed federal bill technically wouldn't apply to those residents (the buildings are not HUD-assisted housing), but their objections highlight much of what has lawmakers worried. For one thing, the residents of Atlantic Plaza Towers only became aware of the introduction of the technology through a "modification of services" application document that must be sent to tenants. In the case of Atlantic Plaza Towers, that notice is only required because facial recognition was not initially used by the building complex.

(Brooklyn Legal Services, which assisted the Atlantic Plaza Towers tenants, has said that only some of the residents got the notice, adding to concerns about basic transparency

with residents.)

The document sent to residents (which you can view at the bottom of this article) argues that traditional key fobs allow people who are not authorized to enter the building, and that key fobs can also be copied. "Facial recognition cannot be duplicated whereas a key fob can be," says the note, explaining that the building owner planned to use facial recognition technology provided by a Kansas-based security company called StoneLock. (AI Now, a research nonprofit, wrote a letter to DHCR explaining that the StoneLock offers a somewhat unique biometric system since it identifies faces through heat-mapping).

Tranae Moran, a community organizer at Atlantic Plaza Towers and privacy advocate, says she was already uncomfortable with the use of facial recognition on social media platforms, and found the idea that the technology would be used to regulate entry into her building "immediately alarming." She said that no significant effort was made to explain the technology to residents.

Residents also had other concerns. The technology is known to be especially inaccurate when applied to women and people of color (who constitute a large majority of Atlantic Plaza Towers residents). Those findings were confirmed by a National Institute of Standards and Technology study released last week.

Moran said she was also worried about children being scanned into the system, and added that the community at Atlantic Plaza Towers already feels surveilled, noting that the system was proposed amid increasing gentrification in her neighborhood.

"You're basically locked out of having agency over your own biometrics, which is worse than being locked out of your credit card or your debit card or having an account frozen because of some funny activity," said Fabian Rogers, a floor captain and community advocate at the Atlantic Plaza Towers Tenant Association.

He expressed concern that residents wouldn't have control over the data collected by these systems, that the technology could be used to enforce evictions, and that the police could potentially gain access to the system and its data.

"Affordable housing populations are being heavily taken advantage of because of the fact that their circumstances hinder them from being part of the fight for better,

essentially. And landlords are running amuck because there aren't proper policies to protect tenants in the first place," he said.

"Imagine coming home from work at the end of the day — you might work one, two, maybe three jobs — you're trying to get into your home. And you can't get through your front door, you can't get past the lobby because the screening [or] the scan of your face doesn't recognize you as you," added Sinovic. "Just because someone happens to be lower-income and in public housing doesn't mean that they should be the ones that are the guinea pigs that are used for this software."

After significant tenant organizing, the residents managed to put a hold on the plans, and the landlord withdrew the application. "I appreciate feedback from residents and stakeholders throughout this process, and look forward to continued progress on upgrades at Atlantic Plaza Towers," said Nelson Management president Robert Nelson in a statement to Recode.

"[Nelson Management] could still put in an application literally months away from now and we still have no proper protection," cautions Rogers. Nelson Management did not clarify to Recode whether it would potentially move to install a facial recognition system in the future.

New York is pushing legislation to give tenants more options

A proposed bill in New York City would guarantee tenants the right to a physical key, and says that landlords can't force tenants to use various security technologies to enter their homes, including "facial recognition" and "biometric scanning." Legislation has also been proposed in the New York State Senate and Assembly that would ban the use of facial recognition in residential buildings.

"Technology that discriminates against tenants of color, denies residents access to their own homes, and robs tenants of their privacy rights and control over their own biometric data does not belong in residential spaces, no matter how the building is zoned," said Samar Katnani, an attorney at Brooklyn Legal Services, in an email. Brooklyn Legal Services says it's aware of at least four other New York City buildings with facial recognition, and a fifth that is moving to install the technology.

But none of that legislation has been enacted yet. Since the case of Atlantic Plaza Towers' proposal, DHCR has received one application for the use of facial recognition technology in a rent-regulated building in Corona, Queens, whose owner wants to install a "virtual doorman" that will provide several methods for entering the building, including facial recognition and a traditional key.

"[The Office of Rent Administration] will not issue an order until it has carefully reviewed both the owner's and tenants' submissions," said Sochet Charni, a spokesperson for DHCR, in an emailed statement to Recode.

Meanwhile, Moran is calling for more collaboration among lawmakers, organizers, and technology experts.

"Terms change every few years in technology. By the time something goes into effect for 'facial recognition,' we're going to be dealing with something new under a new name and new term," said Moran of the laws that have been proposed. "The walls between agencies and between industries are way too high. They need to open some windows and talk to each other."

Below is an excerpt from the document, provided to Recode by Brooklyn Legal Services, sent to some residents of Atlantic Plaza Towers.

	New York State Division of Housing and Community Renewal Gertz Plaza 92-31 Union Hall St. Jamaica, NY 11433 Web Site www.nyshcr.org	Docket Number: **GS210008OD**

Notice of Commencement of Proceeding Upon Owner's Application for Modification of Services

Mailing Address Of Tenant:	Correspondence Address:
Various 216 Rockaway Avenue Brooklyn, NY 11233	NYS Division of Housing & Community Renewal Office of Rent Administration / MCI Unit Gertz Plaza 92-31 Union Hall Street Jamaica, NY 11433

Subject Building (If Different From Tenant's Mailing Address)
(Number and Street) (Apt. No.) (Municipality)
Same as above

Attached is a copy of an owner's application to modify services that are provided with your housing accommodation.

Please read the attached carefully, and file your answer in the space provided below in duplicate, together with any supporting documentation to the Rent Office shown above within twenty (20) days of the date of mailing of this notice.

Reports and Publications

Department of Financial Services

Press Release

January 04, 2020

DEPARTMENT OF FINANCIAL SERVICES ISSUES ALERT TO REGULATED ENTITIES CONCERNING HEIGHTENED RISK OF CYBER ATTACKS

New York — Today the Department of Financial Services (DFS) issued the following industry letter to all regulated entities following recent events and the need for heightened cybersecurity precautions.

January 4, 2020

To: All Regulated Entities

Subject: Cybersecurity Risk Alert

There is currently a heightened risk of cyber attacks from hackers affiliated with the Iranian government.[1] The Iranian government has vowed to retaliate against the United States for the death of Qassem Soleimani. Given Iranian capabilities and history, U.S. entities should prepare for the possibility of cyber attacks.

Reports and Publications

history of launching cyber attacks against the U.S., ance, in 2012 and 2013, Iranian-sponsored hackers launched denial of service attacks against several major U.S. banks. And the U.S. government recently advised in June 2019 it observed "a recent rise in malicious cyber activity directed at United States industries and government agencies by Iranian regime actors and proxies," and that Iranian attackers were increasingly using highly destructive attacks that delete or encrypt data.[2]

DFS therefore strongly recommends that all regulated entities heighten their vigilance against cyber attacks. While currently there are no specific, credible, reports of new Iranian-sponsored cyber attacks in the past few days, all regulated entities should be prepared to respond quickly to any suspected cyber incidents. Iranian-sponsored hackers have historically relied primarily on common hacking tactics such as email phishing, credential stuffing, password spraying, and targeting unpatched devices.

DFS therefore recommends that all regulated entities ensure that all vulnerabilities are patched/remediated (especially publicly disclosed vulnerabilities), ensure that employees are adequately to deal with phishing attacks, fully implement multi-factor authentication, review and update disaster recovery plans, and respond quickly to further alerts from the government or other reliable sources. It is particularly important to make sure that any alerts or incidents are responded to promptly even outside of regular business hours – Iranian hackers are known to prefer attacking over the weekends and at night precisely because they know that weekday staff may not be available to respond immediately.

Regulated entities should also promptly notify DFS of any significant or noteworthy cyber attack. DFS's cyber regulation requires notification "as promptly as possible but in no event later than 72 hours" after a material cybersecurity event. 23 NYCRR 500.17. And, in light of the current threat, we urge all regulated entities to notify DFS of any material incidents as soon as possible given the heightened risk, and certainly no later than the required 72 hours. This will enable DFS to disseminate information about new cyber attacks as quickly as possible.

Any questions or comments regarding this alert should be directed to CyberAlert@dfs.ny.gov.

###

Reports and Publications

There have been a number of media reports regarding the heightened risk. For example, see https://www.nytimes.com/2020/01/03/us/politics/homeland-security-iran-threat.html.

[2] See DHS, Cybersecurity and Infrastructure Security Agency, Statement on Iranian Cybersecurity Threats, June 19, 2019, at https://www.dhs.gov/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats. There have been media reports on the increasing risk of Iranian cyber attacks, such as https://www.forbes.com/sites/zakdoffman/2019/11/14/secret-iranian-network-behind-aggressive-us-cyberattacks-exposed-in-new-report/#d3b7f5579cc8.

Instagram Twitter

Reports and Publications

42-OCT Wyo. Law. 44

Wyoming Lawyer
October, 2019

Tech Tips
Blake A. Klinkner
Washburn University School of Law
Topeka, Kansas

FACIAL RECOGNITION TECHNOLOGY, BIOMETRIC IDENTIFIERS, AND STANDING TO LITIGATE INVASIONS OF DIGITAL PRIVACY

In August 2019, the United States Court of Appeals for the Ninth Circuit became the first appellate court in the United States to declare that a social media website's use of facial recognition software to identify and track individuals may violate the individuals' privacy interests and provide the individuals with standing to sue over their rights to privacy. As individuals grapple with ways to protect online privacy and curb perceived abuses of privacy by tech giants, the Ninth Circuit's opinion may open the door for individuals to seek vindication of their rights to privacy through the filing of tort actions across the country.

In *Patel v. Facebook*, Inc., the plaintiffs filed a class action lawsuit against Facebook alleging that Facebook violated provisions of the Illinois Biometric Information Privacy Act ("BIPA"), which prohibits a party from collecting, storing, and using biometric identifiers for an individual without first obtaining a written release for the biometric identifier and without establishing a retention schedule that requires the permanent destruction of the biometric information. [1] The BIPA defines a "biometric identifier" to include any scanning of a person's "face geometry." [2] Since at least 2010, Facebook has employed facial recognition software to scan uploaded photos in order to create "face signatures" and "face maps" which help Facebook to identify and track the individuals contained within the photos. [3] In order to create these face signatures and maps, Facebook's facial recognition software scans pictures to "extract[] the various geometric data points that make a face unique, such as the distance between the eyes, nose, and ears." [4] Facebook then uses this information to "identify that individual in any of the other hundreds of millions of photos uploaded to Facebook

each day, as well as determine when the individual was present at a specific location." [5] Facebook sought dismissal of the class action lawsuit, arguing that "the plaintiffs' complaint describes a bare procedural violation of BIPA rather than injury to a concrete interest, and therefore plaintiffs failed to allege that they suffered an injury-in-fact that is sufficiently concrete for purposes of standing." [6]

In allowing the class action to proceed, the Ninth Circuit began its analysis by observing that privacy rights are at the heart of the plaintiffs' claim against Facebook and by declaring that "[p]rivacy rights have long been regarded as providing a basis for a lawsuit in English or American courts." [7] The court then concluded that "an invasion of an individual's biometric privacy rights has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," and that more specifically "the capture and use of a person's biometric information invades concrete interests" in the person's privacy. [8]

Privacy advocates have hailed *Patel* as a victory for individual users of social media. The growing use of facial recognition software and other biometric technology has come to the attention of courts nationwide, which increasingly "recognize[] that advances in [such] technology can increase the potential for unreasonable intrusions into personal privacy." [9] This recent recognition within the courts should make it easier for plaintiffs to overcome the issues of standing which have frequently thwarted lawsuits alleging cyber harms, and result in more actions pertaining to digital privacy. Social media giants and other entities with a digital presence would be wise to proceed cautiously in how they obtain, store, and utilize biometric data, especially as the biometric technologies at their disposal become more advanced every day.

Footnotes

1 *Patel v. Facebook, Inc.*, No. 18-15982, 2019 WL 3727424, at *2 (9th Cir. Aug. 8, 2019).

2 *Id.* (citation omitted).

3 *See id.* at *1.

4 *Id.*

5 *Id.* at *5.

6 *Id.* at *4.

7 *See id.*

8 *Id.* at *5-6.

2019 WL 5665577

The Hill

Booker introduces bill banning facial recognition tech in public housing

November 01, 2019

Chris Mills Rodrigo

Sen. Cory Booker (D-N.J.) on Friday introduced a bill banning the use of facial recognition technology in public housing, mirroring legislation proposed in the House in July.

The No Biometric Barriers to Housing Act would block the tech from being installed in housing units that receive funding from the Department of Housing and Urban Development (HUD).

"Using facial recognition technology in public housing without fully understanding its flaws and privacy implications seriously harms our most vulnerable communities," Booker, a 2020 presidential candidate, said in a statement.

"Facial recognition technology has been repeatedly shown to be incomplete and inaccurate, regularly targeting and misidentifying women and people of color. We need better safeguards and more research before we test this emerging technology on those who live in public housing and risk their privacy, safety, and peace of mind."

Facial recognition technology, which scans faces for the purposes of identifying individuals, has received increasing scrutiny over the past few months.

Civil rights groups have expressed concerns that the technology expands unwarranted surveillance and highlighted studies that have found certain products misidentify women and people of color at higher rates.

There is currently no federal law dictating when, how, where or why facial recognition technology can be used.

Lawmakers on both sides of the aisle have pledged they will work up legislation that would limit, or even impose a temporary ban on, facial recognition technology.

The House version of the No Biometric Barriers to Housing Act, introduced by Reps. Yvette Clarke (D-N.Y.), Ayanna Pressley (D-Mass.) and Rashida Tlaib (D-Mich.), has been referred to the House Financial Services Committee.

Booker's is the second bill introduced on the issue in the Senate this year. Sens. Brian Schatz (D-Hawaii) and Roy Blunt (R-Mo.) earlier this year introduced a bill to regulate the commercial use of facial recognition technology.

Several local and state governments have taken it into their own hands to curtail or ban facial recognition technology, including California, Oregon and New Hampshire, where law enforcement has been barred from using it.

End of Document

ACLU blasts use of facial recognition technology at Taylor Swift concert

(December 18, 2018) - The American Civil Liberties Union is criticizing the "shady" use of facial recognition as a method of surveilling potential stalkers at a recent Taylor Swift concert in Los Angeles.

Attendees at the pop star's concert should be concerned about the protocols for collecting facial recognition surveillance data, according to Jay Stanley, a senior policy analyst for the ACLU's Speech, Privacy, and Technology Project.

While the technology can be an effective tool for tracking stalkers, the practice raises several questions, including whether the pictures were saved and shared with anyone or used for marketing purposes, Stanley said.

Privacy advocates are concerned about the growing use of facial recognition in public spaces such as retail stores and sporting venues. For instance, Major League Baseball announced in July it plans to allow fans entrance to stadiums using facial recognition technology instead of traditional tickets.

If venues are going to use facial recognition, operators should at least warn customers, which they did not do in the case of the Swift concert, according to the ACLU. Stanley says officials at Rose Bowl Stadium used a kiosk playing a video of Taylor Swift performance highlights to get concertgoers to present a clear frontal view in order to capture their photos.

"The officials at the concert venue should have told people that their faces would be scanned for security purposes — preferably before they paid for a ticket," Stanley said on the ACLU's website. "They also should have told attendees whether they were saving the photos and what they were planning to do with them."

By Clyde McGrady, CQ Roll Call

End of Document

LATEST SKILLET TWO CENTS VITALS OFFSPRING THE UPGRADE APP DIRECTORY HOW I WORK VIDEO

PARENTING HACKS

'Sharenting' Now May Lead to Identity Theft Later

Meghan Moravcik Walbert
9/13/19 2:30PM • Filed to: SOCIAL MEDIA

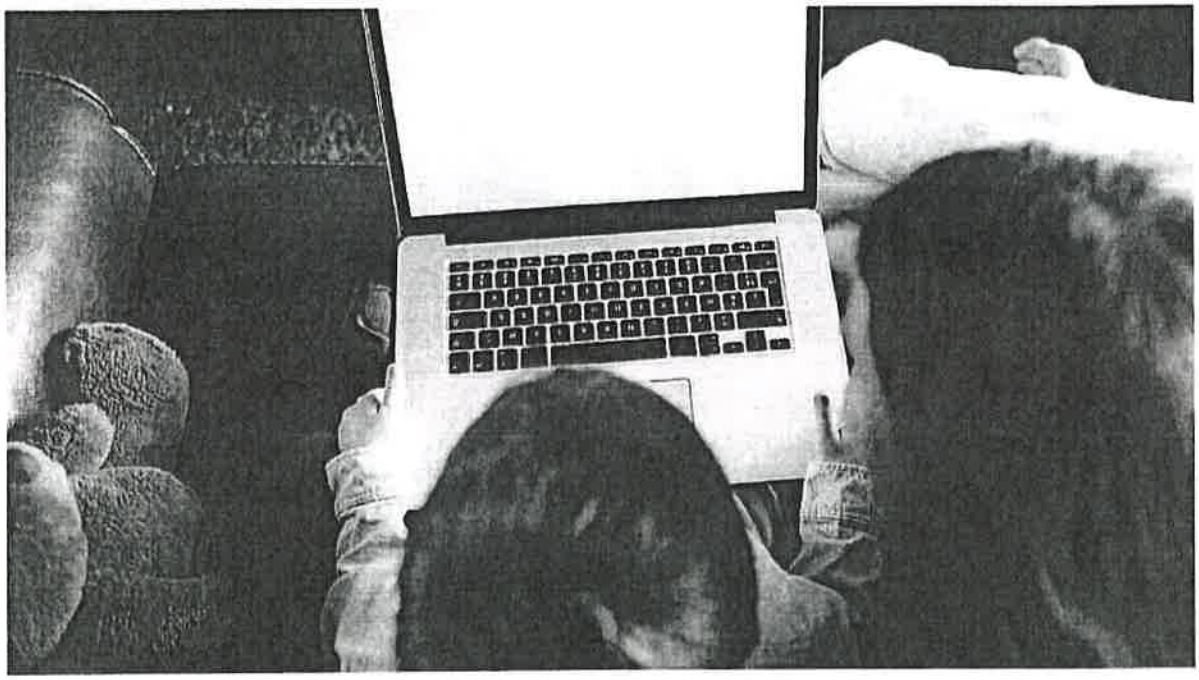


Photo: Shutterstock

There are lots of reasons to think twice before we post pictures and anecdotes about our kids online—they might find it embarrassing later, we're creating a digital life they have no control over, it's an invasion of privacy, etc. But here's another reason to lock down how much we share: We may be helping criminals steal their identity in the future.

2030. Part of the problem, the BBC reports, is that parents may not realize how much data they're producing for fraudsters through seemingly innocent posts on social media.

> The bank says parents can reveal names, ages and dates of births from birthday messages, home addresses, place of birth, mother's maiden name, schools, the names of pets, sports teams they support and photographs.
>
> Barclays warns that such details, which will still be available when young people are adults, could be used for fraudulent loans or credit card transactions or online shopping scams.

Eighteen-year-old Elmer Gomez, in particular, was concerned with information his mom had posted on Facebook, including his full name and address. When his mom defended the sharing of his photos and information—saying it's private and only seen by her friends and family—he responds, "All it takes is one person and one hack, and there goes all your privacy."

In addition to identity theft concerns, the Times points out that "parents also risk unwittingly exposing their children to data broker profiling, hacking, facial recognition tracking, pedophilia and other threats to privacy and security."

Do You Share Too Much About Your Kids Online?

As parents, we do a lot of hand-wringing over how our children will handle social media as they...

Read more

Does that mean you should stop sharing everything about your kids on social media? That's probably not realistic for most parents. However, Forbes reports that Stacey Steinberg of the University of Florida's Levin College of Law has said that parents should be talking with their kids early and often about what they're posting online:

> Steinberg is not trying to convince parents to maintain complete radio silence about their families. Instead, she is suggesting that parents give more thought to what they post, eliminate unnecessary layers of information like geotagging, and

A good rule of thumb before you post might be to pause and ask yourself: If this picture or this information got into the wrong hands, what could that mean for my child's safety and privacy? And then post—or don't post—accordingly.

Meet the smartest parents on Earth! Join our parenting Facebook group.

MORE FROM OFFSPRING

- Don't Post Your Toddler's Tantrum on Social Media
- How to Decide Whether to Post a Photo of Your Kid on Social Media
- How to Hold Off On Giving Your Kid a Smartphone (Without Them Becoming a Social Pariah)

ABOUT THE AUTHOR

Meghan Moravcik Walbert

Meghan is Lifehacker's Parenting Editor. She is a former newspaper journalist and author of the Foster Parent Diary Series for the New York Times.

Twitter Posts

Security is Inconvenient

Published on November 4, 2016

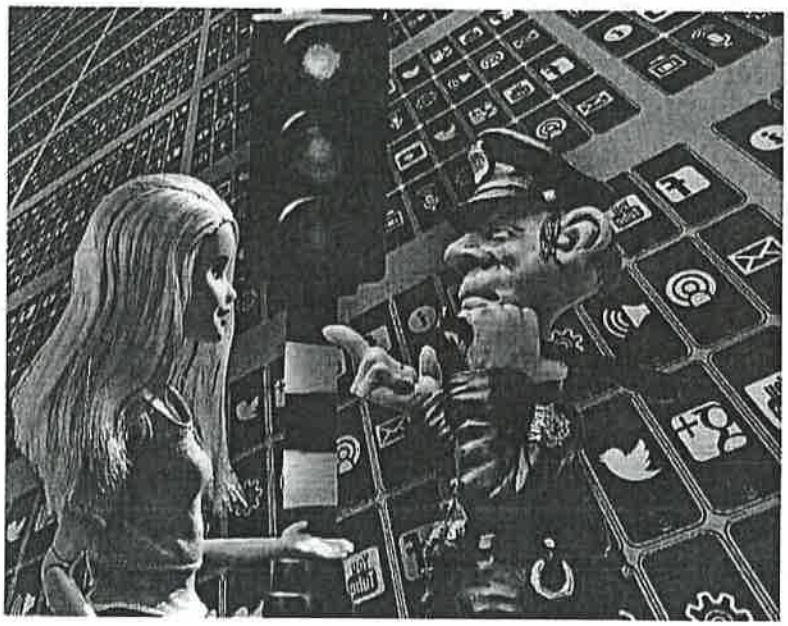
Traci Carnes
Privacy & Data Security ★ CSAP, Security+, CySA+★ IDSeal East Coast Sales Exe... See More

By the time we arrive to work, most of us have locked and unlocked 2-3 doors, entered a password or pin code into one or more devices, passed through one security check and looked both ways before crossing at least one street.

"Security is inconvenient."

James Mottola, former member of Secret Service and forensic investigation specialist, said this at a recent Cyber Security event. My immediate response was, "Yeah, but the wreckage left behind from any kind of breach, break-in or personal invasion is far worse."

Still I get it. Asking someone to change their password every six weeks, set up dual authentication on every website and constantly look over their shoulder is tiring. It's work, it's effort, it's not natural.



The Consequences of Convenience

However, as Hillary Clinton's campaign chairman, John Podesta can attest, it only takes one click of a malicious link in an email to give hackers access. This was the equivalent of not looking both ways before crossing the street. To Podesta's defense, it was a highly camouflaged car and the street was quite shady. Still, there are consequences to taking a lax approach to security.

Examples of Security Failures:

- Living Social: 50 million records compromised in 2013
- Target: 70 million records compromised in 2013
- Ebay: 145 million records compromised in 2014
- Home Depot: 56 million records compromised in 2014
- JP Morgan Chase: 76 million records compromised in 2014
- Anthem: 80 million records compromised in 2015

Security is a Habit

You didn't always lock and unlock doors, enter passwords or look both ways when crossing the street. Someone taught you and you cultivated it into a habit. The Secur

"Security Awareness Training is the most co effective way to begin to change an organizations security posture. But, as you know, security is an inconvenience, especially when we are asking people to change their habits. It must come from the to in an employee inclusive change manageme methodology."

-James Mottola, former member of Secret Service and forensic investigation specialist

Simple Security Habits Worth Cultivating

1. **Lock your computer when you aren't using it.** You can do this by se autolock or on a Windows PC, press the Windows key + L.

2. **Copy and paste links from emails.** If you really need to see what's at the end of that link, at least copy and paste it into your browser and don't click it directly. Look for HTTPS and not just HTTP. If it looks suspicious AT ALL do not press enter. Even better, enter the link at a URL checking site like safeweb.norton.com

3. **Update your security settings on a regular basis**, perhaps every time you add new employees or change systems, or on an annual basis.

4. **Do not "Friend" or return "Follow" every social media request.** Take a few minutes to investigate. Simple tests like using a reverse image search on a profile pic can reveal many suspicious accounts. Stop worrying about motives. It may not be malicious, but you really don't know. Would you feel comfortable carrying on a lengthy personal conversation with a stranger wearing a mask?

5. **Create strong passwords, change them often and use dual authentication on your primary accounts.** This is one that you'll hear time and time again. Yes, it's the most troublesome, especially if you do a lot of shopping online, but it's also the most necessary. You can also use a master password manager like Lastpass.

With nearly Half a Billion Personal Records Stolen or Lost in 2015, it's more important than ever to start taking your security seriously. For more information about protecting your business in the digital age check out All Covered's security website for tools and resources. The best habit you can ever form is the habit of staying informed.

NEW YORK RULES OF PROFESSIONAL CONDUCT

Effective April 1, 2009
As amended through June 1, 2018
With Commentary as amended through June 1, 2018

TABLE OF CONTENTS

RULE 1.6:
CONFIDENTIALITY OF INFORMATION

(a) A lawyer shall not knowingly reveal confidential information, as defined in this Rule, or use such information to the disadvantage of a client or for the advantage of the lawyer or a third person, unless:

(1) the client gives informed consent, as defined in Rule 1.0(j);

(2) the disclosure is impliedly authorized to advance the best interests of the client and is either reasonable under the circumstances or customary in the professional community; or

(3) the disclosure is permitted by paragraph (b).

"Confidential information" consists of information gained during or relating to the representation of a client, whatever its source, that is (a) protected by the attorney-client privilege, (b) likely to be embarrassing or detrimental to the client if disclosed, or (c) information that the client has requested be kept confidential. "Confidential information" does not ordinarily include (i) a lawyer's legal knowledge or legal research or (ii) information that is generally known in the local community or in the trade, field or profession to which the information relates.

(b) A lawyer may reveal or use confidential information to the extent that the lawyer reasonably believes necessary:

(1) to prevent reasonably certain death or substantial bodily harm;

(2) to prevent the client from committing a crime;

(3) to withdraw a written or oral opinion or representation previously given by the lawyer and reasonably believed by the lawyer still to be relied upon by a third person, where the lawyer has discovered that the opinion or representation was based on materially inaccurate information or is being used to further a crime or fraud;

(4) to secure legal advice about compliance with these Rules or other law by the lawyer, another lawyer associated with the lawyer's firm or the law firm;

(5) (i) to defend the lawyer or the lawyer's employees and associates against an accusation of wrongful conduct; or

(ii) to establish or collect a fee; or

(6) when permitted or required under these Rules or to comply with other law or court order.

(c) A lawyer make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).

Comment

Scope of the Professional Duty of Confidentiality

[1] This Rule governs the disclosure of information protected by the professional duty of confidentiality. Such information is described in these Rules as "confidential information" as defined in this Rule. Other rules also deal with confidential information. See Rules 1.8(b) and 1.9(c)(1) for the lawyer's duties with respect to the use of such information to the disadvantage of clients and former clients; Rule 1.9(c)(2) for the lawyer's duty not to reveal information relating to the lawyer's prior representation of a former client; Rule 1.14(c) for information relating to representation of a client with diminished capacity; Rule 1.18(b) for the lawyer's duties with respect to information provided to the lawyer by a prospective client; Rule 3.3 for the lawyer's duty of candor to a tribunal; and Rule 8.3(c) for information gained by a lawyer or judge while participating in an approved lawyer assistance program.

[2] A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, or except as permitted or required by these Rules, the lawyer must not knowingly reveal information gained during and related to the representation, whatever its source. See Rule 1.0(j) for the definition of informed consent. The lawyer's duty of confidentiality contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer, even as to embarrassing or legally damaging subject matter. The lawyer needs this information to represent the client effectively and, if necessary, to advise the client to refrain from wrongful conduct. Typically, clients come to lawyers to determine their rights and what is, in the complex of laws and regulations, deemed to be legal and correct. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is thereby upheld.

[3] The principle of client-lawyer confidentiality is given effect in three related bodies of law: the attorney-client privilege of evidence law, the work-product doctrine of civil procedure and the professional duty of confidentiality established in legal ethics codes. The attorney-client privilege and the work-product doctrine apply when compulsory process by a judicial or other governmental body seeks to compel a lawyer to testify or produce information or evidence concerning a client. The professional duty of client-lawyer confidentiality, in contrast, applies to a lawyer in all settings and at all times, prohibiting the lawyer from disclosing confidential information unless permitted or required by these Rules or to comply with other law or court order. The confidentiality duty applies not only to matters communicated in confidence by the client, which are protected by the attorney-client privilege, but also to all information gained during and relating to the representation, whatever its source. The confidentiality duty, for example, prohibits a lawyer from volunteering confidential information to a friend or to any other person except in compliance with the provisions of this Rule, including the Rule's reference to other law that may compel disclosure. *See* Comments [12]-[13]; *see also* Scope.

[4] Paragraph (a) prohibits a lawyer from knowingly revealing confidential information as defined by this Rule. This prohibition also applies to disclosures by a lawyer that do not in themselves reveal confidential information but could reasonably lead to the discovery of such information by a third person. A lawyer's use of a hypothetical to discuss issues relating to the representation with persons not connected to the representation is permissible so long as there is no reasonable likelihood that the listener will be able to ascertain the identity of the client.

[4A] Paragraph (a) protects all factual information "gained during or relating to the representation of a client." Information relates to the representation if it has any possible relevance to the representation or is received because of the representation. The accumulation of legal knowledge or legal research that a lawyer acquires through practice ordinarily is not client information protected by this Rule. However, in some circumstances, including where the client and the lawyer have so agreed, a client may have a proprietary interest in a particular product of the lawyer's research. Information that is generally known in the local community or in the trade, field or profession to which the information relates is also not protected, unless the client and the lawyer have otherwise agreed. Information is not "generally known" simply because it is in the public domain or available in a public file.

Use of Information Related to Representation

[4B] The duty of confidentiality also prohibits a lawyer from using confidential information to the advantage of the lawyer or a third person or to the disadvantage of a client or former client unless the client or former client has given informed consent. See Rule 1.0(j) for the definition of "informed consent." This part of paragraph (a) applies when information is used to benefit either the lawyer or a third person, such as another client, a former client or a business associate of the lawyer. For example, if a lawyer learns that a client intends to purchase and develop several parcels of land, the lawyer may not (absent the client's informed consent) use that information to buy a nearby parcel that is expected to appreciate in value due to the client's purchase, or to recommend that another client buy the nearby land, even if the lawyer does not reveal any confidential information. The duty also prohibits disadvantageous use of confidential information unless the client gives informed consent, except as permitted or required by these Rules. For example, a lawyer assisting a client in purchasing a parcel of land may not make a competing bid on the same land. However, the fact that a lawyer has once served a client does not preclude the lawyer from using generally known information about that client, even to the disadvantage of the former client, after the client-lawyer relationship has terminated. *See* Rule 1.9(c)(1).

Authorized Disclosure

[5] Except to the extent that the client's instructions or special circumstances limit that authority, a lawyer may make disclosures of confidential information that are impliedly authorized by a client if the disclosures (i) advance the best interests of the client and (ii) are either reasonable under the circumstances or customary in the professional community. In some situations, for example, a lawyer may be impliedly authorized to admit a fact that cannot properly be disputed or to make a disclosure that facilitates a satisfactory conclusion to a matter. In addition, lawyers in a firm may, in the course of the firm's practice, disclose to each other

information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers. Lawyers are also impliedly authorized to reveal information about a client with diminished capacity when necessary to take protective action to safeguard the client's interests. See Rules 1.14(b) and (c).

Disclosure Adverse to Client

[6] Although the public interest is usually best served by a strict rule requiring lawyers to preserve the confidentiality of information relating to the representation of their clients, the confidentiality rule is subject to limited exceptions that prevent substantial harm to important interests, deter wrongdoing by clients, prevent violations of the law, and maintain the impartiality and integrity of judicial proceedings. Paragraph (b) permits, but does not require, a lawyer to disclose information relating to the representation to accomplish these specified purposes.

[6A] The lawyer's exercise of discretion conferred by paragraphs (b)(1) through (b)(3) requires consideration of a wide range of factors and should therefore be given great weight. In exercising such discretion under these paragraphs, the lawyer should consider such factors as: (i) the seriousness of the potential injury to others if the prospective harm or crime occurs, (ii) the likelihood that it will occur and its imminence, (iii) the apparent absence of any other feasible way to prevent the potential injury, (iv) the extent to which the client may be using the lawyer's services in bringing about the harm or crime, (v) the circumstances under which the lawyer acquired the information of the client's intent or prospective course of action, and (vi) any other aggravating or extenuating circumstances. In any case, disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to prevent the threatened harm or crime. When a lawyer learns that a client intends to pursue or is pursuing a course of conduct that would permit disclosure under paragraphs (b)(1), (b)(2) or (b)(3), the lawyer's initial duty, where practicable, is to remonstrate with the client. In the rare situation in which the client is reluctant to accept the lawyer's advice, the lawyer's threat of disclosure is a measure of last resort that may persuade the client. When the lawyer reasonably believes that the client will carry out the threatened harm or crime, the lawyer may disclose confidential information when permitted by paragraphs (b)(1), (b)(2) or (b)(3). A lawyer's permissible disclosure under paragraph (b) does not waive the client's attorney-client privilege; neither the lawyer nor the client may be forced to testify about communications protected by the privilege, unless a tribunal or body with authority to compel testimony makes a determination that the crime-fraud exception to the privilege, or some other exception, has been satisfied by a party to the proceeding. For a lawyer's duties when representing an organizational client engaged in wrongdoing, see Rule 1.13(b).

[6B] Paragraph (b)(1) recognizes the overriding value of life and physical integrity and permits disclosure reasonably necessary to prevent reasonably certain death or substantial bodily harm. Such harm is reasonably certain to occur if it will be suffered imminently or if there is a present and substantial risk that a person will suffer such harm at a later date if the lawyer fails to take action necessary to eliminate the threat. Thus, a lawyer who knows that a client has accidentally discharged toxic waste into a town's water supply may reveal this information to the authorities if there is a present and substantial risk that a person who drinks the water will contract a life-threatening or debilitating disease and the lawyer's disclosure is necessary to

eliminate the threat or reduce the number of victims. Wrongful execution of a person is a life-threatening and imminent harm under paragraph (b)(1) once the person has been convicted and sentenced to death. On the other hand, an event that will cause property damage but is unlikely to cause substantial bodily harm is not a present and substantial risk under paragraph (b)(1); similarly, a remote possibility or small statistical likelihood that any particular unit of a mass-distributed product will cause death or substantial bodily harm to unspecified persons over a period of years does not satisfy the element of reasonably certain death or substantial bodily harm under the exception to the duty of confidentiality in paragraph (b)(1).

[6C] Paragraph (b)(2) recognizes that society has important interests in preventing a client's crime. Disclosure of the client's intention is permitted to the extent reasonably necessary to prevent the crime. In exercising discretion under this paragraph, the lawyer should consider such factors as those stated in Comment [6A].

[6D] Some crimes, such as criminal fraud, may be ongoing in the sense that the client's past material false representations are still deceiving new victims. The law treats such crimes as continuing crimes in which new violations are constantly occurring. The lawyer whose services were involved in the criminal acts that constitute a continuing crime may reveal the client's refusal to bring an end to a continuing crime, even though that disclosure may also reveal the client's past wrongful acts, because refusal to end a continuing crime is equivalent to an intention to commit a new crime. Disclosure is not permitted under paragraph (b)(2), however, when a person who may have committed a crime employs a new lawyer for investigation or defense. Such a lawyer does not have discretion under paragraph (b)(2) to use or disclose the client's past acts that may have continuing criminal consequences. Disclosure is permitted, however, if the client uses the new lawyer's services to commit a further crime, such as obstruction of justice or perjury.

[6E] Paragraph (b)(3) permits a lawyer to withdraw a legal opinion or to disaffirm a prior representation made to third parties when the lawyer reasonably believes that third persons are still relying on the lawyer's work and the work was based on "materially inaccurate information or is being used to further a crime or fraud." *See* Rule 1.16(b)(1), requiring the lawyer to withdraw when the lawyer knows or reasonably should know that the representation will result in a violation of law. Paragraph (b)(3) permits the lawyer to give only the limited notice that is implicit in withdrawing an opinion or representation, which may have the collateral effect of inferentially revealing confidential information. The lawyer's withdrawal of the tainted opinion or representation allows the lawyer to prevent further harm to third persons and to protect the lawyer's own interest when the client has abused the professional relationship, but paragraph (b)(3) does not permit explicit disclosure of the client's past acts unless such disclosure is permitted under paragraph (b)(2).

[7] [Reserved.]

[8] [Reserved.]

[9] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about compliance with these Rules and other law by the lawyer, another lawyer in the lawyer's firm, or the law firm. In many situations, disclosing information to secure

such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized, paragraph (b)(4) permits such disclosure because of the importance of a lawyer's compliance with these Rules, court orders and other law.

[10] Where a claim or charge alleges misconduct of the lawyer related to the representation of a current or former client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. Such a claim can arise in a civil, criminal, disciplinary or other proceeding and can be based on a wrong allegedly committed by the lawyer against the client or on a wrong alleged by a third person, such as a person claiming to have been defrauded by the lawyer and client acting together or by the lawyer acting alone. The lawyer may respond directly to the person who has made an accusation that permits disclosure, provided that the lawyer's response complies with Rule 4.2 and Rule 4.3, and other Rules or applicable law. A lawyer may make the disclosures authorized by paragraph (b)(5) through counsel. The right to respond also applies to accusations of wrongful conduct concerning the lawyer's law firm, employees or associates.

[11] A lawyer entitled to a fee is permitted by paragraph (b)(5) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary.

[12] Paragraph (b) does not mandate any disclosures. However, other law may require that a lawyer disclose confidential information. Whether such a law supersedes Rule 1.6 is a question of law beyond the scope of these Rules. When disclosure of confidential information appears to be required by other law, the lawyer must consult with the client to the extent required by Rule 1.4 before making the disclosure, unless such consultation would be prohibited by other law. If the lawyer concludes that other law supersedes this Rule and requires disclosure, paragraph (b)(6) permits the lawyer to make such disclosures as are necessary to comply with the law.

[13] A tribunal or governmental entity claiming authority pursuant to other law to compel disclosure may order a lawyer to reveal confidential information. Absent informed consent of the client to comply with the order, the lawyer should assert on behalf of the client nonfrivolous arguments that the order is not authorized by law, the information sought is protected against disclosure by an applicable privilege or other law, or the order is invalid or defective for some other reason. In the event of an adverse ruling, the lawyer must consult with the client to the extent required by Rule 1.4 about the possibility of an appeal or further challenge, unless such consultation would be prohibited by other law. If such review is not sought or is unsuccessful, paragraph (b)(6) permits the lawyer to comply with the order.

[14] Paragraph (b) permits disclosure only to the extent the lawyer reasonably believes the disclosure is necessary to accomplish one of the purposes specified in paragraphs (b)(1) through (b)(6). Before making a disclosure, the lawyer should, where practicable, first seek to persuade the client to take suitable action to obviate the need for disclosure. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to accomplish the purpose, particularly when accusations of wrongdoing in the representation of a client have been made by a third party rather than by the client. If the disclosure will be made in connection with an adjudicative proceeding, the disclosure should be

made in a manner that limits access to the information to the tribunal or other persons having a need to know the information, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[15] Paragraph (b) permits but does not require the disclosure of information relating to a client's representation to accomplish the purposes specified in paragraphs (b)(1) through (b)(6). A lawyer's decision not to disclose as permitted by paragraph (b) does not violate this Rule. Disclosure may, however, be required by other Rules or by other law. *See* Comments [12]-[13]. Some Rules require disclosure only if such disclosure would be permitted by paragraph (b). *E.g.*, Rule 8.3(c)(1). Rule 3.3(c), on the other hand, requires disclosure in some circumstances whether or not disclosure is permitted or prohibited by this Rule.

Withdrawal

[15A] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw pursuant to Rule 1.16(b)(1). Withdrawal may also be required or permitted for other reasons under Rule 1.16. After withdrawal, the lawyer is required to refrain from disclosing or using information protected by Rule 1.6, except as this Rule permits such disclosure. Neither this Rule, nor Rule 1.9(c), nor Rule 1.16(e) prevents the lawyer from giving notice of the fact of withdrawal. For withdrawal or disaffirmance of an opinion or representation, see paragraph (b)(3) and Comment [6E]. Where the client is an organization, the lawyer may be in doubt whether the organization will actually carry out the contemplated conduct. Where necessary to guide conduct in connection with this Rule, the lawyer may, and sometimes must, make inquiry within the organization. *See* Rules 1.13(b) and (c).

Duty to Preserve Confidentiality

[16] Paragraph (c) imposes three related obligations. It requires a lawyer to make reasonable efforts to safeguard confidential information against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are otherwise subject to the lawyer's supervision. See Rules 1.1, 5.1 and 5.3. Confidential information includes not only information protected by Rule 1.6(a) with respect to current clients but also information protected by Rule 1.9(c) with respect to former clients and information protected by Rule 1.18(b) with respect to prospective clients. Unauthorized access to, or the inadvertent or unauthorized disclosure of, information protected by Rules 1.6, 1.9, or 1.18, does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the unauthorized access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to: (i) the sensitivity of the information; (ii) the likelihood of disclosure if additional safeguards are not employed; (iii) the cost of employing additional safeguards; (iv) the difficulty of implementing the safeguards; and (v) the extent to which the safeguards adversely affect the lawyer's ability to represent clients (*e.g.*, by making a device or software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule, or may give informed consent to forgo security measures that would otherwise be required by this Rule. For a lawyer's duties when sharing information with nonlawyers inside or outside the lawyer's own firm, see Rule 5.3, Comment [2].

[17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. Paragraph (c) does not ordinarily require that the lawyer use special security measures if the method of communication affords a reasonable expectation of confidentiality. However, a lawyer may be required to take specific steps to safeguard a client's information to comply with a court order (such as a protective order) or to comply with other law (such as state and federal laws or court rules that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information). For example, a protective order may extend a high level of protection to documents marked "Confidential" or "Confidential – Attorneys' Eyes Only"; the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") may require a lawyer to take specific precautions with respect to a client's or adversary's medical records; and court rules may require a lawyer to block out a client's Social Security number or a minor's name when electronically filing papers with the court. The specific requirements of court orders, court rules, and other laws are beyond the scope of these Rules.

Lateral Moves, Law Firm Mergers, and Confidentiality

[18A] When lawyers or law firms (including in-house legal departments) contemplate a new association with other lawyers or law firms though lateral hiring or merger, disclosure of limited information may be necessary to resolve conflicts of interest pursuant to Rule 1.10 and to address financial, staffing, operational, and other practical issues. However, Rule 1.6(a) requires lawyers and law firms to protect their clients' confidential information, so lawyers and law firms may not disclose such information for their own advantage or for the advantage of third parties absent a client's informed consent or some other exception to Rule 1.6.

[18B] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily permitted regarding basic information such as: (i) the identities of clients or other parties involved in a matter; (ii) a brief summary of the status and nature of a particular matter, including the general issues involved; (iii) information that is publicly available; (iv) the lawyer's total book of business; (v) the financial terms of each lawyer-client relationship; and (vi) information about aggregate current and historical payment of fees (such as realization rates, average receivables, and aggregate timeliness of payments). Such information is generally not "confidential information" within the meaning of Rule 1.6.

[18C] Disclosure without client consent in the context of a possible lateral move or law firm merger is ordinarily *not* permitted, however, if information is protected by Rule 1.6(a), 1.9(c), or Rule 1.18(b). This includes information that a lawyer knows or reasonably believes is protected by the attorney-client privilege, or is likely to be detrimental or embarrassing to the client, or is information that the client has requested be kept confidential. For example, many clients would not want their lawyers to disclose their tardiness in paying bills; the amounts they spend on legal fees in particular matters; forecasts about their financial prospects; ir information relating to sensitive client matters (e.g., an unannounced corporate takeover, an undisclosed possible divorce, or a criminal investigation into the client's conduct).

[18D] When lawyers are exploring a new association, whether by lateral move or by merger, all lawyers involved must individually consider fiduciary obligations to their existing firms that may bear on the timing and scope of disclosures to clients relating to conflicts and financial concerns, and should consider whether to ask clients for a waiver of confidentiality if consistent with these fiduciary duties – *see* Rule 1.10(e) (requiring law firms to check for conflicts of interest). Questions of fiduciary duty are legal issues beyond the scope of the Rules.

[18E] For the unique confidentiality and notice provisions that apply to a lawyer or law firm seeking to sell all or part of its practice, see Rule 1.17 and Comment [7] to that Rule.

[18F] Before disclosing information regarding a possible lateral move or law firm merger, law firms and lawyers moving between firms – both those providing information and those receiving information – should use reasonable measures to minimize the risk of any improper, unauthorized or inadvertent disclosures, whether or not the information is protected by Rule 1.6(a), 1.9(c), or 1.18(b). These steps might include such measures as: (1) disclosing client information in stages; initially identifying only certain clients and providing only limited information, and providing a complete list of clients and more detailed financial information only at subsequent stages; (2) limiting disclosure to those at the firm, or even a single person at the firm, directly involved in clearing conflicts and making the business decision whether to move forward to the next stage regarding the lateral hire or law firm merger; and/or (3) agreeing not to disclose financial or conflict information outside the firm(s) during and after the lateral hiring negotiations or merger process.

NYSBA

NEW YORK STATE BAR ASSOCIATION

Serving the legal profession and the community since 1876

ETHICS OPINION 842

COMMITTEE ON PROFESSIONAL ETHICS

Opinion 842 (9/10/10)

Topic: Using an outside online storage provider to store client confidential information.

Digest: A lawyer may use an online data storage system to store and back up client confidential information provided that the lawyer takes reasonable care to ensure that confidentiality will be maintained in a manner consistent with the lawyer's obligations under Rule 1.6. In addition, the lawyer should stay abreast of technological advances to ensure that the storage system remains sufficiently advanced to protect the client's information, and should monitor the changing law of privilege to ensure that storing the information online will not cause loss or waiver of any privilege.

Rules: 1.4, 1.6(a), 1.6(c)

QUESTION

1. MAY A LAWYER USE AN ONLINE SYSTEM TO STORE A CLIENT'S CONFIDENTIAL INFORMATION WITHOUT VIOLATING THE DUTY OF CONFIDENTIALITY OR ANY OTHER DUTY? IF SO, WHAT STEPS SHOULD THE LAWYER TAKE TO ENSURE THAT THE INFORMATION IS SUFFICIENTLY SECURE?

OPINION

2. VARIOUS COMPANIES OFFER ONLINE COMPUTER DATA STORAGE SYSTEMS THAT ARE MAINTAINED ON AN ARRAY OF INTERNET SERVERS LOCATED AROUND THE WORLD. (THE ARRAY OF INTERNET SERVERS THAT STORE THE DATA IS OFTEN CALLED THE "CLOUD.") A SOLO PRACTITIONER WOULD LIKE TO USE ONE OF THESE ONLINE "CLOUD" COMPUTER DATA STORAGE SYSTEMS TO STORE CLIENT CONFIDENTIAL INFORMATION. THE LAWYER'S AIM IS TO ENSURE THAT HIS CLIENTS' INFORMATION WILL NOT BE LOST IF SOMETHING HAPPENS TO THE LAWYER'S OWN COMPUTERS. THE ONLINE DATA STORAGE SYSTEM IS PASSWORD-PROTECTED AND THE DATA STORED IN THE ONLINE SYSTEM IS ENCRYPTED.

3. A DISCUSSION OF CONFIDENTIAL INFORMATION IMPLICATES RULE 1.6 OF THE NEW YORK RULES OF PROFESSIONAL CONDUCT (THE "RULES"), THE GENERAL RULE GOVERNING CONFIDENTIALITY. RULE 1.6(A) PROVIDES AS FOLLOWS:

A LAWYER SHALL NOT KNOWINGLY REVEAL CONFIDENTIAL INFORMATION . . . OR USE SUCH INFORMATION TO THE DISADVANTAGE OF A CLIENT OR FOR THE ADVANTAGE OF A LAWYER OR A THIRD PERSON, UNLESS:

(1) THE CLIENT GIVES INFORMED CONSENT, AS DEFINED IN RULE 1.0(J);

(2) THE DISCLOSURE IS IMPLIEDLY AUTHORIZED TO ADVANCE THE BEST INTERESTS OF THE CLIENT AND IS EITHER REASONABLE UNDER THE CIRCUMSTANCES OR CUSTOMARY IN THE PROFESSIONAL COMMUNITY; OR

(3) THE DISCLOSURE IS PERMITTED BY PARAGRAPH (B).

4. THE OBLIGATION TO PRESERVE CLIENT CONFIDENTIAL INFORMATION EXTENDS BEYOND MERELY PROHIBITING AN ATTORNEY FROM REVEALING CONFIDENTIAL INFORMATION WITHOUT CLIENT CONSENT. A LAWYER MUST ALSO TAKE REASONABLE CARE TO AFFIRMATIVELY PROTECT A CLIENT'S CONFIDENTIAL INFORMATION. *SEE* N.Y. COUNTY 733 (2004) (AN ATTORNEY "MUST DILIGENTLY PRESERVE THE CLIENT'S CONFIDENCES, WHETHER REDUCED TO DIGITAL FORMAT, PAPER, OR OTHERWISE"). AS A NEW JERSEY ETHICS COMMITTEE OBSERVED, EVEN WHEN A LAWYER WANTS A CLOSED CLIENT FILE TO BE DESTROYED, " [S]IMPLY PLACING THE FILES IN THE TRASH WOULD NOT SUFFICE. APPROPRIATE STEPS MUST BE TAKEN TO ENSURE THAT CONFIDENTIAL AND PRIVILEGED INFORMATION REMAINS PROTECTED AND NOT AVAILABLE TO THIRD PARTIES." NEW JERSEY OPINION (2006), *QUOTING* NEW JERSEY OPINION 692 (2002).

5. IN ADDITION, RULE 1.6(C) PROVIDES THAT AN ATTORNEY MUST "EXERCISE REASONABLE CARE TO PREVENT . . . OTHERS WHOSE SERVICES ARE UTILIZED BY THE LAWYER FROM DISCLOSING OR USING CONFIDENTIAL INFORMATION OF A CLIENT" EXCEPT TO THE EXTENT DISCLOSURE IS PERMITTED BY RULE 1.6(B). ACCORDINGLY, A LAWYER MUST TAKE REASONABLE AFFIRMATIVE STEPS TO GUARD AGAINST THE RISK OF INADVERTENT DISCLOSURE

BY OTHERS WHO ARE WORKING UNDER THE ATTORNEY'S SUPERVISION OR WHO HAVE BEEN RETAINED BY THE ATTORNEY TO ASSIST IN PROVIDING SERVICES TO THE CLIENT. WE NOTE, HOWEVER, THAT EXERCISING "REASONABLE CARE" UNDER RULE 1.6 DOES NOT MEAN THAT THE LAWYER GUARANTEES THAT THE INFORMATION IS SECURE FROM *ANY* UNAUTHORIZED ACCESS.

6. TO DATE, NO NEW YORK ETHICS OPINION HAS ADDRESSED THE ETHICS OF *STORING* CONFIDENTIAL INFORMATION ONLINE. HOWEVER, IN N.Y. STATE 709 (1998) THIS COMMITTEE ADDRESSED THE DUTY TO PRESERVE A CLIENT'S CONFIDENTIAL INFORMATION WHEN *TRANSMITTING* SUCH INFORMATION ELECTRONICALLY. OPINION 709 CONCLUDED THAT LAWYERS MAY TRANSMIT CONFIDENTIAL INFORMATION BY E-MAIL, BUT CAUTIONED THAT "LAWYERS MUST ALWAYS ACT REASONABLY IN CHOOSING TO USE E-MAIL FOR CONFIDENTIAL COMMUNICATIONS." THE COMMITTEE ALSO WARNED THAT THE EXERCISE OF REASONABLE CARE MAY DIFFER FROM ONE CASE TO THE NEXT. ACCORDINGLY, WHEN A LAWYER IS ON NOTICE THAT THE CONFIDENTIAL INFORMATION BEING TRANSMITTED IS "OF SUCH AN EXTRAORDINARILY SENSITIVE NATURE THAT IT IS REASONABLE TO USE ONLY A MEANS OF COMMUNICATION THAT IS COMPLETELY UNDER THE LAWYER'S CONTROL, THE LAWYER MUST SELECT A MORE SECURE MEANS OF COMMUNICATION THAN UNENCRYPTED INTERNET E-MAIL." *SEE ALSO* RULE 1.6, CMT. 17 (A LAWYER "MUST TAKE REASONABLE PRECAUTIONS" TO PREVENT INFORMATION COMING INTO THE HANDS OF UNINTENDED RECIPIENTS WHEN TRANSMITTING INFORMATION RELATING TO THE REPRESENTATION, BUT IS NOT REQUIRED TO USE SPECIAL SECURITY MEASURES IF THE MEANS OF COMMUNICATING PROVIDES A REASONABLE EXPECTATION OF PRIVACY).

7. ETHICS ADVISORY OPINIONS IN SEVERAL OTHER STATES HAVE APPROVED THE USE OF ELECTRONIC STORAGE OF CLIENT FILES PROVIDED THAT SUFFICIENT PRECAUTIONS ARE IN PLACE. *SEE, E.G.*, NEW JERSEY OPINION 701 (2006) (LAWYER MAY USE ELECTRONIC FILING SYSTEM WHEREBY ALL DOCUMENTS ARE SCANNED INTO A DIGITIZED FORMAT AND ENTRUSTED TO SOMEONE OUTSIDE THE FIRM PROVIDED THAT THE LAWYER EXERCISES "REASONABLE CARE," WHICH INCLUDES ENTRUSTING DOCUMENTS TO A THIRD PARTY WITH AN ENFORCEABLE OBLIGATION TO PRESERVE CONFIDENTIALITY AND SECURITY, AND EMPLOYING AVAILABLE TECHNOLOGY TO GUARD AGAINST REASONABLY FORESEEABLE ATTEMPTS TO INFILTRATE DATA); ARIZONA OPINION 05-04 (2005) (ELECTRONIC STORAGE OF CLIENT FILES IS PERMISSIBLE PROVIDED LAWYERS AND LAW FIRMS "TAKE COMPETENT AND REASONABLE STEPS TO ASSURE THAT THE CLIENT'S CONFIDENCES ARE NOT DISCLOSED TO THIRD PARTIES THROUGH THEFT OR INADVERTENCE"); *SEE ALSO* ARIZONA OPINION 09-04 (2009) (LAWYER MAY PROVIDE CLIENTS WITH AN ONLINE FILE STORAGE AND

RETRIEVAL SYSTEM THAT CLIENTS MAY ACCESS, PROVIDED LAWYER TAKES REASONABLE PRECAUTIONS TO PROTECT SECURITY AND CONFIDENTIALITY AND LAWYER PERIODICALLY REVIEWS SECURITY MEASURES AS TECHNOLOGY ADVANCES OVER TIME TO ENSURE THAT THE CONFIDENTIALITY OF CLIENT INFORMATION REMAINS REASONABLY PROTECTED).

8. BECAUSE THE INQUIRING LAWYER WILL USE THE ONLINE DATA STORAGE SYSTEM FOR THE PURPOSE OF PRESERVING CLIENT INFORMATION - A PURPOSE BOTH RELATED TO THE RETENTION AND NECESSARY TO PROVIDING LEGAL SERVICES TO THE CLIENT - USING THE ONLINE SYSTEM IS CONSISTENT WITH CONDUCT THAT THIS COMMITTEE HAS DEEMED ETHICALLY PERMISSIBLE. *SEE* N.Y. STATE 473 (1977) (ABSENT CLIENT'S OBJECTION, LAWYER MAY PROVIDE CONFIDENTIAL INFORMATION TO OUTSIDE SERVICE AGENCY FOR LEGITIMATE PURPOSES RELATING TO THE REPRESENTATION PROVIDED THAT THE LAWYER EXERCISES CARE IN THE SELECTION OF THE AGENCY AND CAUTIONS THE AGENCY TO KEEP THE INFORMATION CONFIDENTIAL); *CF.* NY CPLR 4548 (PRIVILEGED COMMUNICATION DOES NOT LOSE ITS PRIVILEGED CHARACTER SOLELY BECAUSE IT IS COMMUNICATED BY ELECTRONIC MEANS OR BECAUSE "PERSONS NECESSARY FOR THE DELIVERY OR FACILITATION OF SUCH ELECTRONIC COMMUNICATION MAY HAVE ACCESS TO" ITS CONTENTS).

9. WE CONCLUDE THAT A LAWYER MAY USE AN ONLINE "CLOUD" COMPUTER DATA BACKUP SYSTEM TO STORE CLIENT FILES PROVIDED THAT THE LAWYER TAKES REASONABLE CARE TO ENSURE THAT THE SYSTEM IS SECURE AND THAT CLIENT CONFIDENTIALITY WILL BE MAINTAINED. "REASONABLE CARE" TO PROTECT A CLIENT'S CONFIDENTIAL INFORMATION AGAINST UNAUTHORIZED DISCLOSURE MAY INCLUDE CONSIDERATION OF THE FOLLOWING STEPS:

(1) ENSURING THAT THE ONLINE DATA STORAGE PROVIDER HAS AN ENFORCEABLE OBLIGATION TO PRESERVE CONFIDENTIALITY AND SECURITY, AND THAT THE PROVIDER WILL NOTIFY THE LAWYER IF SERVED WITH PROCESS REQUIRING THE PRODUCTION OF CLIENT INFORMATION;

(2) INVESTIGATING THE ONLINE DATA STORAGE PROVIDER'S SECURITY MEASURES, POLICIES, RECOVERABILITY METHODS, AND OTHER PROCEDURES TO DETERMINE IF THEY ARE ADEQUATE UNDER THE CIRCUMSTANCES;

(3) EMPLOYING AVAILABLE TECHNOLOGY TO GUARD AGAINST REASONABLY FORESEEABLE ATTEMPTS TO INFILTRATE THE DATA THAT IS STORED; AND/OR

(4) INVESTIGATING THE STORAGE PROVIDER'S ABILITY TO PURGE AND WIPE ANY COPIES OF THE DATA, AND TO MOVE THE DATA TO A DIFFERENT HOST, IF THE LAWYER BECOMES DISSATISFIED WITH THE STORAGE PROVIDER OR FOR OTHER REASONS CHANGES STORAGE PROVIDERS.

10. TECHNOLOGY AND THE SECURITY OF STORED DATA ARE CHANGING RAPIDLY. EVEN AFTER TAKING SOME OR ALL OF THESE STEPS (OR SIMILAR STEPS), THEREFORE, THE LAWYER SHOULD PERIODICALLY RECONFIRM THAT THE PROVIDER'S SECURITY MEASURES REMAIN EFFECTIVE IN LIGHT OF ADVANCES IN TECHNOLOGY. IF THE LAWYER LEARNS INFORMATION SUGGESTING THAT THE SECURITY MEASURES USED BY THE ONLINE DATA STORAGE PROVIDER ARE INSUFFICIENT TO ADEQUATELY PROTECT THE CONFIDENTIALITY OF CLIENT INFORMATION, OR IF THE LAWYER LEARNS OF ANY BREACH OF CONFIDENTIALITY BY THE ONLINE STORAGE PROVIDER, THEN THE LAWYER MUST INVESTIGATE WHETHER THERE HAS BEEN ANY BREACH OF HIS OR HER OWN CLIENTS' CONFIDENTIAL INFORMATION, NOTIFY ANY AFFECTED CLIENTS, AND DISCONTINUE USE OF THE SERVICE UNLESS THE LAWYER RECEIVES ASSURANCES THAT ANY

SECURITY ISSUES HAVE BEEN SUFFICIENTLY REMEDIATED. *SEE* RULE 1.4 (MANDATING COMMUNICATION WITH CLIENTS); *SEE ALSO* N.Y. STATE 820 (2008) (ADDRESSING WEB-BASED EMAIL SERVICES).

11. NOT ONLY TECHNOLOGY ITSELF BUT ALSO THE LAW RELATING TO TECHNOLOGY AND THE PROTECTION OF CONFIDENTIAL COMMUNICATIONS IS CHANGING RAPIDLY. LAWYERS USING ONLINE STORAGE SYSTEMS (AND ELECTRONIC MEANS OF COMMUNICATION GENERALLY) SHOULD MONITOR THESE LEGAL DEVELOPMENTS, ESPECIALLY REGARDING INSTANCES WHEN USING TECHNOLOGY MAY WAIVE AN OTHERWISE APPLICABLE PRIVILEGE. *SEE, E.G., CITY OF ONTARIO, CALIF. V. QUON*, 130 S. CT. 2619, 177 L.ED.2D 216 (2010) (HOLDING THAT CITY DID NOT VIOLATE FOURTH AMENDMENT WHEN IT REVIEWED TRANSCRIPTS OF MESSAGES SENT AND RECEIVED BY POLICE OFFICERS ON POLICE DEPARTMENT PAGERS); *SCOTT V. BETH ISRAEL MEDICAL CENTER*, 17 MISC. 3D 934, 847 N.Y.S.2D 436 (N.Y. SUP. 2007) (E-MAILS BETWEEN HOSPITAL EMPLOYEE AND HIS PERSONAL ATTORNEYS WERE NOT PRIVILEGED BECAUSE EMPLOYER'S POLICY REGARDING COMPUTER USE AND E-MAIL MONITORING STATED THAT EMPLOYEES HAD NO REASONABLE EXPECTATION OF PRIVACY IN E-MAILS SENT OVER THE EMPLOYER'S E-MAIL SERVER). *BUT SEE STENGART V. LOVING CARE AGENCY, INC.*, 201 N.J. 300, 990 A.2D 650 (2010) (DESPITE EMPLOYER'S E-MAIL POLICY STATING THAT COMPANY HAD RIGHT TO REVIEW AND DISCLOSE ALL INFORMATION ON "THE COMPANY'S MEDIA SYSTEMS AND SERVICES" AND THAT E-MAILS WERE "NOT TO BE CONSIDERED PRIVATE OR PERSONAL" TO ANY EMPLOYEES, COMPANY VIOLATED EMPLOYEE'S ATTORNEY-CLIENT PRIVILEGE BY REVIEWING E-MAILS SENT TO EMPLOYEE'S PERSONAL ATTORNEY ON EMPLOYER'S LAPTOP THROUGH EMPLOYEE'S PERSONAL, PASSWORD-PROTECTED E-MAIL ACCOUNT).

12. THIS COMMITTEE'S PRIOR OPINIONS HAVE ADDRESSED THE DISCLOSURE OF CONFIDENTIAL INFORMATION IN METADATA AND THE PERILS OF PRACTICING LAW OVER THE INTERNET. WE HAVE NOTED IN THOSE OPINIONS THAT THE DUTY TO "EXERCISE REASONABLE CARE" TO PREVENT DISCLOSURE OF CONFIDENTIAL INFORMATION "MAY, IN SOME CIRCUMSTANCES, CALL FOR THE LAWYER TO STAY ABREAST OF TECHNOLOGICAL ADVANCES AND THE POTENTIAL RISKS" IN TRANSMITTING INFORMATION ELECTRONICALLY. N.Y. STATE 782 (2004), *CITING* N.Y. STATE 709 (1998) (WHEN CONDUCTING TRADEMARK PRACTICE OVER THE INTERNET, LAWYER HAD DUTY TO "STAY ABREAST OF THIS EVOLVING TECHNOLOGY TO ASSESS ANY CHANGES IN THE LIKELIHOOD OF INTERCEPTION AS WELL AS THE AVAILABILITY OF IMPROVED TECHNOLOGIES THAT MAY REDUCE SUCH RISKS AT REASONABLE COST"); *SEE ALSO* N.Y. STATE 820 (2008) (SAME IN CONTEXT OF USING E-MAIL SERVICE PROVIDER THAT SCANS E-

MAILS TO GENERATE COMPUTER ADVERTISING). THE SAME DUTY TO STAY CURRENT WITH THE TECHNOLOGICAL ADVANCES APPLIES TO A LAWYER'S CONTEMPLATED USE OF AN ONLINE DATA STORAGE SYSTEM.

CONCLUSION

13. A LAWYER MAY USE AN ONLINE DATA STORAGE SYSTEM TO STORE AND BACK UP CLIENT CONFIDENTIAL INFORMATION PROVIDED THAT THE LAWYER TAKES REASONABLE CARE TO ENSURE THAT CONFIDENTIALITY IS MAINTAINED IN A MANNER CONSISTENT WITH THE LAWYER'S OBLIGATIONS UNDER RULE 1.6. A LAWYER USING AN ONLINE STORAGE PROVIDER SHOULD TAKE REASONABLE CARE TO PROTECT CONFIDENTIAL INFORMATION, AND SHOULD EXERCISE REASONABLE CARE TO PREVENT OTHERS WHOSE SERVICES ARE UTILIZED BY THE LAWYER FROM DISCLOSING OR USING CONFIDENTIAL INFORMATION OF A CLIENT. IN ADDITION, THE LAWYER SHOULD STAY ABREAST OF TECHNOLOGICAL ADVANCES TO ENSURE THAT THE STORAGE SYSTEM REMAINS SUFFICIENTLY ADVANCED TO PROTECT THE CLIENT'S INFORMATION, AND THE LAWYER SHOULD MONITOR THE CHANGING LAW OF PRIVILEGE TO ENSURE THAT STORING INFORMATION IN THE "CLOUD" WILL NOT WAIVE OR JEOPARDIZE ANY PRIVILEGE PROTECTING THE INFORMATION.

(75-09)

One Elk Street, Albany , NY 12207
Phone: 518-463-3200 **Secure Fax:** 518.463.5993

NEW YORK STATE BAR ASSOCIATION

Serving the legal profession and the community since 1876

ETHICS OPINION 1019

New York State Bar Association
Committee on Professional Ethics

Opinion 1019 (8/6/2014)

Topic: Confidentiality; Remote Access to Firm's Electronic Files

Digest: A law firm may give its lawyers remote access to client files, so that lawyers may work from home, as long as the firm determines that the particular technology used provides reasonable protection to client confidential information, or, in the absence of such reasonable protection, if the law firm obtains informed consent from the client, after informing the client of the risks.

Rules: 1.0(j), 1.5(a), 1.6, 1.6(a), 1.6(b), 1.6(c), 1.15(d).

QUESTION

1. May a law firm provide its lawyers with remote access to its electronic files, so that they may work from home?

OPINION

2. Our committee has often been asked about the application of New York's ethical rules -- now the Rules of Professional Conduct -- to the use of modern technology. While some of our technology opinions involve the application of the advertising rules to advertising using electronic means, many involve other ethical issues. See, *e.g.:*

N.Y. State 680 (1996). Retaining records by electronic imaging during the period required by DR 9-102(D) [now Rule 1.15(d)].

N.Y. State 709 (1998). Operating a trademark law practice over the internet and using e-mail.

N.Y. State 782 (2004). Use of electronic documents that may contain "metadata".

N.Y. State 820 (2008). Use of an e-mail service provider that conducts computer scans of emails to generate computer advertising.

N.Y. State 833 (2009). Whether a lawyer must respond to unsolicited emails requesting representation.

N.Y. State 842 (2010). Use of a "cloud" data storage system to store and back up client confidential information.

N.Y. State 940 (2012). Storage of confidential information on off-site backup tapes.

N.Y. State 950 (2012). Storage of emails in electronic rather than paper form.

3. Much of our advice in these opinions turns on whether the use of technology would violate the lawyer's duty to preserve the confidential information of the client. Rule 1.6(a) sets forth a simple prohibition against disclosure of such information, i.e. "A lawyer shall not knowingly reveal confidential information, as defined in this Rule . . . unless . . . the client gives informed consent, as defined in Rule 1.0(j)." In addition, Rule 1.6(c) provides that a lawyer must "exercise reasonable care to prevent . . . others whose services are utilized by the lawyer from disclosing or using confidential information of a client" except as provided in Rule 1.6(b).

4. Comment 17 to Rule 1.6 provides some additional guidance that reflects the advent of the information age:

> [17] When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. The duty does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered to determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to use a means of communication or security measures not required by this Rule, or may give informed consent (as in an engagement letter or similar document) to the use of means or measures that would otherwise be prohibited by this Rule.

5. As is clear from Comment 17, the key to whether a lawyer may use any particular technology is whether the lawyer has determined that the technology affords reasonable protection against disclosure and that the lawyer has taken reasonable precautions in the use of the technology.

6. In some of our early opinions, despite language indicating that the inquiring lawyer must make the reasonableness determination, this Committee had reached general conclusions. In N.Y. State 709, we concluded that there is a reasonable expectation that e-mails will be as private as other forms of telecommunication, such as telephone or fax machine, and that a lawyer ordinarily may utilize unencrypted e-mail to transmit confidential information, unless there is a heightened risk of interception. We also

noted, however, that "when the confidential information is of such an extraordinarily sensitive nature that it is reasonable to use only a means of communication that is completely under the lawyer's control, the lawyer must select a more secure means of communication than unencrypted internet e-mail." Moreover, we said the lawyer was obligated to stay abreast of evolving technology to assess changes in the likelihood of interception, as well as the availability of improved technologies that might reduce the risks at a reasonable cost.

7. In N.Y. State 820, we approved the use of an internet service provider that scanned e-mails to assist in providing user-targeted advertising, in part based on the published privacy policies of the provider.

8. Our more recent opinions, however, put the determination of reasonableness squarely on the inquiring lawyer. See, e.g. N.Y. State 842, 940, 950. For example, in N.Y. State 842, involving the use of "cloud" data storage, we were told that the storage system was password protected and that data stored in the system was encrypted. We concluded that the lawyer could use such a system, but only if the lawyer took reasonable care to ensure that the system was secure and that client confidentiality would be maintained. We said that "reasonable care" to protect a client's confidential information against unauthorized disclosure may include consideration of the following steps:

(1) Ensuring that the online data storage provider has an enforceable obligation to preserve confidentiality and security, and that the provider will notify the lawyer if served with process requiring the production of client information;

(2) Investigating the online data storage provider's security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances;

(3) Employing available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored; and/or

(4) Investigating the storage provider's ability to purge and wipe any copies of the data, and to move the data to a different host, if the lawyer becomes dissatisfied with the storage provider or for other reasons changes storage providers.

Moreover, in view of rapid changes in technology and the security of stored data, we suggested that the lawyer should periodically reconfirm that the provider's security measures remained effective in light of advances in technology. We also warned that, if the lawyer learned information suggesting that the security measures used by the online data storage provider were insufficient to adequately protect the confidentiality of client information, or if the lawyer learned of any breaches of confidentiality by the provider, then the lawyer must discontinue use of the service unless the lawyer received assurances that security issues had been sufficiently remediated.

9. Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks. That is particularly true where there is outside access to the internal system by third parties, including law firm employees working at other firm offices, at home or when traveling, or clients who have been given access to the firm's document system. See, e.g. Matthew Goldstein, "Law Firms Are Pressed on Security For

Data," N.Y. Times (Mar. 22, 2014) at B1 (corporate clients are demanding that their law firms take more steps to guard against online intrusions that could compromise sensitive information as global concerns about hacker threats mount; companies are asking law firms to stop putting files on portable thumb drives, emailing them to non-secure iPads or working on computers linked to a shared network in countries like China or Russia where hacking is prevalent); Joe Dysart, "Moving Targets: New Hacker Technology Threatens Lawyers' Mobile Devices," ABA Journal 25 (September 2012); Rachel M. Zahorsky, "Being Insecure: Firms are at Risk Inside and Out," ABA Journal 32 (June 2013); Sharon D. Nelson, John W. Simek & David G. Ries, Locked Down: Information Security for Lawyers (ABA Section of Law Practice Management, 2012).

10. In light of these developments, it is even more important for a law firm to determine that the technology it will use to provide remote access (as well as the devices that firm lawyers will use to effect remote access), provides reasonable assurance that confidential client information will be protected. Because of the fact-specific and evolving nature of both technology and cyber risks, we cannot recommend particular steps that would constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients, including the degree of password protection to ensure that persons who access the system are authorized, the degree of security of the devices that firm lawyers use to gain access, whether encryption is required, and the security measures the firm must use to determine whether there has been any unauthorized access to client confidential information. However, assuming that the law firm determines that its precautions are reasonable, we believe it may provide such remote access. When the law firm is able to make a determination of reasonableness, we do not believe that client consent is necessary.

11. Where a law firm cannot conclude that its precautions would provide reasonable protection to client confidential information, Rule 1.6(a) allows the law firm to request the client's informed consent. See also Comment 17 to Rule 1.6, which provides that a client may give informed consent (as in an engagement letter or similar document) to the use of means that would otherwise be prohibited by the rule. In N.Y. State 842, however, we stated that the obligation to preserve client confidential information extends beyond merely prohibiting an attorney from revealing confidential information without client consent. A lawyer must take reasonable care to affirmatively protect a client's confidential information. Consequently, we believe that before requesting client consent to a technology system used by the law firm, the firm must disclose the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j), i.e. that the client has information adequate to make an informed decision.

CONCLUSION

12. A law firm may use a system that allows its lawyers to access the firm's document system remotely, as long as it takes reasonable steps to ensure that confidentiality of information is maintained. Because of the fact-specific and evolving nature of both technology and cyber risks, this Committee cannot recommend particular steps that constitute reasonable precautions to prevent confidential information from coming into the hands of unintended recipients. If the firm cannot conclude that its security precautions are reasonable, then it may request the informed consent of the client to its security precautions, as long as the firm discloses the risks that the system does not provide reasonable assurance of confidentiality, so that the consent is "informed" within the meaning of Rule 1.0(j).

October 09, 2018

Cybersecurity: Ethical obligations outlined by legal tech experts

Share this:

Data breaches are an everyday event, and legal professionals have a specific obligation to protect themselves and their clients from exposure to these threats. The webinar "Darkest Hour? Shining a Light on Cyber Ethical Obligations," is one in a five-part series sponsored by the ABA Cybersecurity Task Force and supported by "The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals, Second Edition."

The first thing lawyers must know is that it's not usually obvious when a firm has been hacked. "The vast majority of the time, (hackers) are using your stolen credentials, as opposed to breaking through technical walls," said panelist Arlan McMillan, chief security officer at Kirkland & Ellis in Chicago. "Then they act like you in the firm's network, accessing all the files you have access to."

Another common threat comes through malware in an email, also known as a phishing attack, where an individual is asked to click on a link or open an attachment that has been weaponized in such a way that the attacker gains access to your computer. Nation-state attackers target private businesses in 21 percent of breaches to steal data to advance their espionage activities or interests. And firm employees often don't realize they've been hacked for weeks or months, and they usually find out after being contacted by the FBI.

Hackers may insert themselves into an email conversation related to a wire transfer, then redirect the funds to accounts they control. "This is a growing type of attack," McMillan said. "This is real, and this is happening every day," McMillan said. Traditional security measures – build big walls to keep out the bad guys – don't work anymore. Now, firms must leverage good industry standard frameworks, regulatory requirements and tactical responses to guard against common threats.

"This is not an IT issue," McMillan said. "This is a risk management issue about how you protect your data." He recommends five steps to improve a firm's security posture:

1. Aggressively patch your computer systems (laptops, servers, etc.). Microsoft releases patches every month, and program patches are released regularly. "If you're patching, it makes it much harder for hackers to take advantage of your computer systems." On average, an unpatched computer exposed to the internet will be hacked within 90 minutes.

2. Be a regular user, not an administrator. "Administrator" and "user" are designations that define how much authority you have to make changes on a computer system. Logging in as an "admin" exposes the computer to hacking; it's more secure to log in as a "user."

3. Use strong passwords. McMillan recommends using pass phrases instead of passwords.

4. Invest in email message and attachment scanning tools. This will help protect from phishing attacks.

5. Invest in web-filtering tools. This will help you guard against malicious websites.

McMillan also advises designating a chief information security officer (CISO), which will decrease the cost and likelihood of a breach. "Hire somebody that is specialized in this field." Define the role in your firm's leadership and make sure the CISO reports to your general counsel.

Moderator Lucian T. Pera, a partner at Adams and Reese in Memphis, said the ABA Ethics 20/20 Commission proposed updates to the Model Rules involving the use of technology, which were passed in 2017. Most of the changes involve elements of competency (Rule 1.1), and confidentiality (Rule 1.6).

The changes are mostly common sense, but Pera warns that all lawyers run the risk of facing disciplinary measures if they are not familiar with the updates involving a lawyer's duty to make "reasonable efforts" to secure client information, including email encryption. "If you're only going to read one thing as a lawyer on cybersecurity, this is it ... because it lays out a framework for how you should think about cybersecurity and your obligation to make reasonable efforts."

In a nutshell, ABA Formal Opinion 477R offers the following considerations as guidance:

1. Understand the nature of the threat.

2. Understand how client confidential information is transmitted and where it is stored.

3. Understand and use reasonable electronic security measures.

4 Determine how electronic communications about client matters should be protected.

5 Label client confidential information.

6 Train lawyers and nonlawyer assistants in technology and information security.

7 Conduct due diligence on vendors providing communication technology.

Panelist Karen Painter Randall, a partner and chair of the cybersecurity and data privacy practice at Connell Foley in Roseland, N.J., said law firms are targeted because they are rich targets for hackers due to the concentration of sensitive data. "It's not a matter of if, but when," she said.

What do you do when you discover a breach? "If you're not prepared, it can be difficult to respond within a reasonable time period," she said, especially the critical first 72 hours. Once a breach has been detected and verified, activate the data breach response team (representatives from firm leadership, IT, communications and human resources). The team will evaluate the severity of the breach and decide on next steps, including notification of law enforcement and clients.

Panelist Catherine Sanders Reach, director of Law Practice Management & Technology at the Chicago Bar Association, said many firms store information in the cloud. You should assume at least some of your information is stored on the cloud, and is therefore vulnerable, even in a private cloud. Check the terms of service and privacy policies on free services, and you'll discover a surprising lack of privacy. "Generally, you get what you pay for," Reach said.

You should assess the data security standards a cloud-computing vendor must comply with. Is data stored on servers owned by the provider? Where is the data stored, physically? And the backups? Is any data stored outside of the United States? Will the service notify the firm before providing access to government or law enforcement?

For third-party vendors, firms must keep an updated list of vendors they use. They should make sure all contracts are up to date and include terms to protect the firm in the event of a breach. Reach added that access to the firm's data may need to be limited. Employees taking documents home on personal laptops is a security risk.

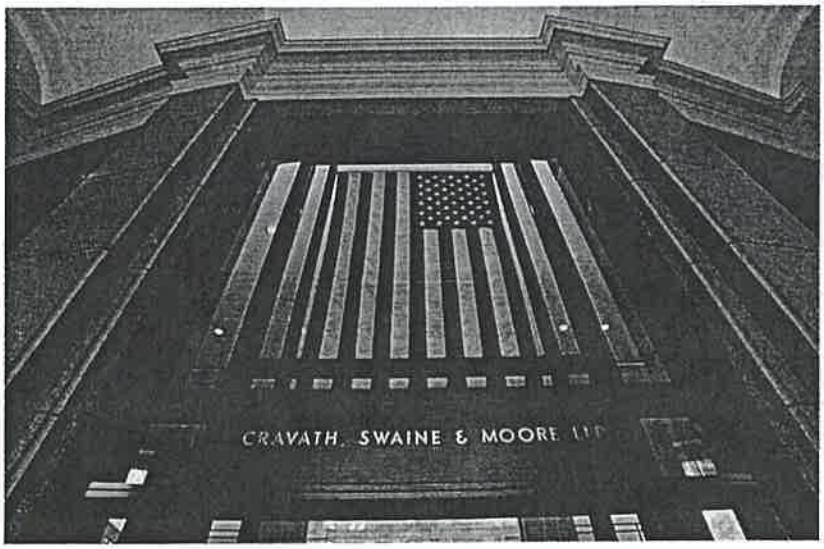
The bottom line is that all firms – big and small – need to be careful with data to protect themselves and clients, McMillan said. Practice good cyber hygiene and make sure your providers and vendors follow suit. "You can never outsource accountability."

https://www.wsj.com/articles/hackers-breach-cravath-swaine-other-big-law-firms-1459293504

MARKETS

Hackers Breach Law Firms, Including Cravath and Weil Gotshal

Investigators explore whether cybercriminals wanted information for insider trading



It isn't clear what information, if any, hackers stole from Cravath Swaine & Moore, Weil Gotshal & Manges and other law firms.
PHOTO: DANIEL ACKER/BLOOMBERG NEWS

By Nicole Hong and Robin Sidel

Updated March 29, 2016 9:14 pm ET

Hackers broke into the computer networks at some of the country's most prestigious law firms, and federal investigators are exploring whether they stole confidential information for the purpose of insider trading, according to people familiar with the matter.

The firms include Cravath Swaine & Moore LLP and Weil Gotshal & Manges LLP, which represent Wall Street banks and Fortune 500 companies in everything from lawsuits to multibillion-dollar merger negotiations.

Other law firms also were breached, the people said, and hackers, in postings on the Internet, are threatening to attack more.

It isn't clear what information the hackers stole, if any, but the focus of the investigation is on whether confidential data were taken for the purpose of insider trading, according to a person familiar with the matter.

The Manhattan U.S. attorney's office and Federal Bureau of Investigation are conducting the probe, which began in the past year and is in its early stages, the people said. Representatives for both declined to comment.

Cravath said the incident, which occurred last summer, involved a "limited breach" of its systems and that the firm is "not aware that any of the information that may have been accessed has been used improperly." The firm said its client confidentiality is sacrosanct and that it is working with law enforcement as well as outside consultants to assess its security.

A spokeswoman for Weil Gotshal declined to comment.

The cyberattacks show what law-enforcement officials have been warning companies about for years. As hacking tools and hackers for hire proliferate in certain corners of the Internet, it has become easier for criminals to breach computer networks as a way to further a range of crimes, from insider trading to identity theft.

In recent years, a number of major retailers have been breached, as was J.P. Morgan Chase & Co., the country's biggest bank by assets. In those cases, hackers stole data such as credit-card numbers and email addresses that they could use to make fraudulent purchases or entice customers into scams.

The attacks on law firms appear to show thieves scouring the digital landscape for more sophisticated types of information. Law firms are attractive targets because they hold trade secrets and other sensitive information about corporate clients, including details about undisclosed mergers and acquisitions that could be stolen for insider trading.

Hackers often steal large amounts of information indiscriminately and then analyze it later to see how it could be useful, making it difficult to determine early on in these types of investigations whether any information was actually used for insider trading, observers said.

The potential vulnerability of law firms is raising concerns among their clients, who are conducting their own assessments of the firms they hire, according to senior lawyers at a number of firms.

A case last year shows that hackers have gone after sensitive material to fuel illegal trading. In that case, brought by federal prosecutors in New Jersey and Brooklyn, N.Y., hackers in Ukraine allegedly breached newswires companies in the U.S. and stole news releases about corporate earnings before they became public. Stock traders then made lucrative bets based on the releases, prosecutors said. At least three of the defendants have pleaded guilty, and the case is pending.

The federal investigation into the law firms is one of several recent cyber-related incidents that have affected the legal industry.

In February, a posting appeared on an underground Russian website called DarkMoney.cc, in which the person offered to sell his phishing services to other would-be cyberthieves and identified specific law firms as potential targets. In phishing attacks, criminals send emails to employees, masked as legitimate messages, in an effort to learn sensitive information like passwords or account information.

Security firm Flashpoint issued alerts to law firms in January and February about the threats and has acquired a copy of a phishing email that is aimed at law firms, according to a person familiar with the alerts. "It has definitely picked up steam," this person said.

The FBI also issued an alert in recent weeks that warned law firms about potential attacks, according to people familiar with the alert. The FBI declined to comment.

Law firms said they have double-checked their cybersecurity defenses in response to the posting and raised more awareness about the issue internally. It isn't clear if the hacker's efforts have resulted in any breaches. A Flashpoint spokeswoman declined to comment on the alerts.

One senior partner at a top law firm said he often receives suspicious emails from people who pretend to be seeking legal representation. "Law firms are being deluged with attempts to crack their systems," he said.

Law firms last year formed an information-sharing group to disseminate information about cyberthreats and other vulnerabilities. It is modeled after a similar organization for financial institutions.

So far, 75 law firms have joined the group, said Bill Nelson, chief executive officer of the Financial Services Information Sharing and Analysis Center, which oversees the legal group and similar entities that focus on other industries, such as retail.

One of the trickiest questions for law firms is when they are required to publicly disclose a data breach. Forty-seven U.S. states have their own breach-notification laws, forcing law firms and other companies to navigate a patchwork of different rules.

Write to Nicole Hong at nicole.hong@wsj.com and Robin Sidel at robin.sidel@wsj.com

Appeared in the March 30, 2016, print edition as 'Hackers Hit Cravath, Weil Gotshal.'

January 28, 2019

TECHREPORT 2018

2018 Cybersecurity

David G. Ries

Share this:

Security breaches are so prevalent that there is a new mantra in cybersecurity today—it's "when, not if" a law firm or other entity will suffer a breach. In an address at a major information security conference in 2012, then-FBI director Robert Mueller put it this way:

> "I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."

Mueller's observation continues to be true today for attorneys and law firms as well as for small businesses through large global companies. There have been numerous reports for over a decade of law firm data breaches in the popular and legal press—print and online. The FBI has reported that law firms are often viewed as "one-stop shops" for attackers (with information on multiple clients) and it has seen hundreds of law firms being increasingly targeted by hackers. Law firm breaches have ranged from simple (like those resulting from a lost or stolen laptop or mobile device) to highly sophisticated (like the deep penetration of a law firm network, with access to everything, for a year or more).

New York Ethics Opinion 1019 warned attorneys in May 2014 about this threat environment:

> "Cyber-security issues have continued to be a major concern for lawyers, as cyber-criminals have begun to target lawyers to access client information, including trade secrets, business plans and personal data. Lawyers can no longer assume that their document systems are of no interest to cyber-crooks."

Several years later, ABA Formal Opinion 477, "Securing Communication of Protected Client Information" (May 11, 2017), observed:

> "At the same time, the term 'cybersecurity' has come into existence to encompass the broad range of issues relating to preserving individual privacy from intrusion by nefarious actors throughout the Internet. Cybersecurity recognizes a ... world where law enforcement discusses hacking and data loss in terms of 'when,' and not 'if.' Law firms are targets for two general reasons: (1) they obtain, store and use highly sensitive information about their clients while at times utilizing safeguards to shield that information that may be inferior to those deployed by the client, and (2) the information in their possession is more likely to be of interest to a hacker and likely less voluminous than that held by the client."

Most recently, ABA Formal Opinion 483, "Lawyers' Obligations After an Electronic Data Breach or Cyberattack" (October 17, 2018) starts with the following observations about current threats:

> "Data breaches and cyber threats involving or targeting lawyers and law firms are a major professional responsibility and liability threat facing the legal profession. As custodians of highly sensitive information, law firms are inviting targets for hackers. In one highly publicized incident, hackers infiltrated the computer networks at some of the country's most well-known law firms, likely looking for confidential information to exploit through insider trading schemes. Indeed, the data security threat is so high that law enforcement officials regular regularly divide business entities into two categories: those that have been hacked and those that will be."

The ABA's *2018 Legal Technology Survey Report* explores security threats and incidents and safeguards that reporting attorneys and their law firms are using to protect against them. As in past years, it shows that many attorneys and law firms are employing some of the safeguards covered in the questions and generally increasing use of the safeguards over time. However, it also shows that many are not using security measures that are viewed as basic by security professionals and are used more frequently in other businesses and professions.

Some attorneys and law firms may not be devoting more attention and resources to security because they mistakenly believe "it won't happen to me." The increasing threats to attorneys and law firms and the reports of security breaches should dispel this mistaken viewpoint. Significantly, 23% of respondents overall reported this year that their firm had experienced a data breach at some time.

Data security is addressed most directly in *2018 Survey,* "Volume I: Technology Basics & Security." It is further addressed in "Volume IV: Marketing and Communications Technology," and "Volume VI: Mobile Lawyers." This *TECHREPORT* reviews responses to the security questions in this year's Survey and discusses them in light of both attorneys' duty to safeguard information and standard information security practices. Each volume includes a Trend Report, which breaks down the information by size of firm and compares it to prior years, followed by sections with more detailed information on survey responses. This gives attorneys and law firms (and clients) information to compare their security posture to law firms of similar size.

Attorneys' Duty to Safeguard Information

The ethics rules require attorneys to take competent and reasonable measures to safeguard information relating to clients (ABA Model Rules 1.1 and 1.6 and Comments). These duties are covered in these rules and comments and in the recent ethics opinions like the ones discussed above. Attorneys also have common law duties to protect client information and often have contractual and regulatory obligations to protect information relating to clients and other personally identifiable information, like health and financial information. These duties present a challenge to attorneys using technology because most are not technologists and often lack training and experience in security. Compliance requires attorneys to understand limitations in their knowledge and obtain sufficient information to protect client information, to get qualified assistance if necessary, or both. These obligations are minimum standards—failure to comply with them may constitute unethical or unlawful conduct. Attorneys should aim for security that goes beyond these minimums as a matter of sound professional practice and client service.

Recognizing the Risk

Information security starts with an inventory and risk assessment to determine what needs to be protected and the threats that it faces. The inventory should include both technology and data. You can't protect it if you don't know that you have it and where it is.

Comment [18] to Model Rule 1.6 includes a risk-based approach to determine reasonable measures that attorneys should employ. The first two factors in the analysis are "the sensitivity of the information" and "the likelihood of disclosure if additional safeguards are not employed." This analysis should include a review of security incidents that an attorney or law firm has experienced and those experienced by others—generally and in the legal profession. The *2018 Survey* includes information about threats in its questions about security breaches.

The next factors in the risk analysis cover available safeguards. Comment [18] to Model Rule 1.6 includes them in the risk analysis for attorneys for determining what is reasonable:

> "...the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use)."

Comment [18] uses a risk-based approach that is now standard in information security. The *2018 Survey* includes information about the available safeguards that various attorneys and firms are using.

The *2018 Survey* reports that about 23% of respondents overall reported that their firms had experienced a security breach at some point. The question is not limited to the past year, it's "ever." A breach broadly includes incidents like a lost/stolen computer or smartphone, hacker, break-in, or website exploit. This compares with 22% last year, 14% in 2016, 15% in 2015, 14% in 2014, and 15% in 2013—an increase of 8% in 2017 after being basically steady from 2013 through 2016.

This year, the reported percentage of firms experiencing a breach generally increased with firm size, ranging from 14% of solos, 24% of firms with 2-9 attorneys, about 24% for firms with 2-9 and 10-49, 42% with 50-99, and about 31% with 100+. As noted above, this is for firms who have experienced a breach *ever*, not just in the past year.

Larger firms have more people, more technology, and more data, so there is a greater exposure surface, but they also should have more resources to protect them. It is difficult to tell the completeness of larger firm's responses on breaches because the percentage of those reporting that they "don't know" about breaches (18% overall) directly goes up with firm size—reaching 57% in firms with 100-499 attorneys and 61% in firms with 500+. This makes sense because attorneys in medium and large firms may not learn about security incidents that don't impact the entire firm, particularly minor incidents and ones at remote offices.

The majority of respondents—60%—reported that their firm had not experienced a breach in the past. Hopefully, this does not include firms that have experienced a security breach and never detected it. Another common saying in security today is that there are two kinds of companies: Those that have been breached and know it, and those that have been breached but don't know it. The same is likely true for law firms.

The most serious consequence of a security breach for a law firm would most likely be unauthorized access to sensitive client data (although the loss of data would also be very serious). The *2018 Survey* shows a very low incidence of this result for firms that experienced a breach—about 6% overall, up from 1% last year. The reports of unauthorized access to sensitive client data by firms that experienced a breach is 11% for solos (up from none last year); 6-8% for firms with 2-9, 10-49, and 50-99; none reported for firms with 100+. While the percentages are low, any exposure of client data can be a major disaster for a law firm and its clients.

The information on breaches with exposure of client data is incomplete because almost 7% overall report that they don't know about the consequences, with "don't know" responses increasing from none for solos to 38% for firms of 500+. The uncertainty is increased by the high percentage of respondents (18%), discussed above, who don't even know whether their firm experienced a data breach.

Unauthorized access to non-client sensitive data is 6% overall, with 8% for solos, 5% for firms with 2-9, 10% for firms with 10-49, 8% for firms with 50-99, 5% for firms of 100-499, and none for firms with 500+.

The other reported consequences of data breaches are significant. Downtime/loss of billable hours was reported by 41% of respondents; consulting fees for repair were reported by 40%; destruction or loss of files by 11%, and replacement of hardware/software reported by 27% (percentages for firms that experienced breaches). Any of these could be very serious, particularly for solos and small firms that may have limited resources to recover. No significant business disruption or loss was reported by 65% overall.

About 9% overall responded that they notified a client or clients of the breach. The percentage reporting notice to clients ranges from 11% for solos, 8% for firms with 2-9, 7% for firms with 10-49, 17% for firms with 50-99, none for firms with 100-499 and 19% for firms with 500+. This is equal to or in excess of the reported incidence of unauthorized access to client data for firms of each size, consistent with the view that ethical and common law obligations require notice to clients.

Overall, 14% of respondents that experienced a breach reported that they gave notice to law enforcement, ranging from 13% for solos, 10% with 2-9 attorneys, 20% of firms with 10-49, 25% of firms with 50-99, 5% of firms with 100-499 attorneys to 25% of firms with 500+.

The *2018 Survey* also inquired whether respondents ever experienced an infection with viruses/spyware/malware. Overall, 40% reported infections, 37% reported none, and 23% reported that they don't know. Reported infections were greatest in firms with 10-49 attorneys (57%) and 2-9 (48%), and lowest in firms with 500+ (20%). Infections can cause serious consequences, including compromise of confidentiality and loss of data. With over one third of respondents reporting infections (down from almost half last year), strong safeguards to protect against them, including up to date security software, using current versions of operating systems and software, promptly applying patches to the operating system and all application software, effective backup, and training of attorneys and staff are clearly warranted.

Security Programs and Policies

At the ABA Annual Meeting in August, 2014, the ABA adopted a resolution on cybersecurity that "encourages all private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations and is tailored to the nature and scope of the organization and the data and systems to be protected." The organizations covered by it include law firms.

A security program should address people, policies and procedures, and technology. All three areas are necessary for an effective program. Security should not be left solely to IT staff and tech consultants. In addition to measures to prevent security incidents and breaches, there has been a growing recognition that security includes the full spectrum of measures to identify and protect information assets and to detect, respond to, and recover from data breaches and security incidents. Security programs should cover all of these functions.

An important initial step in establishing an information security program is defining responsibility for security. The program should designate an individual or individuals responsible for coordinating security—someone must be in charge. It should also define everyone's responsibility for security, from the managing partner or CEO to support staff.

While a dedicated, full-time Chief Information Security Officer is generally only appropriate (and affordable) for larger law firms, every firm should have someone who is responsible for coordinating security. The larger the firm, the more necessary it is to have a full-time security officer or someone who is to dedicate an appropriate part of their time and effort to security. The *2018 Survey* asks who has primary responsibility for security in respondents' firms. As expected, responses vary by size of firm. The respondent has primary responsibility in solo firms (84%), the

respondent or an external consultant/expert in firms of 2-9 attorneys (27% and 33%, respectively); IT staff for firms of 10-49 attorneys (41%) and 50-99 (47%), a chief information officer in firms of 100-499 (56%) and firms of 500+ (62%). A small percentage (2%) report that nobody has primary responsibility for security—a high-risk situation.

The *2018 Survey* asks respondents about a variety of technology-related policies, rather than about an overall comprehensive information security program. Attorneys and law firms should view these kinds of policies as part of a coordinated program rather than individually.

According to the *2018 Survey*, 53% of respondents report that their firms have a policy to manage the retention of information/data held by the firm, 50% report a policy on email use, 44% for internet use, 41% for computer acceptable use, 37% remote access, 38% for social media, 21% personal technology use/BYOD, and 32% for employee privacy. The numbers generally increase with firm size. For example, about 33% of solo respondents report having an information/data retention policy, increasing to 51% in firms with 2-9, 60% with 10-49, 77% with 50-99, and approximately 90% in 100+ attorneys.

Two responses that raise a major security concern are those that report having no policies (29% overall) and those reporting that they don't know about security policies (7%). There is a clear trend by firm size in the responses of having no policies. There are no respondents in firms of 100+ attorneys reporting none. The percentage with none generally decreases by firm size, ranging from 3% of firms with 50-99, 6% with 10-49, 25% in firms with 2-9, to 58% of responding solos. While it is understandable that solos and smaller firms may not appreciate the need for policies, all firms should have policies, appropriately scaled to the size of the firm and the sensitivity of the data.

Incident response is a critical element of an information security program. Overall, 25% report having an incident response plan. The percentage of respondents reporting that they have incident response plans varies with firm size, ranging from 9% for solos and 16% for firms with 2-9 to approximately 70% forms with 100+. As with a comprehensive security program, all attorneys and law firms should have an incident response plan scaled to the size of the firm. For solos and small firms, it may just be a checklist plus who to call for what, but they should have a basic plan.

Security awareness is a key to effective security. There cannot be effective security if users are not trained and do not understand the threats, how to protect against them, and the applicable

security policies. Obviously, they can't understand policies if they don't even know whether their law firm has any policies.

In accordance with the ABA resolution on cybersecurity programs (and generally accepted security practices), all attorneys and law firms should have security programs tailored to the size of the firm and the data and systems to be protected. They should include training and constant security awareness.

Security Assessments and Client Requirements

Clients are increasingly focusing on the information security of law firms representing them and using approaches like required third-party security assessments, security requirements, and questionnaires.

The increased use of security assessments conducted by independent third parties has been a growing security practice for businesses and enterprises generally. Law firms have been slow to adopt this security tool, with only 28% of law firms overall reporting that they had a full assessment, but it increased from 27% last year and 18% in 2017. Affirmative responses generally increase by size of firm.

Third-party assessments are often conducted for law firms only when a client requests it or requires it. Overall, 11% report that a client or prospective client has requested an audit or other review. The percentage of firms reporting a client request gradually goes up by size of firm, from 2% for solos to 39% for firms of 500+.

Overall, 34% of respondents report that they have received a client security requirements document or guidelines. Firms receiving them generally increase by size of firm, from 15% of solos to about 66% with 100+ attorneys. There is a growing recognition in the information security profession of the importance of securing data that business partners and service providers can access, process, and store. This includes law firms. In March of 2017, the Association of Corporate Counsel (ACC) published the *Model Information Protection and Security Controls for Outside Counsel Possessing Company Confidential Information* that provides a list of baseline security measures and controls that legal departments can consider in developing requirements for outside counsel. Attorneys and law firms are likely to continue to face increasing client requirements for security.

Cyber Insurance

As the headlines continue to be filled with reports of data breaches, including law firms, there has been a growing recognition of the need for cyber insurance. Many general liability and malpractice policies do not cover security incidents or data breaches. The percentage of attorneys reporting that they have cyber liability coverage is small but has been increasing—34% overall (up from 27% in 2017, 17% in 2016, and 11% in 2015). It gradually increases from 27% for solos to about 35-45% for midsize firms, then drops to 23% for firms of 500+. In addition to cyber liability insurance, covering liability to third parties, there is also coverage available for first-party losses to the law firm (like lost productivity, data restoration, and technical and legal expenses). A review of the need for cyber insurance coverage should be a part of the risk assessment process for law firms of all sizes.

Security Standards and Frameworks

A growing number of law firms are using information security standards and frameworks, like those published by the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), and the Center for Internet Security (CIS). They provide consensus approaches to a comprehensive information security program. Some firms use them as guidelines for their security programs, while a smaller group of firms seek formal security certification. The *2018 Survey* asks whether respondents' firms have received a security certification. Overall, only 9% report that they have received certification, with a low of 3% for solos and a high of 27% for firms with 500+.

Authentication and Access Control

Authentication and access controls are the first lines of defense. They are the "keys to the kingdom"—controlling access to networks, computers, and mobile devices.

The *2018 Survey* includes a general question about mandatory passwords without specifying the access for which they are required. Overall, 68% of respondents report using mandatory passwords. They are required by 53% of solos, 71% of firms of 2-10 attorneys, and about 80% or higher for larger firms. This question does not ask about other forms of authentication like fingerprints or facial recognition. Some form of strong authentication should be required for access to computers and networks for all attorneys and all law firms.

For laptops, a strong majority of responding attorneys—nearly all—report that they use access controls. Overall, 98% report using passwords, with 99% for solos, 98% for firms of 2-9 attorneys, 94% for firms of 10-49, and firms of 50-500+ at 100%. In addition, 19% overall report using other authentication, which would include fingerprint readers, facial recognition, and other alternatives. While this might suggest that all attorneys use some form of access control (98% + 19%), that is not the case. About 1% report that they use none of the listed laptop security measures. The response of "none" only includes solos and firms 10-49 attorneys. As noted above, larger firms report 100% use of passwords for laptops.

Use of authentication controls on smartphones is similar to those on laptops. Reported use of passwords is 92% overall—generally increasing with firm size from 87% for solos to 100% for firms of 500+. Firms of other sizes range from about 90% to 99%. Use of other authentication is 40% overall, while 5% reporting none of the listed security measures.

For both laptops and smartphones (as well as other mobile and portable devices), all attorneys should be using strong passwords or other strong authentication.

Most, if not all, attorneys need multiple passwords for a number of devices, networks, services, and websites—for both work and personal use. It is recommended that users have a different, strong password for each device, network, service, and website. While password standards are evolving—stressing length over complexity—it is very difficult, or impossible, to remember numerous passwords. Password management tools allow a user to remember a single, strong password for the tool or locker with automatic access to the others. Respondents report that 24% overall use password management tools. 16% report that they don't know. It is unlikely that respondents who don't know are using these tools because a user would have to know that they are using a single password to access others. There is some difference in use by size of firm, ranging from a low of 16% for firms with 50-99 attorneys to a high of 30% for firms with 100-499.

Encryption

Encryption is a strong security measure that protects data in storage (on computers, laptops, smartphones, tablets, and portable devices) and transmitted data (over wired and wireless networks, including email). Security professionals view encryption as a basic safeguard that should be widely deployed. It is increasingly being required by law for personal information, like health and financial information. The recent battle between the FBI and Apple and the current debate about mandated "backdoors" to encryption for law enforcement and national security

show how strong encryption can be for protecting sensitive data. The *2018 Survey* shows that use by attorneys of the covered encryption tools has been growing, but its use is limited.

Full-drive encryption provides strong protection for all of the data on a server, desktop, laptop, or portable device. The data is readable only when it is decrypted through use of the correct password or other access control. Respondents report an overall use of full-drive encryption of only 24% (up from 21% last year and 15% in 2016), ranging from 15% for solos to about 48% for firms of 100+, with percentages increasing by firm size. File encryption protects individual files rather than all the data on a drive or device. Reported use of file encryption is higher than full disk at 46% overall, ranging from 36% for solos to 72% in firms of 500+. This question is general and is not broken down in Volume I of the *2018 Survey* by servers, desktops, laptops, smartphones, etc. As discussed below, all attorneys should use encryption on laptops, smartphones, and mobile devices. While some law firms are starting to encrypt desktops and firm servers, it is not yet a common practice.

Volume VI of the *2018 Survey* has separate questions for laptops and smartphones. For laptops, 25% overall report using file/data encryption and 18% report using hard drive encryption. Both of these numbers are down slightly from last year. File/data protection relies on the user to encrypt individual files or to put sensitive information in an encrypted file or partition on the drive. Full-drive encryption provides broader protection because it protects all data on the drive. Use of full-drive encryption for laptops does not vary directly with firm size—reported use is 18% for solos, 13% for firms with 2-9, 26% for firms with 10-49, 18% of firms with 50-99, 30% of firms with 100-499, and only 15% of firms with 500+ attorneys.

The *2018 Survey* also reported on additional security measures for laptops, like remote data wiping (12% overall) and tracking software (7% overall). These kinds of measures can provide additional security, but should not be a substitute for strong authentication and encryption.

Use of encryption on smartphones appears to be significantly under-reported by attorneys responding to the *2018 Survey*, as in past years. Respondents report an overall use of encryption of smartphones by only 18%. However, 72% overall of attorneys who use smartphones for work report using iPhones and 94% report that they use password protection on their smartphones. On current iPhones, encryption is automatically enabled when a PIN or passcode is set. Google is also moving to automatic encryption with a PIN or swipe pattern for Android devices. It appears that many attorneys are using encryption on their smartphones without knowing it. Encryption can

be that easy! Encryption of laptops may also be under-reported because it can be transparent to the user if it has been enabled or installed by a law firm's IT staff or a technology consultant.

Verizon's *2014 Data Breach Investigation Report* concludes that "encryption is as close to a no-brainer solution as it gets" for lost or stolen devices. Attorneys who do not use encryption on laptops, smartphones, and portable devices should consider the question: Is failure to employ what many consider to be a no-brainer solution taking competent and reasonable measures?

Secure email is another safeguard with limited reported use by responding attorneys. Overall, 29% of respondents reported that they use encryption of email for confidential/privileged communications/documents sent to clients (down from 36% last year). This ranges from 19% for solos, gradually increasing to 70% with firms of 50-99 and 73% for firms of 500+. Firms of 100-499 are an exception, with only 47% reporting use of encryption for email. Another question asks about registered/secure email, which appears to also include encryption. Overall, 18% report using registered/secure email, increasing directly with firm size from 12% for solos to 36% for firms with 500+. If there is no overlap between this response and the use of encryption, the overall percentage using email security would be 47% overall, increasing with firm size to 100% of firms with 500+.

Email encryption has now become easy to use and inexpensive with commercial email services. Google and Yahoo, at least in part driven by the disclosures about NSA interception, announced in 2014 that they would be making encryption available for their email services. In its announcement, Google compared unencrypted email to a postcard and encryption as adding an envelope. This postcard analogy has been used by security professionals for years. Hopefully, the percentages of attorneys reporting that they have added the envelopes, where appropriate, will grow in future survey results.

During the last several years, some state ethics opinions have increasingly expressed the view that encryption of email may sometimes be required to comply with attorneys' duty of confidentiality. On May 11, 2017, the ABA issued Formal Opinion 477, Securing Communication of Protected Client Information. The Opinion revisits attorneys' duty to use encryption and other safeguards to protect email and electronic communications in light of evolving threats, developing technology, and available safeguards. It suggests a fact-based analysis and concludes "the use of un-encrypted routine email generally remains an acceptable method of lawyer-client communication," but "particularly strong protective measures, like encryption, are warranted in some circumstances." It notes that attorneys are required to use special security precautions, like encryption, "when

required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security."

If encrypted email is not available, a strong level of protection can be provided by putting the sensitive information in an encrypted attachment instead of in the text of the email. In current versions of Microsoft Office, Adobe Acrobat, and WinZip, setting a password for the document encrypts it. While password protection of documents is not as strong as encryption of a complete email and attachments because it depends on the strength of the password, it is much more secure than no encryption. If this approach is used, it is important to securely provide the passwords or passphrase to the recipient(s), preferably through a different communication channel like a phone call or text message (and certainly not in the email used to send the document).

Overall, a low percentage of respondents report using password protection for documents. There is not a pattern by firm size, with a low of 12% reported by solos and a high of 35% reported by firms of 100-499.

It has now reached the point where all attorneys should generally understand encryption and have encryption available for use in appropriate circumstances.

Some Basic Security Tools

In addition to authentication and encryption, the *2018 Survey* asks about various security tools that are available to responding attorneys. Most, if not all, of these tools are security basics that should be used by all attorneys and law firms.

The most common tool is the spam filter, used by 87% of respondents. This may be under-reported because most email service providers have at least basic spam filters. Spam filters can be a strong first line of defense against phishing (malicious emails that try to steal information or plant malware). Filters are only part of the defense that weeds out some phishing emails but are an important first step.

Other tools with high reported use include anti-spyware (80%), software-based firewalls (80%), antivirus for desktops/laptops (73%), for email (69%), for networks (66%), and hardware firewalls (57%). Use of intrusion detection and prevention systems is reported by about 33% of respondents overall. There has been a growing trend for a number of years to use security suites that combine

some of these tools like malware protection, spyware protection, software firewalls, and basic intrusion protection in a single tool. Availability of the various security tools is generally stable across firms of all sizes, with increases for some of them with the size of the firm. For all of these security tools, the use by firms should be 100%. There is a generally low incidence of "don't know" responses for these tools, about 7% overall.

Remote Access

Approximately 90% of respondents reported that they remotely access work assets other than email, like applications and files, consistent with today's mobile practice of law. 39% report regular use of remote access, 31% report occasional use, and 19% report "seldom." Reported use generally increases with firm size, reaching 68% for firms of 500+. Respondents report using the following security measures: web-based applications (42%), virtual private networks (VPNs) (37%), remote access software (30%), and other (10%). Security for remote access is critical because it can provide unauthorized access for outsiders (to the communication or network) if it is not properly secured with an encrypted communication connection and strong authentication. There is a growing practice of using multifactor authentication or two-step verification for authentication in remote access. It requires a second method of authentication, in addition to a password, like a set of numbers transmitted to a smartphone or generated by an app. Multiple inexpensive and easy-to-use options are available.

Wireless Networks

Public wireless (WiFi) networks present a high-security risk, particularly if they are open, as in not requiring a password for connection. Without appropriate security measures, others connected to the network—both authorized users and attackers—may be able to intercept or view data and electronic communications transmitted over the network. The *2018 Survey* asks about security measures that attorneys use when accessing public wireless networks. 31% report that they do not use public wireless networks. Overall, 38% report that they use a VPN (a technology that provides an encrypted connection over the internet or other networks), 20% report that they use remote access software, 15% report that they use website-provided SSL/HTTPS encryption, and 0.6% report using other security measures. The remaining 15% are living dangerously, reporting that they use none of the security measures.

Cell carriers' data networks generally provide stronger security than public WiFi, either with access built into a smartphone, tablet, or laptop, or by using a smartphone, tablet, or separate

device as a personal hotspot.

Up-to-date equipment and secure configuration (using encryption) are also important for a law firm and home wireless networks.

Disaster Recovery/Business Continuity

Threats to the availability of data can range from failure of a single piece of equipment to a major disaster like a fire or hurricane. An increasing threat to attorneys and law firms of all sizes is ransomware, generally spread through phishing. It encrypts a user's or network's data and demands ransom (to be paid by Bitcoin) for release of the decryption key. Effective backup, which is isolated from production networks, can provide timely recovery from ransomware.

Overall, 17% of respondents report that their firm had experienced a natural or man-made disaster, like a fire or flood. The highest incidence, about 32%, was in firms of 50-99 and 500+. The lowest reported incidence was for solos at 10%, with the rest were between these numbers. Disasters of this kind can put a firm out of business temporarily or permanently. These positive responses, from 10% to 32% of respondents, and the potentially devastating results demonstrate the importance for law firms of all sizes to be prepared to respond and recover.

Despite this clear need, only 40% overall of responding attorneys report that their firms have a disaster recovery/business continuity plan. Firms with a plan generally increase with the size of the firm, ranging from 22% of solos to over 85% of firms with 50-99 and 500+ attorneys. As with comprehensive security programs, all law firms should have a disaster recovery/business continuity plan, appropriately scaled to its size.

In the equipment failure area, 34% of respondents reported that their firm experienced a hard drive failure, while 44% reported that they did not. The remainder reported that they do not know, with the "don't knows" increasing by firm size. In firms of 500+, 73% responded that they don't know. In firms of 100-499, it was 61%. It is very likely that most large firms have suffered multiple hard drive failures, just not known by the individual responding attorneys. Even limiting the analysis to known hard drive failures, they have impacted about one-third of respondents. That's a high risk, particularly considering the potential consequences of lost data, and all attorneys and law firms should implement backup and recovery measures.

Backup of data is critical for business continuity, particularly with the current epidemic of ransomware. Fortunately, most firms report that they employ some form of backup. Only 1.5% report that they don't back up their computer files. 21% of respondents report that they don't know about backup. The most frequently reported form of backup is external hard drives (38%), followed by offsite backup (30%), online backup (30%), network attached storage (15%), USB (9%), tape (7%), RAID (7%), CDs (4%), and DVDs (4%).

The *2018 Survey* responses show that 49% of respondents back up once a day, 22% more than once a day, 11% weekly, 5% monthly, and 2% quarterly. 8% report that they don't know, with unknowns increasing with firm size. Attorneys and firms that don't back up on a daily basis, or more frequently, should reevaluate the risk in light of ransomware, hardware failures, disasters, and other incidents reported in the *2018 Survey*.

Conclusion

The *2018 Survey* provides a good overview, with supporting details, of what attorneys and law firms are doing to protect confidential information. Like the last several years, the data generally shows increasing attention to security and increasing use of the covered safeguards but also demonstrates that there is still a lot of room for improvement. Attorneys and law firms who are behind the reporting attorneys and firms on safeguards should evaluate their security posture to determine whether they need to do more to provide, at minimum, competent and reasonable safeguards—and hopefully more. Those who are in the majority on safeguards, or ahead of the curve, still need to review and update their security as new technology, threats, and available safeguards evolve over time. Effective security is an ongoing process, not just a "set it and forget it" effort. All attorneys and law firms should have appropriate comprehensive, risk-based security programs that include appropriate safeguards, training, periodic review and updating, and constant security awareness.

Authors

ENTITY:

LAW PRACTICE DIVISION, LEGAL TECHNOLOGY RESOURCE CENTER

TOPIC:

CYBERSECURITY, TECHNOLOGY

GEDmatch.Com Terms of Service and Privacy Policy

Revised December 9, 2019

As of December 9, 2019, GEDmatch is operated by Verogen, Inc. ("Verogen") following the acquisition by Verogen of the GEDmatch website.

Verogen respects your privacy and recognizes the importance of your personal information. We are committed to protecting your information through our compliance with this Privacy Policy.

This Privacy Policy describes our practices in connection with information we may collect through your use of our website (our 'Site'). By using our Site, you consent to our collection and use of the information described in this Privacy Policy.

GEDmatch Collection and Use of Information

When you register on GEDmatch, we collect your name, an optional alias, and email address to process your registration. Once you are registered, you can provide other personal information such as your sex, Y-DNA or mtDNA haplogroup, genetic sequence/information, Genealogy data, and/or Tier1 payment information. GEDmatch will only collect your personal information if you provide it to us voluntarily. If you are located outside the United States, you consent to the storage, processing, and transfer of your personal information outside your country.

In addition, we automatically collect certain information regarding visitors to our Site, including IP address, information about your equipment, browsing actions, and usage patterns. The information we collect automatically is statistical data and does not include personal information. We use this information solely for internal purposes, such as to improve our Site.

Our Site may use third party tools to help us understand, in aggregate, the age, gender and interests of Site visitors. These tools do not reveal to GEDmatch your name or other identifying information. GEDmatch does not combine the information collected through use of these tools with personally identifiable information. The information received from these tools is used only to improve our Site and the type of information displayed to Site visitors so we can better serve those interested in GEDmatch.

GEDmatch offers you opportunities to engage in forums that are designed to be visible to other users, including comments and postings. You should be aware that any personally identifiable information you choose to submit via these forums can be read, collected, and used by other participants and could be used to send you unsolicited messages. We are not responsible for the personally identifiable information you choose to submit when you engage in such activities.

We may disclose your Raw Data, personal information, and/or Genealogy Data if it is necessary to comply with a legal obligation such as a subpoena or warrant. We will attempt to alert you to this disclosure of your Raw Data, personal information, and/or Genealogy Data, unless notification is prohibited under law.

GEDmatch's products and services are not intended for children under the age of 13. GEDmatch does not knowingly collect any information from children. If we learn that we have collected or received personal information from a child under 13 without verification of parental consent, we will delete that information.

GEDmatch purpose
GEDmatch exists to provide DNA and genealogy tools for comparison and research purposes. It is supported entirely by users, volunteers, and researchers. DNA and Genealogical research, by its very nature, requires the sharing of information. Because of that, users participating in this Site agree that their information will be shared with other users.

Raw DNA Data Provided to GEDmatch
When you upload Raw Data to GEDmatch, you agree that the Raw Data is one of the following:

- Your DNA;
- DNA of a person for whom you are a legal guardian;
- DNA of a person who has granted you specific authorization to upload their DNA to GEDmatch;
- DNA of a person known by you to be deceased;
- DNA obtained and authorized by law enforcement to identify a perpetrator of a violent crime against another individual, where 'violent crime' is defined as murder, nonnegligent manslaughter, aggravated rape, robbery, or aggravated assault ;
- DNA obtained and authorized by law enforcement to identify remains of a deceased individual;
- An artificial DNA kit (if and only if: (1) it is intended for research purposes; and (2) it is not used to identify anyone in the GEDmatch database); or
- DNA obtained from an artifact (if and only if: (1) you have a reasonable belief that the Raw Data is DNA from a previous owner or user of the artifact rather than from a living individual; and (2) that previous owner or user of the artifact is known to you to be deceased).

By registering for GEDmatch and using the Site, you agree that you will not upload Raw Data that does not satisfy one of these categories. If you have previously uploaded Raw Data that does not satisfy one of these categories, you hereby agree that you will remove it immediately.

GEDmatch will not be responsible for any Raw Data provided to GEDmatch in violation of this Policy. Violators of this Policy will have their Raw Data or other personal information deleted without warning, their access will be blocked, and/or other remedial steps may be taken, including any legal action allowed under law.

Privacy
Although you may provide a real name for registration and data upload, you have the option of providing an alias for either login or data. If an alias has been provided, it will be displayed in place of the real name along with results. If your DNA is linked to your Genealogy Data, and only one or the other uses an alias, it may be possible for users to see the real name in the linked data.

In today's world, there are real dangers of identity theft, credit fraud, etc. We try to strike a balance between these conflicting realities and the need to share information with other users. In the end, if you require absolute privacy and security, you agree that you will not provide your personal information, Raw Data, or Genealogy Data to GEDmatch. If you do not agree and you have already provided your personal information, Raw Data, or Genealogy Data, you agree to delete it immediately.

Security

Although GEDmatch has endeavored to create a secure and reliable Site for you, the confidentiality of any communication, material, or personal information provided to GEDmatch via the Site or email cannot be guaranteed.

The original Raw DNA and GEDCOM data you provide to GEDmatch is not kept in its original form. It is converted to a form that makes it more efficient for the software to perform searches and comparisons. The Genealogical Data is loaded into a relational database that might still be recognizable as text. The Raw DNA is converted to a compressed binary format in a process we call 'tokenization.' Although the Raw DNA is not encrypted in the usual sense of the word, it would be very difficult for a human to read it. Original uploaded files are deleted from the Site servers soon after they are processed and archived.

We encrypt your login password before putting it in our database. We cannot tell what your password is. However, there have been cases in the news of encrypted data being hacked and decoded. Be aware that may be a possibility on this or any other Site. We take measures to ensure that only registered users have access to your results, but those measures have not been and never will be perfect. Direct access to your data is available to GEDmatch personnel, including volunteers, on a need to know basis.

Information such as Raw Data, Genealogy Data, and profile information may be stored as an archive copy as part of a backup or recovery plan. When a registered GEDmatch user deletes or requests deletion of Raw Data, Genealogy Data, and/or profile information, copies of that information stored in an archive copy will be deleted upon storage of an updated archive copy, no later than 30 days after the user request.

Research
We may use your data in our own research, to develop or improve applications.

Email addresses
Everybody who registers with the Site must provide a valid email address for the principal contact. It provides log-in verification and allows GEDmatch to contact them if necessary. It also provides a mechanism to verify your identity if you want to contact GEDmatch. You agree to keep your log-in information secure, and to keep your email address up to date.

Your email address and name (or alias, if provided) will be displayed along with any matches to your Raw Data or Genealogy Data. Some users obtain an email address separate from their primary email for this purpose.

You understand that any registered GEDmatch user using the tools available on the Site may gain access to the email address you provide.

Tier1 Payment Information You may voluntarily obtain access to Tier1 tools on the Site for the recited amount (subject to change). You may provide a one-time payment of any monthly amount, or you may use a 'Monthly Auto Renewal' to establish a recurring amount. Instructions for cancelling a recurring payment are available in the GEDmatch Wiki. Payments can be made via PayPal, and GEDmatch is not responsible for any information provided to GEDmatch by PayPal. Payments may also be provided by personal check to Verogen, Inc., Attn: Tom Mohr, 11111 Flintkote Avenue, San Diego, CA 92121. You understand that your personal account information will be made available to Verogen when paying by personal check.

GEDCOMs
GEDCOMs (family trees) or other genealogy ('Genealogy Data') provided to GEDmatch remain the property of the person who uploaded it. When you upload your Genealogy Data, you will be provided a unique ID number for that GEDCOM. If you want your Genealogy Data removed from the Site, you may do so yourself by clicking on the 'Manage your resources' link on your home page. If you need assistance deleting a Genealogy Data, contact the Site administrator at gedmatch@verogen.com.

Genealogy research requires the exchange of information. For that reason, all Genealogy Data provided to GEDmatch can be viewed, searched, and compared by any GEDmatch user.

Unless you have permission from living individuals in your Genealogy Data, you agree to privatize living individuals in your Genealogy Data prior to providing it to GEDmatch. This usually involves changing the names of living individuals to 'LIVING' or something similar.

We take steps to prevent your Genealogy Data from being available to the casual web surfer or to the search engines (e.g. Google). However, we cannot guarantee that your information will never be accessed by individuals other than GEDmatch users. If you require absolute security, you agree that you will not upload your Genealogy Data to GEDmatch. If you have already uploaded it, you agree to delete it immediately.

You will be given the opportunity to link your Genealogy Data with your DNA data. This is a powerful tool and we encourage people to use it. It also provides a means of access to your Genealogy Data to people who may have no Genealogy Data of their own at GEDmatch. It will also enable identification of individuals within the provided Genealogy Data, even if the individuals are not identified in the Genealogy Data.

DNA Data
Raw DNA data uploaded to GEDmatch.Com ('Raw Data') remains the property of the person who uploaded it. When you upload a file, a kit number will be assigned at the end of the upload process. This number is unique to the individual DNA upload, and will be used on the pages of this Site to identify your data, including being provided to anyone that shares DNA with the Raw Data. If you wish to contact the Site administrator regarding your data, you must provide the kit number associated with your data. A link or other means is provided within your GEDmatch account to remove your Raw Data from the Site. Alternatively, you can request deletion of your personal information at any time by contacting us at gedmatch@verogen.com. It is possible that an old kit number may be reassigned to another user's uploaded data in the future if you delete your Raw Data.

No means are provided on the Site to make Raw DNA or other DNA data available for download.

There are 4 classes of DNA data on this Site: 'Private', 'Research', 'Public + opt-in' and 'Public + opt-out'. You may be asked to select which category you want to be in when you upload your DNA data. If you ever want to change the category, use the pencil icon link next to the kit number on your home page.
'Private' DNA data is not available for comparisons with other people. It may be usable in some utilities that do not depend on comparisons with other DNA.
'Public + opt-in' DNA data is available for comparison to any Raw Data in the GEDmatch database using the various tools provided for that purpose.
'Public + opt-out' DNA data is available for comparison to any Raw Data in the GEDmatch database,

except DNA kits identified as being uploaded for Law Enforcement purposes.
Comparison results, including your kit number, name (or alias), and email will be displayed for 'Public' kits that share DNA with the kit being used to make the comparison, except that kits identified as being uploaded for Law Enforcement purposes will only be matched with kits that have 'opted-in'. **'Research'** DNA data is available for one-to-one comparison to other Public or Research DNA. It is not shown in other people's 'one-to-many' results lists. The Raw Data that you uploaded is not made available.
By default, your Raw Data is not available to any user of the Site - not even you. However, you understand that anyone with the kit number for Raw Data can perform many or all of the same GEDmatch functions with that Raw Data that the provider of that Raw Data can perform.

There may be options where you may join a 'sharing pool' which has the potential for disclosing additional information about you or your data. If you choose to join a sharing pool, you should carefully read the conditions and disclaimers associated with that sharing pool. By joining the sharing pool, you are agreeing to abide by those conditions and disclaimers.

Use of Results
The nature of genealogy research requires the exchange of information. That use must also be tempered by respect for the rights and privacy of other individuals. Anybody found to be using this Site in ways not consistent with this principle of human decency will be subject to an immediate ban with all their data removed. Examples include, but are not specifically limited to, spam mailing lists or publishing other people's results or personal information without their permission. This principle also applies to the related or non-related persons included in Genealogy Data or other data uploaded to this Site. Determination of any violation of this principle will be at the sole discretion of GEDmatch administrators.

While the results presented on this Site are intended solely for genealogical research, we are unable to guarantee that users will not find other uses, including both current and new genealogical and non-genealogical uses. For example, some of these possible uses of Raw Data, personal information, and/or Genealogy Data by any registered user of GEDmatch include but are not limited to:

- Discovery of identity, even if there is an alias, unidentifiable email address, and other obscuring information;
- Finding genetic matches (individuals that share DNA);
- Paternity and maternity testing;
- Discovery of unknown or unidentified children, parents, or siblings;
- Discovery of other genetic and genealogical relatives, including both known and unknown or unexpected genetic and genealogical relatives;
- Discovery of ethnic background;
- Discovery of a genetic relationship between parents;
- Discovery of biological sex;
- Discovery of medical information or physical traits;
- Obtaining an email address; and/or
- Familial searching by third parties such as law enforcement agencies to identify the perpetrator of a crime, or to identify remains.

You understand that future genealogical and non-genealogical uses may be developed, including uses that GEDmatch cannot predict or foresee. If you find any of these current or future uses unacceptable, do not provide Raw Data to GEDmatch, and remove any of your Raw Data already provided to this Site. It is our policy to never provide your Genealogy Data, Raw DNA, personal information, or email address to third parties, except as noted herein. You have the right to access the personal information that GEDmatch has collected about you. You may do the following at any time by contacting us at gedmatch@verogen.com:

- Opt out of any future contacts from us;
- See what information we have about you, if any;
- Change, correct, or have us delete any information we have about you (including personal information, Raw Data, and Genealogy Data); and
- Express any concern you have about our use of your information.

Accuracy of Results

The analysis and comparison results presented on this Site are provided 'as is' and no representations are made regarding their accuracy or usability. Changes in software and analysis tools may be made from time to time that could change results from those previously provided. We do not make any promises about: (a) the functionality of the Site or the Site tools; or (b) the quality, accuracy, reliability, or availability of the Site, including about any personal information, Raw Data, or Genealogical Data provided to the Site. Any reliance you place on information found at the Site is strictly at your own risk. We disclaim all liability and responsibility arising from any reliance placed on such information by you and any other visitor to the Site, and by anyone who may be informed of any of its contents. The operators of this Site are not responsible for the consequences of using the information provided on this Site.

Termination of Service

Anybody wishing to have their provided Raw Data or Genealogy Data removed from the GEDmatch database may do so using the removal/deletion link or other means provided within your GEDmatch account. Alternatively, you can request deletion of your personal information at any time by contacting us at gedmatch@verogen.com.

GEDmatch administrators reserve the right to remove any Raw Data, Genealogy Data, or personal information from the database, for any reason, at any time, either with or without notice. Any or all services at GEDmatch.Com may be terminated at any time, without notice, for any reason, at the sole discretion of the GEDmatch administrators.

Cookies

Cookies may be used by this Site to enable certain privacy and log-in capabilities. A cookie is a small file placed on your computer. You have the ability to delete cookie files from your computer at any time or avoid cookies by configuring your browser to reject them or to notify you when a cookie is being placed on your computer.

This Site may contain links to advertising placed by third party sites. Advertising by third party sites may be placing and reading cookies on your browser, or using web beacons to collect information, in the course of ads being served on this Site. We have no control over how third party sites may utilize cookies. If you feel that a third party site is engaging in unethical or illegal use of this capability, please notify us so that we may take appropriate action to remove that link.

Loss of data
GEDmatch operators will not be held responsible for the loss of Raw Data, whether as a result of mechanical failure, software malfunction, human error, or any other means.

Future
We cannot predict what the future holds for DNA or genealogy research. We cannot predict what the future will be for GEDmatch. It is possible that, in the future, GEDmatch will merge with, or operations will be transferred to other individuals or entities. If that happens, the operating personnel at GEDmatch will change. GEDmatch reserves the right to provide access to your data (including Raw Data, Genealogy Data, profile information, and other personal information) to those other individuals or entities, which may include people not currently involved in GEDmatch operations. This Policy will continue to apply to the Site until you receive notification of changes to the Policy. If this possibility is not acceptable to you, you agree that you will not provide your personal information, Raw Data, or Genealogy Data to GEDmatch. If you have already provided personal information, Raw Data, or Genealogy Data, you agree to remove it from GEDmatch immediately.

Limitation of Liability
GEDmatch shall have no liability to you under this Policy, it being acknowledged and agreed that the Site is provided solely for your convenience. If the foregoing limitation of liability is found to be unenforceable, GEDmatch's liability to you for any cause of action arising from the Site or under this Policy will be limited to any amount paid by you to GEDmatch for the Site during the twelve (12) months preceding such cause of action. Notwithstanding anything to the contrary contained herein, this Policy shall not limit or exclude either party's liability for gross negligence or intentional misconduct of a party or its agents or employees, or for death or personal injury. The parties agree that the limitations on and exclusions of liability in this Policy were freely negotiated and are an integral part of the bargain, in that the Site would not have been available for the same price and under the same terms and conditions had such limitations on and exclusions of liability not been included in this Policy. Some states or jurisdictions do not allow the exclusion of certain warranties, so some of the above limitations may not apply to you. Further, some jurisdictions prohibit the exclusion or limitation of liability for consequential or incidental damages, so the above limitations may not apply to you.

Indemnification
You agree to indemnify, defend, and hold GEDmatch and any of their affiliates, any of their successors and assigns, and any of their respective officers, directors, employees, volunteers, contractors, consultants, agents, representatives, licensors, advertisers, suppliers, and service providers, harmless from any liability, loss, claim, and expense, including reasonable attorneys' fees, related to your violation of this Policy or use or misuse of the Site. We reserve the right, at our own expense, to assume the exclusive defense and control of any matter otherwise subject to indemnification by you, in which event you will cooperate with us in asserting any available defenses.

Updates to This Policy
We may update the GEDmatch.Com Terms of Service and Privacy Policy at any time. We will inform you of updates by posting an announcement on the Site. You agree to review the updated terms and policy, and by continuing to use the Site after we have posted a notice on the Site about the update, you accept the changes to the GEDmatch.Com Terms of Service and Privacy Policy.

Contact us:

OCTOBER 9, 2019

eff.org

Victory! California Governor Signs A.B. 1215

California's Governor Gavin Newsom has officially signed a bill that puts a moratorium on law enforcement's use of face recognition for three years.

Under Assemblymember Phil Ting's bill, A.B. 1215, police departments and law enforcement agencies across the state of California will have until January 1, 2020 to end any existing use of face recognition on body-worn cameras. Three years without police use of this invasive technology means three years without a particularly pernicious and harmful technology on the streets and has the potential to facilitate better relationships between police officers and the communities they serve. As EFF's Associate Director of Community Organizing Nathan Sheard told the California Assembly, using face recognition technology "in connection with police body cameras would force Californians to decide between actively avoiding interaction and cooperation with law enforcement, or having their images collected, analyzed, and stored as perpetual candidates for suspicion."

This moratorium brings to the entire state the privacy that some cities in California have already won. In May 2019, San Francisco became the first city in the country to ban police use of Face recognition technology and was followed in June by Oakland.

Because A.B. 1215 will end on January 1, 2023, we are encouraging communities across the state to advocate for face recognition bans in your own cities and towns. Take this opportunity to advocate for the end of the harmful technology in your own neighborhoods.

STATE OF NEW YORK

5642

2019-2020 Regular Sessions

IN SENATE

May 9, 2019

Introduced by Sens. THOMAS, CARLUCCI, MYRIE -- read twice and ordered printed, and when printed to be committed to the Committee on Consumer Protection

AN ACT to amend the general business law, in relation to the management and oversight of personal data

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

1 Section 1. Short title. This act may be known and cited as the "New
2 York privacy act".
3 § 2. The general business law is amended by adding a new article 42 to
4 read as follows:
5 **ARTICLE 42**
6 NEW YORK PRIVACY ACT
7 Section 1100. Definitions.
8 1101. Jurisdictional scope.
9 1102. Data fiduciary.
10 1103. Consumer rights.
11 1104. Transparency.
12 1105. Responsibility according to role.
13 1106. De-identified data.
14 1107. Exemptions.
15 1108. Liability.
16 1109. Enforcement.
17 1110. Preemption.
18 § 1100. Definitions. The definitions in this article apply unless the
19 context clearly requires otherwise:
20 1. "Affiliate" means a legal entity that controls, is controlled by,
21 or is under common control with, another legal entity, where the entity
22 holds itself out as affiliated or under common ownership such that a
23 consumer acting reasonably under the circumstances would anticipate
24 their personal data being provided to an affiliate.

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD10868-05-9

2. "Consent" means a clear affirmative act establishing a freely given, specific, informed, and unambiguous indication of a consumer's agreement to the processing of personal data relating to the consumer, such as by a written statement or other clear affirmative action.

3. "Consumer" means a natural person who is a New York resident. It does not include an employee or contractor of a business acting in their role as an employee or contractor.

4. "Controller" means the natural or legal person who, alone or jointly with others, determines the purposes and means of the processing of personal data.

5. "Data broker" means a business, or unit or units of a business, separately or together, that earns its primary revenue from supplying data or inferences about people gathered mainly from sources other than the data sources themselves.

6. "De-identified data" means:

(a) data that cannot be linked to a known natural person without additional information not available to the controller; or

(b) data (i) that has been modified to a degree that the risk of re-identification is small as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data, (ii) that is subject to a public commitment by the controller not to attempt to re-identify the data, and (iii) to which one or more enforceable controls to prevent re-identification has been applied. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

7. "Developer" means a person who creates or modifies the set of instructions or programs instructing a computer or device to perform tasks.

8. "Identified or identifiable natural person" means a person who can be identified, directly or indirectly, in particular by reference to specific information including, but not limited to, a name, an identification number, specific geolocation data, or an online identifier.

9. "Minor" means any person under eighteen years of age.

10. "Personal data" means information relating to an identified or identifiable natural person.

(a) "Personal data" includes:

(i) an identifier such as a real name, alias, signature, date of birth, gender identity, sexual orientation, marital status, physical characteristic or description, postal address, telephone number, unique personal identifier, military identification number, online identifier, Internet Protocol address, email address, account name, mother's maiden name, social security number, driver's license number, passport number, or other similar identifier;

(ii) information such as employment, employment history, bank account number, credit card number, debit card number, insurance policy number, or any other financial information, medical information, mental health information, or health insurance information;

(iii) commercial information, including a record of personal property, income, assets, leases, rentals, products or services purchased, obtained, or considered, or other purchasing or consuming history;

(iv) biometric information, including a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry;

(v) internet or other electronic network activity information, including browsing history, search history, content, including text, photographs, audio or video recordings, or other user generated-content,

1 non-public communications, and information regarding an individual's
2 interaction with an internet website, mobile application, or advertise-
3 ment;
4 (vi) historical or real-time geolocation data;
5 (vii) audio, electronic, visual, thermal, olfactory, or similar infor-
6 mation;
7 (viii) education records, as defined in section thirty-three hundred
8 two of the education law;
9 (ix) political information or information on criminal convictions or
10 arrests;
11 (x) any required security code, access code, password, or username
12 necessary to permit access to the account of an individual;
13 (xi) characteristics of protected classes under the human rights law,
14 including race, color, national origin, religion, sex, age, or disabili-
15 ty; or
16 (xii) an inference drawn from any of the information described in this
17 paragraph to create a profile about an individual reflecting the indi-
18 vidual's preferences, characteristics, psychological trends, prefer-
19 ences, predispositions, behavior, attitudes, intelligence, abilities, or
20 aptitudes.
21 (b) The term personal data does not include publicly available infor-
22 mation. "Publicly available information":
23 (i) means information that is lawfully made available from federal,
24 state, or local government records; and
25 (ii) does not include biometric information collected by a covered
26 entity about an individual without the individual's knowledge, or infor-
27 mation used for a purpose that is not compatible with the purpose for
28 which the information is maintained and made available in government
29 records.
30 (c) Personal data does not include de-identified data.
31 11. "Process" or "processing" means any operation or set of operations
32 that is performed on personal data or on sets of personal data, whether
33 or not by automated means, such as collection, recording, organization,
34 structuring, storage, adaptation or alteration, retrieval, consultation,
35 use, disclosure by transmission, dissemination or otherwise making
36 available, alignment or combination, restriction, deletion, or
37 destruction.
38 12. "Processor" means a natural or legal person who processes personal
39 data on behalf of the controller.
40 13. "Profiling" means any form of automated processing of personal
41 data consisting of the use of personal data to evaluate certain personal
42 aspects relating to a natural person, in particular to analyze or
43 predict aspects concerning that natural person's economic situation,
44 health, personal preferences, interests, reliability, behavior,
45 location, or movements.
46 14. "Restriction of processing" means the marking of stored personal
47 data with the aim of limiting the processing of such personal data in
48 the future.
49 15.(a) "Sale", "sell" or "sold" means the exchange of personal data
50 for consideration by the controller to a third party.
51 (b) "Sale" does not include the following: (i) the disclosure of
52 personal data to a processor who processes the personal data on behalf
53 of the controller; (ii) the disclosure of personal data to a third party
54 with whom the consumer has a direct relationship for purposes of provid-
55 ing a product or service requested by the consumer or otherwise in a
56 manner that is consistent with a consumer's reasonable expectations

1 considering the context in which the consumer provided the personal data
2 to the controller; (iii) the disclosure or transfer of personal data to
3 an affiliate of the controller; or (iv) the disclosure or transfer of
4 personal data to a third party as an asset that is part of a merger,
5 acquisition, bankruptcy, or other transaction in which the third party
6 assumes control of all or part of the controller's assets, if consumers
7 are notified of the transfer of their data and of their rights under
8 this article and affirmatively consent to the disclosure and transfer of
9 data.
10 16. "Targeted advertising" means displaying advertisements to a
11 consumer where the advertisement is selected based on personal data
12 obtained or inferred over time from a consumer's activities across web
13 sites, applications or online services. It does not include advertising
14 to a consumer based upon the consumer's current visit to a web site,
15 application, or online service, or in response to the consumer's request
16 for information or feedback.
17 17. "Opt-in" means affirmative, express consent of an individual for a
18 covered entity to use, disclose, or permit access to the individual's
19 personal data after the individual has received explicit notification of
20 the request of the covered entity with respect to that data.
21 § 1101. Jurisdictional scope. 1. This article applies to legal enti-
22 ties that conduct business in New York state or produce products or
23 services that are intentionally targeted to residents of New York state.
24 2. This article does not apply to:
25 (a) state and local governments;
26 (b) personal data sets to the extent that they are regulated by the
27 federal health insurance portability and accountability act of 1996, the
28 federal health information technology for economic and clinical health
29 act, or the Gramm-Leach-Bliley act of 1999; or
30 (c) data sets maintained for employment records purposes.
31 § 1102. Data fiduciary. 1. Personal data of consumers shall not be
32 used, processed or transferred to a third party, unless the consumer
33 provides express and documented consent. Every legal entity, or any
34 affiliate of such entity, and every controller and data broker, which
35 collects, sells or licenses personal information of consumers, shall
36 exercise the duty of care, loyalty and confidentiality expected of a
37 fiduciary with respect to securing the personal data of a consumer
38 against a privacy risk; and shall act in the best interests of the
39 consumer, without regard to the interests of the entity, controller or
40 data broker, in a manner expected by a reasonable consumer under the
41 circumstances.
42 (a) Every legal entity, or affiliate of such entity, and every
43 controller and data broker to which this article applies shall:
44 (i) reasonably secure personal data from unauthorized access; and
45 (ii) promptly inform a consumer of any breach of the duty described in
46 this paragraph with respect to personal data of such consumer.
47 (b) A legal entity, an affiliate of such entity, controller or data
48 broker may not use personal data, or data derived from personal data, in
49 any way that:
50 (i) will benefit the online service provider to the detriment of an
51 end user; and
52 (ii) (A) will result in reasonably foreseeable and material physical
53 or financial harm to a consumer; or
54 (B) would be unexpected and highly offensive to a reasonable consumer.
55 (c) A legal entity, or affiliate of such entity, controller or data
56 broker:

(i) may not disclose or sell personal data to, or share personal data with, any other person except as consistent with the duties of care and loyalty under paragraphs (a) and (b) of this subdivision;

(ii) may not disclose or sell personal data to, or share personal data with, any other person unless that person enters into a contract that imposes the same duties of care, loyalty, and confidentially toward the consumer as are imposed under this section; and

(iii) shall take reasonable steps to ensure that the practices of any person to whom the entity, or affiliate of such entity, controller or data broker discloses or sells, or with whom the entity, or affiliate of such entity, controller or data broker shares, Personal data fulfills the duties of care, loyalty, and confidentiality assumed by the person under the contract described in subparagraph (ii) of this paragraph, including by auditing, on a regular basis, the data security and data information practices of any such entity, or affiliate of such entity, controller or data broker.

2. For the purposes of this section the term "privacy risk" means potential adverse consequences to consumers and society arising from the processing of personal data, including, but not limited to:

(a) direct or indirect financial loss or economic harm;

(b) physical harm;

(c) psychological harm, including anxiety, embarrassment, fear, and other demonstrable mental trauma;

(d) significant inconvenience or expenditure of time;

(e) adverse outcomes or decisions with respect to an individual's eligibility for rights, benefits or privileges in employment (including, but not limited to, hiring, firing, promotion, demotion, compensation), credit and insurance (including, but not limited to, denial of an application or obtaining less favorable terms), housing, education, professional certification, or the provision of health care and related services;

(f) stigmatization or reputational harm;

(g) disruption and intrusion from unwanted commercial communications or contacts;

(h) price discrimination;

(i) effects on an individual that are not reasonably foreseeable, contemplated by, or expected by the individual to whom the personal data relates, that are nevertheless reasonably foreseeable, contemplated by, or expected by the controller assessing privacy risk, that:

(A) alters that individual's experiences;

(B) limits that individual's choices;

(C) influences that individual's responses; or

(D) predetermines results; or

(j) other adverse consequences that affect an individual's private life, including private family matters, actions and communications within an individual's home or similar physical, online, or digital location, where an individual has a reasonable expectation that personal data will not be collected or used.

3. The fiduciary duty owed to a consumer under this section shall supersede any duty owed to owners or shareholders of a legal entity or affiliate thereof, controller or data broker, to whom this article applies.

§ 1103. Consumer rights. Any entity subject to the provisions of this article shall provide notice to consumers of their rights under this article and shall provide consumers the opportunity to opt in or opt out of processing their personal data in such a manner that the consumer

must select and clearly indicate their consent or denial of consent. Controllers shall facilitate requests to exercise the consumer rights set forth in subdivisions one through six of this section. 1. On request from a consumer, a controller shall confirm whether or not personal data concerning the consumer is being processed by the controller, including whether such personal data is sold to data brokers, and, where personal data concerning the consumer is being processed by the controller, provide access to such personal data concerning the consumer and the names of third parties to whom personal data is sold or licensed. On request from a consumer, a controller shall provide a copy of the personal data undergoing processing free of charge, up to twice annually. For any further copies requested by the consumer, the controller may charge a reasonable fee based on administrative costs. Where the consumer makes the request by electronic means, and unless otherwise requested by the consumer, the information shall be provided in a commonly used electronic form.

2. On request from a consumer, the controller, without undue delay, shall correct inaccurate personal data concerning the consumer. Taking into account the purposes of the processing, the controller shall complete incomplete personal data, including by means of providing a supplementary statement.

3. (a) On request from a consumer, a controller shall delete the consumer's personal data without undue delay where one of the following grounds applies:

(i) The personal data is no longer necessary in relation to the purposes for which the personal data was collected or otherwise processed;

(ii) For processing that requires consent under section eleven hundred five of this article, the consumer withdraws consent to processing;

(iii) The personal data has been unlawfully processed;

(iv) To comply with a legal obligation under federal, state, or local law to which the controller is subject; or

(v) The consumer otherwise requests that the data be deleted.

(b) Where the controller is obliged to delete personal data under this section that has been disclosed to third parties by the controller, including data brokers that received the data through a sale, the controller shall take reasonable steps, which may include technical measures, to inform other controllers that are processing the personal data that the consumer has requested the deletion by the other controllers of any links to, or copy or replication of, the personal data. Compliance with this obligation shall take into account available technology and cost of implementation.

(c) This subdivision does not apply to the extent processing is necessary:

(i) for exercising the right of free speech;

(ii) for compliance with a legal obligation that requires processing by federal, state, or local law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(iii) for reasons of public interest in the area of public health, where the processing (A) is subject to suitable and specific measures to safeguard the rights of the consumer; and (B) is processed by or under the responsibility of a professional subject to confidentiality obligations under federal, state, or local law;

(iv) for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes, where the

deletion of such personal data is likely to render impossible or seriously impair the achievement of the objectives of the processing; or

(v) for the establishment, exercise, or defense of legal claims.

4. (a) The controller shall cease processing if one of the following grounds applies:

(i) The accuracy of the personal data is contested by the consumer, for a period enabling the controller to verify the accuracy of the personal data;

(ii) The processing is unlawful and the consumer opposes the deletion of the personal data and requests the restriction of processing instead;

(iii) The controller no longer needs the personal data for the purposes of the processing, but such personal data is required by the consumer for the establishment, exercise, or defense of legal claims; or

(iv) The consumer otherwise requests that the controller cease processing.

(b) Where personal data is subject to a restriction or processing under this subdivision, the personal data shall, with the exception of storage, only be processed (i) with the consumer's consent; (ii) for the establishment, exercise, or defense of legal claims; or (iii) for reasons of important public interest under federal, state, or local law.

(c) Where a consumer has taken steps by the online selection of options related to sharing personal data a controller is obligated to adhere to such selections.

5. (a) On request from a consumer, the controller shall provide the consumer any personal data concerning such consumer that such consumer has provided to the controller in a structured, commonly used, and machine-readable format if (i)(A) the processing of such personal data requires consent under section eleven hundred five of this article, (B) the processing of such personal data is necessary for the performance of a contract to which the consumer is a party, or (C) in order to take steps at the request of the consumer prior to entering into a contract; and (ii) the processing is carried out by automated means.

(b) Controllers shall transmit the personal data requested under this subdivision directly from one controller to another, where technically feasible, and transmit the personal data to another controller without hindrance from the controller to which the personal data was provided.

(c) Requests for personnel data under this subdivision shall be without prejudice to subdivision three of this section.

(d) The rights provided in this subdivision do not apply to processing necessary for the performance of a task carried out in the public interest and shall not adversely affect the rights of consumers.

6. A consumer shall not be subject to a decision based solely on profiling which produces legal effects concerning such consumer or similarly significantly affects the consumer. Legal or similarly significant effects include, but are not limited to, denial of consequential services or support, such as financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, and health care services.

(a) This subdivision does not apply if the decision is authorized by federal or state law to which the controller is subject and which incorporates suitable measures to safeguard the consumer's rights and legitimate interests, as indicated by the risk assessments required by section eleven hundred five of this article.

(b) Notwithstanding paragraph (a) of this subdivision, the controller shall implement suitable measures to safeguard consumer's rights and legitimate interests with respect to decisions based solely on profil-

ing, including providing human review of the decision, to express the consumer's point of view with respect to the decision, and to contest the decision.

7. A controller shall communicate any correction, deletion, or restriction of processing carried out in accordance with subdivisions two, three or four of this section to each third-party recipient to whom the personal data has been disclosed, including third parties that received the data through a sale, unless this proves impossible. The controller shall inform the consumer about such third-party recipients, if any, if the consumer requests such information.

8. A controller shall provide information on action taken on a request under subdivisions one through six of this section without undue delay and in any event within thirty days of receipt of the request. That period may be extended by sixty additional days where necessary, taking into account the complexity and number of the requests. The controller shall inform the consumer of any such extension within thirty days of receipt of the request, together with the reasons for the delay. Where the consumer makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the consumer.

(a) If a controller does not take action on the request of a consumer, the controller shall inform the consumer without undue delay and at the latest within thirty days of receipt of the request of the reasons for not taking action and any possibility for internal review of the decision by the controller.

(b) Information provided under this section must be provided by the controller free of charge to the consumer. Where requests from a consumer are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either: (i) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (ii) refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

(c) Where the controller has reasonable doubts concerning the identity of the consumer making a request under subdivisions one through six of this section, the controller may request the provision of additional information necessary to confirm the identity of the consumer.

(d) A controller shall conduct an internal review on any action taken upon request of a consumer under subdivisions one through six of this section.

§ 1104. Transparency. 1. Controllers shall be transparent and accountable for their processing of personal data, by making available in a form that is reasonably accessible to consumers a clear, meaningful privacy notice that is easily understood and which includes:

(a) the categories of personal data collected by the controller;

(b) the purposes for which the categories of personal data is used and disclosed to third parties, if any;

(c) the rights that consumers may exercise pursuant to section eleven hundred three of this article, if any;

(d) the categories of personal data that the controller shares with third parties, if any; and

(e) the names and categories of third parties, if any, with whom the controller shares personal data.

2. Controllers that engage in profiling shall disclose such profiling to the consumer at or before the time personal data is obtained, includ-

1 ing meaningful information about the logic involved and the significance
2 and envisaged consequences of the profiling.
3 3. If a controller sells personal data to data brokers or processes
4 personal data for direct marketing purposes, including targeted market-
5 ing and profiling to the extent that it is related to such direct
6 marketing, it shall disclose such processing, as well as the manner in
7 which a consumer may exercise the right to object to such processing, in
8 a clear and prominent manner.
9 § 1105. Responsibility according to role. 1. Controllers and brokers
10 shall be responsible for meeting the obligations set forth under this
11 article.
12 2. Processors and brokers are responsible under this article for
13 adhering to the instructions of the controller and assisting the
14 controller to meet its obligations under this article.
15 3. Processing by a processor shall be governed by a contract between
16 the controller and the processor that is binding on the processor and
17 that sets out the processing instructions to which the processor is
18 bound.
19 § 1106. De-identified data. A controller or processor that uses de-i-
20 dentified data shall exercise reasonable oversight to monitor compliance
21 with any contractual commitments to which the de-identified data is
22 subject, and shall take appropriate steps to address any breaches of
23 contractual commitments.
24 § 1107. Exemptions. 1. The obligations imposed on controllers or
25 processors under this article do not restrict a controller's or process-
26 or's ability to:
27 (a) comply with federal, state, or local laws;
28 (b) comply with a civil, criminal, or regulatory inquiry, investi-
29 gation, subpoena, or summons by federal, state, local, or other govern-
30 mental authorities;
31 (c) disclose personal data to a law enforcement agency if such infor-
32 mation:
33 (i) was inadvertently obtained by the controller or data broker; and
34 (ii) appears to pertain to the commission of a crime;
35 (d) cooperate with a governmental entity if the controller or data
36 broker, in good faith, believes that an emergency involving danger of
37 death or serious physical injury to any person requires disclosure of
38 personal data without delay;
39 (e) investigate, exercise, or defend legal claims; or
40 (f) prevent or detect identity theft, fraud, or other criminal activ-
41 ity or verify identities.
42 2. The obligations imposed on controllers or processors under this
43 article do not apply where compliance by the controller or processor
44 with this article would violate an evidentiary privilege under New York
45 law and do not prevent a controller or processor from providing personal
46 data concerning a consumer to a person covered by an evidentiary privi-
47 lege under New York law as part of a privileged communication.
48 3. A controller or processor that discloses personal data to a third-
49 party controller or processor in compliance with the requirements of
50 this article is not in violation of this article, including under
51 section eleven hundred eight of this article, if the third-party recipi-
52 ent processes such personal data in violation of this article, provided
53 that, at the time of disclosing the personal data, the disclosing
54 controller or processor did not have actual knowledge that the third-
55 party recipient intended to commit a violation. A third-party recipient
56 receiving personal data from a controller or processor is likewise not

1 liable under this article, including under section eleven hundred eight
2 of this article, for the obligations of a controller or processor to
3 whom it provides services.
4 4. This article does not require a controller or processor to do the
5 following:
6 (a) re-identify de-identified data;
7 (b) retain personal data concerning a consumer that he or she would
8 not otherwise retain in the ordinary course of business; or
9 (c) comply with a request to exercise any of the rights under subdivi-
10 sions one through six of section eleven hundred three of this article if
11 the controller is unable to verify, using commercially reasonable
12 efforts, the identity of the consumer making the request.
13 5. Obligations imposed on controllers and processors under this arti-
14 cle do not apply to the processing of personal data by a natural person
15 in the course of a purely personal or household activity.
16 § 1108. Liability. Where more than one controller or processor, or
17 both a controller and a processor, involved in the same processing, is
18 in violation of this article, the liability shall be allocated among the
19 parties according to principles of comparative fault, unless such
20 liability is otherwise allocated by contract among the parties.
21 § 1109. Enforcement. 1. The legislature finds that the practices
22 covered by this article are matters vitally affecting the public inter-
23 est for the purpose of providing consumer protection from deceptive acts
24 and practices under article twenty-two-A of this chapter. A violation of
25 this article is not reasonable in relation to the development and pres-
26 ervation of business and is an unfair or deceptive act in trade or
27 commerce and an unfair method of competition for the purpose of applying
28 article twenty-two-A of this chapter.
29 2. The attorney general may bring an action in the name of the state,
30 or as parens patriae on behalf of persons residing in the state, to
31 enforce this article.
32 3. In addition to any right of action granted to any governmental body
33 pursuant to this section, any person who has been injured by reason of a
34 violation of this article may bring an action in his or her own name to
35 enjoin such unlawful act, or to recover his or her actual damages, or
36 both such actions. The court may award reasonable attorney's fees to a
37 prevailing plaintiff.
38 4. Any controller or processor who violates this article is subject to
39 an injunction and liable for damages and a civil penalty. When calculat-
40 ing damages and civil penalties, the court shall consider the number of
41 affected individuals, the severity of the violation, and the size and
42 revenues of the covered entity. Each individual whose information was
43 unlawfully processed counts as a separate violation. Each provision of
44 this article that was violated counts as a separate violation.
45 § 1110. Preemption. This article supersedes and preempts laws adopted
46 by any local entity regarding the processing of personal data by
47 controllers or processors.
48 § 3. This act shall take effect on the one hundred eightieth day after
49 it shall have become a law.

KeyCite Yellow Flag - Negative Treatment
Declined to Extend by United States v. Beverly, 5th Cir.(Tex.), November 14, 2019

138 S.Ct. 2206
Supreme Court of the United States

Timothy Ivory CARPENTER, Petitioner
v.
United States.

No. 16–402.
|
Argued Nov. 29, 2017.
|
Decided June 22, 2018.

Synopsis
Background: In prosecution for multiple counts of robbery and carrying a firearm during federal crime of violence, the United States District Court for the Eastern District of Michigan, Sean F. Cox, J., 2013 WL 6385838, denied defendant's motion to suppress cell-site location information (CSLI), and denied defendant's posttrial motion for acquittal, 2013 WL 6729900, and the District Court, Sean F. Cox, J., 2014 WL 943094, denied defendant's motion for new trial. Defendant appealed. The United States Court of Appeals for the Sixth Circuit, Kethledge, Circuit Judge, 819 F.3d 880, affirmed. Certiorari was granted.

Holdings: The Supreme Court, Chief Justice Roberts, held that:

[1] an individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through CSLI;

[2] seven days of historical CSLI obtained from defendant's wireless carrier, pursuant to an order issued under the Stored Communications Act (SCA), was the product of a "search";

[3] Government's access to 127 days of historical CSLI invaded defendant's reasonable expectation of privacy; and

[4] Government must generally obtain a search warrant supported by probable cause before acquiring CSLI from a wireless carrier.

Reversed and remanded.

Justice Kennedy filed a dissenting opinion, in which Justices Thomas and Alito joined.

Justice Thomas filed a dissenting opinion.

Justice Alito filed a dissenting opinion, in which Justice Thomas joined.

Justice Gorsuch filed a dissenting opinion.

West Headnotes (20)

[1] **Searches and Seizures**
⇐Fourth Amendment and reasonableness in general

The basic purpose of the Fourth Amendment is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials. U.S.C.A. Const.Amend. 4.

34 Cases that cite this headnote

[2] **Searches and Seizures**
⇐Persons, Places and Things Protected

Property rights are not the sole measure of Fourth Amendment violations; the Fourth Amendment protects people, not places. U.S.C.A. Const.Amend. 4.

41 Cases that cite this headnote

[3] **Searches and Seizures**
⇐What Constitutes Search or Seizure
Searches and Seizures
⇐Expectation of privacy

When an individual seeks to preserve something as private, and his expectation of privacy is one that society is prepared to recognize as reasonable, official intrusion into that private sphere generally qualifies as a search under the Fourth Amendment, and requires a warrant supported by probable cause. U.S.C.A. Const.Amend. 4.

37 Cases that cite this headnote

[4] **Searches and Seizures**
Expectation of privacy

Although no single rubric definitively resolves which expectations of privacy are entitled to protection under the Fourth Amendment, the analysis is informed by historical understandings of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted. U.S.C.A. Const.Amend. 4.

12 Cases that cite this headnote

[5] **Searches and Seizures**
Expectation of privacy

While property rights are often informative in resolving which expectations of privacy are entitled to protection under the Fourth Amendment, such an interest is not fundamental or dispositive in determining which expectations of privacy are legitimate. U.S.C.A. Const.Amend. 4.

25 Cases that cite this headnote

[6] **Searches and Seizures**
Fourth Amendment and reasonableness in general

The Fourth Amendment seeks to secure the privacies of life against arbitrary power. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[7] **Searches and Seizures**
Fourth Amendment and reasonableness in general

A central aim of the Framers in adopting the Fourth Amendment was to place obstacles in the way of a too permeating police surveillance. U.S.C.A. Const.Amend. 4.

3 Cases that cite this headnote

[8] **Searches and Seizures**
Use of electronic devices; tracking devices or "beepers."

In light of the immense storage capacity of modern cell phones, police officers must generally obtain a warrant before searching the contents of a phone. U.S.C.A. Const.Amend. 4.

12 Cases that cite this headnote

[9] **Searches and Seizures**
Abandoned, surrendered, or disclaimed items

Under the third-party doctrine, a person has no legitimate expectation of privacy, for Fourth Amendment purposes, in information he voluntarily turns over to third parties, and that remains true even if the information is revealed on the assumption that it will be used only for a limited purpose; as a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections. U.S.C.A. Const.Amend. 4.

39 Cases that cite this headnote

[10] **Searches and Seizures**
Expectation of privacy
Telecommunications
Carrier's cooperation; pen registers and tracing

An individual maintains a legitimate expectation of privacy, for Fourth Amendment purposes, in the record of his physical movements as captured through cell-site location information (CSLI). U.S.C.A. Const.Amend. 4.

119 Cases that cite this headnote

[11] **Searches and Seizures**
Use of electronic devices; tracking devices or "beepers."

Seven days of historical cell-site location information (CSLI) obtained from suspect's wireless carrier, pursuant to an order issued by a federal magistrate judge under the Stored Communications Act (SCA), was the product of a "search" under the Fourth Amendment. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

75 Cases that cite this headnote

[12] **Searches and Seizures**
Persons, Places and Things Protected

A person does not surrender all Fourth Amendment protection by venturing into the public sphere, and to the contrary, what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. U.S.C.A. Const.Amend. 4.

15 Cases that cite this headnote

[13] **Searches and Seizures**
Expectation of privacy
Telecommunications
Carrier's cooperation; pen registers and tracing

Government's access to 127 days of historical cell-site location information (CSLI) obtained from suspect's wireless carrier, pursuant to an order issued by a federal magistrate judge under the Stored Communications Act (SCA), invaded suspect's reasonable expectation of privacy, under the Fourth Amendment, in the whole world of his physical movements. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

78 Cases that cite this headnote

[14] **Searches and Seizures**
Abandoned, surrendered, or disclaimed items

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another, but the fact of diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely. U.S.C.A. Const.Amend. 4.

14 Cases that cite this headnote

[15] **Telecommunications**
Carrier's cooperation; pen registers and tracing

The Government must generally obtain a search warrant supported by probable cause before acquiring cell-site location information (CSLI) from a wireless carrier. U.S.C.A. Const.Amend. 4.

164 Cases that cite this headnote

[16] **Searches and Seizures**
Necessity of and preference for warrant, and exceptions in general

Although the ultimate measure of the constitutionality of a governmental search, under the Fourth Amendment, is reasonableness, warrantless searches are typically unreasonable where a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing, and thus, in the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[17] **Telecommunications**
Carrier's cooperation; pen registers and tracing

An order issued by a federal magistrate judge under the Stored Communications Act (SCA) is not a permissible mechanism for the Government to access cell-site location information (CSLI), and before compelling a wireless carrier to turn over a subscriber's CSLI, the Fourth Amendment requires the Government to get a search warrant. U.S.C.A. Const.Amend. 4; 18 U.S.C.A. § 2703(d).

56 Cases that cite this headnote

[18] **Searches and Seizures**
Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant

One well-recognized exception to the search warrant requirement applies when the exigencies of the situation make the needs of law enforcement so compelling that a warrantless search is objectively reasonable under the Fourth Amendment. U.S.C.A. Const.Amend. 4.

11 Cases that cite this headnote

[19] **Searches and Seizures**
Emergencies and Exigent Circumstances; Opportunity to Obtain Warrant

Exigencies that support an exception to the Fourth Amendment's search warrant requirement include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence. U.S.C.A. Const.Amend. 4.

12 Cases that cite this headnote

[20] **Searches and Seizures**
Expectation of privacy

The Supreme Court is obligated, as subtler and more far-reaching means of invading privacy have become available to the Government, to ensure that the progress of science does not erode Fourth Amendment protections. U.S.C.A. Const.Amend. 4.

3 Cases that cite this headnote

***2208** *Syllabus**

Cell phones perform their wide and growing variety of functions by continuously connecting to a set of radio antennas called "cell sites." Each time a phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). Wireless carriers collect and store this information for their own business purposes. Here, after the FBI identified the cell phone numbers of several robbery suspects, prosecutors were ***2209** granted court orders to obtain the suspects' cell phone records under the Stored Communications Act. Wireless carriers produced CSLI for petitioner Timothy Carpenter's phone, and the Government was able to obtain 12,898 location points cataloging Carpenter's movements over 127 days—an average of 101 data points per day. Carpenter moved to suppress the data, arguing that the Government's seizure of the records without obtaining a warrant supported by probable cause violated

the Fourth Amendment. The District Court denied the motion, and prosecutors used the records at trial to show that Carpenter's phone was near four of the robbery locations at the time those robberies occurred. Carpenter was convicted. The Sixth Circuit affirmed, holding that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers.

Held :

1. The Government's acquisition of Carpenter's cell-site records was a Fourth Amendment search. Pp. 2212 - 2221.

(a) The Fourth Amendment protects not only property interests but certain expectations of privacy as well. *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576. Thus, when an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," official intrusion into that sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith v. Maryland,* 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (internal quotation marks and alterations omitted). The analysis regarding which expectations of privacy are entitled to protection is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll v. United States,* 267 U.S. 132, 149, 45 S.Ct. 280, 69 L.Ed. 543. These Founding-era understandings continue to inform this Court when applying the Fourth Amendment to innovations in surveillance tools. See, *e.g., Kyllo v. United States,* 533 U.S. 27, 121 S.Ct. 2038, 150 L.Ed.2d 94. Pp. 2212 - 2215.

(b) The digital data at issue—personal location information maintained by a third party—does not fit neatly under existing precedents but lies at the intersection of two lines of cases. One set addresses a person's expectation of privacy in his physical location and movements. See, *e.g., United States v. Jones,* 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (five Justices concluding that privacy concerns would be raised by GPS tracking). The other addresses a person's expectation of privacy in information voluntarily turned over to third parties. See *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (no expectation of privacy in financial records held by a bank), and *Smith,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (no expectation of privacy in records of dialed telephone numbers conveyed to telephone company). Pp. 2214 - 2216.

(c) Tracking a person's past movements through CSLI partakes of many of the qualities of GPS monitoring considered in *Jones*—it is detailed, encyclopedic, and effortlessly compiled. At the same time, however, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller.* Given the unique nature of cell-site records, this Court declines to extend *Smith* and *Miller* to cover them. Pp. 2216 - 2221.

(1) A majority of the Court has already recognized that individuals have a ***2210** reasonable expectation of privacy in the whole of their physical movements. Allowing government access to cell-site records—which "hold for many Americans the 'privacies of life,' " *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2494–2495, 189 L.Ed.2d 430—contravenes that expectation. In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring considered in *Jones* : They give the Government near perfect surveillance and allow it to travel back in time to retrace a person's whereabouts, subject only to the five-year retention policies of most wireless carriers. The Government contends that CSLI data is less precise than GPS information, but it thought the data accurate enough here to highlight it during closing argument in Carpenter's trial. At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development," *Kyllo,* 533 U.S., at 36, 121 S.Ct. 2038, and the accuracy of CSLI is rapidly approaching GPS-level precision. Pp. 2217 - 2219.

(2) The Government contends that the third-party doctrine governs this case, because cell-site records, like the records in *Smith* and *Miller,* are "business records," created and maintained by wireless carriers. But there is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers.

The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. *Smith* and *Miller,* however, did not rely solely on the act of sharing. They also considered "the nature of the particular documents sought" and limitations on any "legitimate 'expectation of privacy' concerning their contents." *Miller,* 425 U.S., at 442, 96 S.Ct. 1619. In mechanically applying the third-party doctrine to this case the Government fails to appreciate the lack of comparable limitations on the revealing nature of CSLI.

Nor does the second rationale for the third-party

doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as the term is normally understood. First, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley*, 573 U.S., at ——, 134 S.Ct., at 2484. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the user's part beyond powering up. Pp. 2219 - 2220.

(d) This decision is narrow. It does not express a view on matters not before the Court; does not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras; does not address other business records that might incidentally reveal location information; and does not consider other collection techniques involving foreign affairs or national security. Pp. 2220 - 2221.

2. The Government did not obtain a warrant supported by probable cause before acquiring Carpenter's cell-site records. It acquired those records pursuant to a court order under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). That showing falls well short of the probable cause required for a warrant. Consequently, an order issued under § 2703(d) is not a permissible mechanism for accessing historical cell-site ***2211** records. Not all orders compelling the production of documents will require a showing of probable cause. A warrant is required only in the rare case where the suspect has a legitimate privacy interest in records held by a third party. And even though the Government will generally need a warrant to access CSLI, case-specific exceptions—*e.g.*, exigent circumstances—may support a warrantless search. Pp. 2220 - 2223.

819 F.3d 880, reversed and remanded.

ROBERTS, C.J., delivered the opinion of the Court, in which GINSBURG, BREYER, SOTOMAYOR, and KAGAN, JJ., joined. KENNEDY, J., filed a dissenting opinion, in which THOMAS and ALITO, JJ., joined. THOMAS, J., filed a dissenting opinion. ALITO, J., filed a dissenting opinion, in which THOMAS, J., joined. GORSUCH, J., filed a dissenting opinion.

Attorneys and Law Firms

Nathan Freed Wessler, Ben Wizner, Brett Max Kaufman, American Civil Liberties, Union Foundation, New York, NY, David D. Cole, American Civil Liberties, Union Foundation, Washington, DC, Cecillia D. Wang, Jennifer Stisa Granick, American Civil Liberties, Union Foundation, San Francisco, CA, Harold Gurewitz, Gurewitz & Raben, PLC, Detroit, MI, Daniel S. Korobkin, Michael J. Steinberg, Kary L. Moss, American Civil Liberties, Union Fund of Michigan, Detroit, MI, Jeffrey L. Fisher, Stanford Law School, Supreme Court Litigation Clinic, Stanford, CA, for Petitioner.

Noel J. Francisco, Solicitor General, Kenneth A. Blanco, Acting Assistant Attorney General, Michael R. Dreeben, Deputy Solicitor General, Elizabeth B. Prelogar, Assistant to the Solicitor General, Jenny C. Ellickson, Attorney, Department of Justice, Washington, DC, for Respondent.

Opinion

Chief Justice ROBERTS delivered the opinion of the Court.

This case presents the question whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.

IA

There are 396 million cell phone service accounts in the United States—for a Nation of 326 million people. Cell phones perform their wide and growing variety of functions by connecting to a set of radio antennas called "cell sites." Although cell sites are usually mounted on a tower, they can also be found on light posts, flagpoles, church steeples, or the sides of buildings. Cell sites typically have several directional antennas that divide the covered area into sectors.

Cell phones continuously scan their environment looking for the best signal, which generally comes from the closest cell site. Most modern devices, such as smartphones, tap into the wireless network several times a minute whenever their signal is on, even if the owner is not using one of the phone's features. Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. The greater the concentration of cell sites, the smaller the coverage area. As data usage from cell phones has increased, ***2212** wireless carriers have installed more cell sites to handle the traffic. That has led to increasingly compact coverage areas, especially in urban areas.

Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. In addition, wireless carriers often sell aggregated location records to data brokers, without individual identifying information of the sort at issue here. While carriers have long retained CSLI for the start and end of incoming calls, in recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

B

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and (ironically enough) T–Mobile stores in Detroit. One of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts) had robbed nine different stores in Michigan and Ohio. The suspect identified 15 accomplices who had participated in the heists and gave the FBI some of their cell phone numbers; the FBI then reviewed his call records to identify additional numbers that he had called around the time of the robberies.

Based on that information, the prosecutors applied for court orders under the Stored Communications Act to obtain cell phone records for petitioner Timothy Carpenter and several other suspects. That statute, as amended in 1994, permits the Government to compel the disclosure of certain telecommunications records when it "offers specific and articulable facts showing that there are reasonable grounds to believe" that the records sought "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Federal Magistrate Judges issued two orders directing Carpenter's wireless carriers—MetroPCS and Sprint—to disclose "cell/site sector [information] for [Carpenter's] telephone[ ] at call origination and at call termination for incoming and outgoing calls" during the four-month period when the string of robberies occurred. App. to Pet. for Cert. 60a, 72a. The first order sought 152 days of cell-site records from MetroPCS, which produced records spanning 127 days. The second order requested seven days of CSLI from Sprint, which produced two days of records covering the period when Carpenter's phone was "roaming" in northeastern Ohio. Altogether the Government obtained 12,898 location points cataloging Carpenter's movements—an average of 101 data points per day.

Carpenter was charged with six counts of robbery and an additional six counts of carrying a firearm during a federal crime of violence. See 18 U.S.C. §§ 924(c), 1951(a). Prior to trial, Carpenter moved to suppress the cell-site data provided by the wireless carriers. He argued that the Government's seizure of the records violated the Fourth Amendment because they had been obtained without a warrant supported by probable cause. The District Court denied the motion. App. to Pet. for Cert. 38a–39a.

At trial, seven of Carpenter's confederates pegged him as the leader of the operation. In addition, FBI agent Christopher Hess offered expert testimony about the cell-site data. Hess explained that each time a cell phone taps into the wireless network, the carrier logs a time-stamped record of the cell site and particular sector that were used. With this information, ***2213** Hess produced maps that placed Carpenter's phone near four of the charged robberies. In the Government's view, the location records clinched the case: They confirmed that Carpenter was "right where the ... robbery was at the exact time of the robbery." App. 131 (closing argument). Carpenter was convicted on all but one of the firearm counts and sentenced to more than 100 years in prison.

The Court of Appeals for the Sixth Circuit affirmed. 819 F.3d 880 (2016). The court held that Carpenter lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers. Given that cell phone users voluntarily convey cell-site data to their carriers as "a means of establishing communication," the court concluded that the resulting business records are not entitled to Fourth Amendment protection. *Id.*, at 888 (quoting *Smith v. Maryland,* 442 U.S. 735, 741, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)).

We granted certiorari. 582 U.S. ——, 137 S.Ct. 2211, 198 L.Ed.2d 657 (2017).

IIA

[1] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." The "basic purpose of this Amendment," our cases have recognized, "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." *Camara v. Municipal Court of City and County of San Francisco,* 387 U.S. 523, 528, 87 S.Ct. 1727, 18 L.Ed.2d 930 (1967). The Founding generation crafted the Fourth Amendment as a "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." *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014). In fact, as John Adams recalled, the patriot James Otis's 1761 speech condemning writs of assistance was "the first act of opposition to the arbitrary claims of Great Britain" and helped spark the Revolution itself. *Id.,* at —— – ——, 134 S.Ct., at 2494 (quoting 10 Works of John Adams 248 (C. Adams ed. 1856)).

[2] [3] For much of our history, Fourth Amendment search doctrine was "tied to common-law trespass" and focused on whether the Government "obtains information by physically intruding on a constitutionally protected area." *United States v. Jones,* 565 U.S. 400, 405, 406, n. 3, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). More recently, the Court has recognized that "property rights are not the sole measure of Fourth Amendment violations." *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992). In *Katz v. United States,* 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), we established that "the Fourth Amendment protects people, not places," and expanded our conception of the Amendment to protect certain expectations of privacy as well. When an individual "seeks to preserve something as private," and his expectation of privacy is "one that society is prepared to recognize as reasonable," we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause. *Smith,* 442 U.S., at 740, 99 S.Ct. 2577 (internal quotation marks and alterations omitted).

[4] [5] [6] [7] Although no single rubric definitively resolves which expectations of privacy ***2214** are entitled to protection,[1] the analysis is informed by historical understandings "of what was deemed an unreasonable search and seizure when [the Fourth Amendment] was adopted." *Carroll v. United States,* 267 U.S. 132, 149, 45 S.Ct. 280, 69 L.Ed. 543 (1925). On this score, our cases have recognized some basic guideposts. First, that the Amendment seeks to secure "the privacies of life" against "arbitrary power." *Boyd v. United States,* 116 U.S. 616, 630, 6 S.Ct. 524, 29 L.Ed. 746 (1886). Second, and relatedly, that a central aim of the Framers was "to place obstacles in the way of a too permeating police surveillance." *United States v. Di Re,* 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948).

We have kept this attention to Founding-era understandings in mind when applying the Fourth Amendment to innovations in surveillance tools. As technology has enhanced the Government's capacity to encroach upon areas normally guarded from inquisitive eyes, this Court has sought to "assure [ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). For that reason, we rejected in *Kyllo* a "mechanical interpretation" of the Fourth Amendment and held that use of a thermal imager to detect heat radiating from the side of the defendant's home was a search. *Id.,* at 35, 121 S.Ct. 2038. Because any other conclusion would leave homeowners "at the mercy of advancing technology," we determined that the Government—absent a warrant—could not capitalize on such new sense-enhancing technology to explore what was happening within the home. *Ibid.*

[8] Likewise in *Riley,* the Court recognized the "immense storage capacity" of modern cell phones in holding that police officers must generally obtain a warrant before searching the contents of a phone. 573 U.S., at ——, 134 S.Ct., at 2489. We explained that while the general rule allowing warrantless searches incident to arrest "strikes the appropriate balance in the context of physical objects, neither of its rationales has much force with respect to" the vast store of sensitive information on a cell phone. *Id.,* at ——, 134 S.Ct., at 2484.

B

The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls. This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform ***2215** our understanding of the privacy interests at stake.

The first set of cases addresses a person's expectation of privacy in his physical location and movements. In *United States v. Knotts,* 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), we considered the Government's use of a "beeper" to aid in tracking a vehicle through traffic. Police officers in that case planted a beeper in a container of chloroform before it was purchased by one of Knotts's co-conspirators. The officers (with intermittent aerial assistance) then followed the automobile carrying the container from Minneapolis to Knotts's cabin in Wisconsin, relying on the beeper's signal to help keep the vehicle in view. The Court concluded that the "augment[ed]" visual surveillance did not constitute a search because "[a] person traveling in an automobile on

public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." *Id.*, at 281, 282, 103 S.Ct. 1081. Since the movements of the vehicle and its final destination had been "voluntarily conveyed to anyone who wanted to look," Knotts could not assert a privacy interest in the information obtained. *Id.*, at 281, 103 S.Ct. 1081.

This Court in *Knotts*, however, was careful to distinguish between the rudimentary tracking facilitated by the beeper and more sweeping modes of surveillance. The Court emphasized the "limited use which the government made of the signals from this particular beeper" during a discrete "automotive journey." *Id.*, at 284, 285, 103 S.Ct. 1081. Significantly, the Court reserved the question whether "different constitutional principles may be applicable" if "twenty-four hour surveillance of any citizen of this country [were] possible." *Id.*, at 283–284, 103 S.Ct. 1081.

Three decades later, the Court considered more sophisticated surveillance of the sort envisioned in *Knotts* and found that different principles did indeed apply. In *United States v. Jones*, FBI agents installed a GPS tracking device on Jones's vehicle and remotely monitored the vehicle's movements for 28 days. The Court decided the case based on the Government's physical trespass of the vehicle. 565 U.S., at 404–405, 132 S.Ct. 945. At the same time, five Justices agreed that related privacy concerns would be raised by, for example, "surreptitiously activating a stolen vehicle detection system" in Jones's car to track Jones himself, or conducting GPS tracking of his cell phone. *Id.*, at 426, 428, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.*, at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring). Since GPS monitoring of a vehicle tracks "every movement" a person makes in that vehicle, the concurring Justices concluded that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"—regardless whether those movements were disclosed to the public at large. *Id.*, at 430, 132 S.Ct. 945 (opinion of Alito, J.); *id.*, at 415, 132 S.Ct. 945 (opinion of Sotomayor, J.).[2]

***2216** [9] In a second set of decisions, the Court has drawn a line between what a person keeps to himself and what he shares with others. We have previously held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S., at 743–744, 99 S.Ct. 2577. That remains true "even if the information is revealed on the assumption that it will be used only for a limited purpose." *United States v. Miller*, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). As a result, the Government is typically free to obtain such information from the recipient without triggering Fourth Amendment protections.

This third-party doctrine largely traces its roots to *Miller*. While investigating Miller for tax evasion, the Government subpoenaed his banks, seeking several months of canceled checks, deposit slips, and monthly statements. The Court rejected a Fourth Amendment challenge to the records collection. For one, Miller could "assert neither ownership nor possession" of the documents; they were "business records of the banks." *Id.*, at 440, 96 S.Ct. 1619. For another, the nature of those records confirmed Miller's limited expectation of privacy, because the checks were "not confidential communications but negotiable instruments to be used in commercial transactions," and the bank statements contained information "exposed to [bank] employees in the ordinary course of business." *Id.*, at 442, 96 S.Ct. 1619. The Court thus concluded that Miller had "take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government." *Id.*, at 443, 96 S.Ct. 1619.

Three years later, *Smith* applied the same principles in the context of information conveyed to a telephone company. The Court ruled that the Government's use of a pen register—a device that recorded the outgoing phone numbers dialed on a landline telephone—was not a search. Noting the pen register's "limited capabilities," the Court "doubt[ed] that people in general entertain any actual expectation of privacy in the numbers they dial." 442 U.S., at 742, 99 S.Ct. 2577. Telephone subscribers know, after all, that the numbers are used by the telephone company "for a variety of legitimate business purposes," including routing calls. *Id.*, at 743, 99 S.Ct. 2577. And at any rate, the Court explained, such an expectation "is not one that society is prepared to recognize as reasonable." *Ibid.* (internal quotation marks omitted). When Smith placed a call, he "voluntarily conveyed" the dialed numbers to the phone company by "expos[ing] that information to its equipment in the ordinary course of business." *Id.*, at 744, 99 S.Ct. 2577 (internal quotation marks omitted). Once again, we held that the defendant "assumed the risk" that the company's records "would be divulged to police." *Id.*, at 745, 99 S.Ct. 2577.

III

The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in

Jones. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.

At the same time, the fact that the individual continuously reveals his location to his wireless carrier implicates the third-party principle of *Smith* and *Miller*. But while the third-party doctrine applies to telephone numbers and bank records, it is not clear whether its logic extends to the qualitatively different category of cell-site ***2217** records. After all, when *Smith* was decided in 1979, few could have imagined a society in which a phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements.

[10] [11] We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection. Whether the Government employs its own surveillance technology as in *Jones* or leverages the technology of a wireless carrier, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI. The location information obtained from Carpenter's wireless carriers was the product of a search.[3]

A

[12] A person does not surrender all Fourth Amendment protection by venturing into the public sphere. To the contrary, "what [one] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz*, 389 U.S., at 351–352, 88 S.Ct. 507. A majority of this Court has already recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. *Jones*, 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.*, at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring). Prior to the digital age, law enforcement might have pursued a suspect for a brief stretch, but doing so "for any extended period of time was difficult and costly and therefore rarely undertaken." *Id.*, at 429, 132 S.Ct. 945 (opinion of Alito, J.). For that reason, "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period." *Id.*, at 430, 132 S.Ct. 945.

[13] Allowing government access to cell-site records contravenes that expectation. Although such records are generated for commercial purposes, that distinction does not negate Carpenter's anticipation of privacy in his physical location. Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations." *Id.*, at 415, 132 S.Ct. 945 (opinion of SOTOMAYOR, J.). These location records "hold for many Americans the 'privacies of life.' " *Riley*, 573 U.S., at ——, 134 S.Ct., at 2494–2495 (quoting *Boyd*, 116 U.S., at 630, 6 S.Ct. 524). And like GPS monitoring, cell phone ***2218** tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools. With just the click of a button, the Government can access each carrier's deep repository of historical location information at practically no expense.

In fact, historical cell-site records present even greater privacy concerns than the GPS monitoring of a vehicle we considered in *Jones*. Unlike the bugged container in *Knotts* or the car in *Jones*, a cell phone—almost a "feature of human anatomy," *Riley*, 573 U.S., at ——, 134 S.Ct., at 2484—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. See *id.*, at ——, 134 S.Ct., at 2490 (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); contrast *Cardwell v. Lewis*, 417 U.S. 583, 590, 94 S.Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality opinion) ("A car has little capacity for escaping public scrutiny."). Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user.

Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those

belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in *Jones,* police need not even know in advance whether they want to follow a particular individual, or when.

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. Only the few without cell phones could escape this tireless and absolute surveillance.

The Government and Justice KENNEDY contend, however, that the collection of CSLI should be permitted because the data is less precise than GPS information. Not to worry, they maintain, because the location records did "not on their own suffice to place [Carpenter] at the crime scene"; they placed him within a wedge-shaped sector ranging from one-eighth to four square miles. Brief for United States 24; see *post,* at 2232 - 2233. Yet the Court has already rejected the proposition that "inference insulates a search." *Kyllo,* 533 U.S., at 36, 121 S.Ct. 2038. From the 127 days of location data it received, the Government could, in combination with other information, deduce a detailed log of Carpenter's movements, including when he was at the site of the robberies. And the Government thought the CSLI accurate enough to highlight it during the closing argument of his trial. App. 131.

At any rate, the rule the Court adopts "must take account of more sophisticated systems that are already in use or in development." ***2219** *Kyllo,* 533 U.S., at 36, 121 S.Ct. 2038. While the records in this case reflect the state of technology at the start of the decade, the accuracy of CSLI is rapidly approaching GPS-level precision. As the number of cell sites has proliferated, the geographic area covered by each cell sector has shrunk, particularly in urban areas. In addition, with new technology measuring the time and angle of signals hitting their towers, wireless carriers already have the capability to pinpoint a phone's location within 50 meters. Brief for Electronic Frontier Foundation et al. as *Amici Curiae* 12 (describing triangulation methods that estimate a device's location inside a given cell sector).

Accordingly, when the Government accessed CSLI from the wireless carriers, it invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements.

B

The Government's primary contention to the contrary is that the third-party doctrine governs this case. In its view, cell-site records are fair game because they are "business records" created and maintained by the wireless carriers. The Government (along with Justice KENNEDY) recognizes that this case features new technology, but asserts that the legal question nonetheless turns on a garden-variety request for information from a third-party witness. Brief for United States 32–34; *post,* at 2229 - 2231.

The Government's position fails to contend with the seismic shifts in digital technology that made possible the tracking of not only Carpenter's location but also everyone else's, not for a short period but for years and years. Sprint Corporation and its competitors are not your typical witnesses. Unlike the nosy neighbor who keeps an eye on comings and goings, they are ever alert, and their memory is nearly infallible. There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information.

[14] The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another. But the fact of "diminished privacy interests does not mean that the Fourth Amendment falls out of the picture entirely." *Riley,* 573 U.S., at ——, 134 S.Ct., at 2488. *Smith* and *Miller,* after all, did not rely solely on the act of sharing. Instead, they considered "the nature of the particular documents sought" to determine whether "there is a legitimate 'expectation of privacy' concerning their contents." *Miller,* 425 U.S., at 442, 96 S.Ct. 1619. *Smith* pointed out the limited capabilities of a pen register; as explained in *Riley,* telephone call logs reveal little in the way of "identifying information." *Smith,* 442 U.S., at 742, 99 S.Ct. 2577; *Riley,* 573 U.S., at ——, 134 S.Ct., at 2493. *Miller* likewise noted that checks were "not confidential communications but negotiable instruments to be used in commercial transactions." 425 U.S., at 442, 96 S.Ct. 1619. In mechanically applying the third-party doctrine to this case, the Government fails to appreciate that there are no comparable limitations on the revealing nature of CSLI.

The Court has in fact already shown special solicitude for location information in the third-party context. In *Knotts,* the Court relied on *Smith* to hold that an individual has no

reasonable expectation of privacy in public movements that he "voluntarily ***2220** conveyed to anyone who wanted to look." *Knotts,* 460 U.S., at 281, 103 S.Ct. 1081; see *id.,* at 283, 103 S.Ct. 1081 (discussing *Smith*). But when confronted with more pervasive tracking, five Justices agreed that longer term GPS monitoring of even a vehicle traveling on public streets constitutes a search. *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment); *id.,* at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring). Justice GORSUCH wonders why "someone's location when using a phone" is sensitive, *post,* at 2262, and Justice KENNEDY assumes that a person's discrete movements "are not particularly private," *post,* at 2232. Yet this case is not about "using a phone" or a person's movement at a particular time. It is about a detailed chronicle of a person's physical presence compiled every day, every moment, over several years. Such a chronicle implicates privacy concerns far beyond those considered in *Smith* and *Miller.*

Neither does the second rationale underlying the third-party doctrine—voluntary exposure—hold up when it comes to CSLI. Cell phone location information is not truly "shared" as one normally understands the term. In the first place, cell phones and the services they provide are "such a pervasive and insistent part of daily life" that carrying one is indispensable to participation in modern society. *Riley,* 573 U.S., at ——, 134 S.Ct., at 2484. Second, a cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI, including incoming calls, texts, or e-mails and countless other data connections that a phone automatically makes when checking for news, weather, or social media updates. Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily "assume[ ] the risk" of turning over a comprehensive dossier of his physical movements. *Smith,* 442 U.S., at 745, 99 S.Ct. 2577.

We therefore decline to extend *Smith* and *Miller* to the collection of CSLI. Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment.

* * *

Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information. Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future." *Northwest Airlines, Inc. v. Minnesota,* 322 U.S. 292, 300, 64 S.Ct. 950, 88 L.Ed. 1283 (1944).[4]

***2221** IV

[15] [16] Having found that the acquisition of Carpenter's CSLI was a search, we also conclude that the Government must generally obtain a warrant supported by probable cause before acquiring such records. Although the "ultimate measure of the constitutionality of a governmental search is 'reasonableness,' " our cases establish that warrantless searches are typically unreasonable where "a search is undertaken by law enforcement officials to discover evidence of criminal wrongdoing." *Vernonia School Dist. 47J v. Acton,* 515 U.S. 646, 652–653, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995). Thus, "[i]n the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement." *Riley,* 573 U.S., at ——, 134 S.Ct., at 2482.

[17] The Government acquired the cell-site records pursuant to a court order issued under the Stored Communications Act, which required the Government to show "reasonable grounds" for believing that the records were "relevant and material to an ongoing investigation." 18 U.S.C. § 2703(d). That showing falls well short of the probable cause required for a warrant. The Court usually requires "some quantum of individualized suspicion" before a search or seizure may take place. *United States v. Martinez–Fuerte,* 428 U.S. 543, 560–561, 96 S.Ct. 3074, 49 L.Ed.2d 1116 (1976). Under the standard in the Stored Communications Act, however, law enforcement need only show that the cell-site evidence might be pertinent to an ongoing investigation—a "gigantic" departure from the probable cause rule, as the Government explained below. App. 34. Consequently, an order issued under Section 2703(d) of the Act is not a permissible mechanism for accessing historical cell-site records. Before compelling a wireless carrier to turn over a subscriber's CSLI, the Government's obligation is a familiar one—get a warrant.

Justice ALITO contends that the warrant requirement simply does not apply when the Government acquires records using compulsory process. Unlike an actual search, he says, subpoenas for documents do not involve the direct taking of evidence; they are at most a "constructive search" conducted by the target of the subpoena. *Post,* at 2252 - 2253. Given this lesser intrusion on personal privacy, Justice ALITO argues that the compulsory production of records is not held to the same probable cause standard. In his view, this Court's precedents set forth a categorical rule—separate and distinct from the third-party doctrine—subjecting subpoenas to lenient scrutiny without regard to the suspect's expectation of privacy in the records. *Post,* at 2250 - 2257.

But this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy. Almost all of the examples Justice ALITO cites, see *post,* at 2253 - 2255, contemplated requests for evidence implicating diminished privacy interests or for a corporation's own books.[3] The lone exception, of course, is ***2222** *Miller,* where the Court's analysis of the third-party subpoena merged with the application of the third-party doctrine. 425 U.S., at 444, 96 S.Ct. 1619 (concluding that Miller lacked the necessary privacy interest to contest the issuance of a subpoena to his bank).

Justice ALITO overlooks the critical issue. At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers. When confronting new concerns wrought by digital technology, this Court has been careful not to uncritically extend existing precedents. See *Riley,* 573 U.S., at ——, 134 S.Ct., at 2485 ("A search of the information on a cell phone bears little resemblance to the type of brief physical search considered [in prior precedents].").

If the choice to proceed by subpoena provided a categorical limitation on Fourth Amendment protection, no type of record would ever be protected by the warrant requirement. Under Justice ALITO's view, private letters, digital contents of a cell phone—any personal information reduced to document form, in fact—may be collected by subpoena for no reason other than "official curiosity." *United States v. Morton Salt Co.,* 338 U.S. 632, 652, 70 S.Ct. 357, 94 L.Ed. 401 (1950). Justice KENNEDY declines to adopt the radical implications of this theory, leaving open the question whether the warrant requirement applies "when the Government obtains the modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party." *Post,* at 2230 (citing *United States v. Warshak,* 631 F.3d 266, 283–288 (C.A.6 2010)). That would be a sensible exception, because it would prevent the subpoena doctrine from overcoming any reasonable expectation of privacy. If the third-party doctrine does not apply to the "modern-day equivalents of an individual's own 'papers' or 'effects,' " then the clear implication is that the documents should receive full Fourth Amendment protection. We simply think that such protection should extend as well to a detailed log of a person's movements over several years.

This is certainly not to say that all orders compelling the production of documents will require a showing of probable cause. The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party.

[18] [19] Further, even though the Government will generally need a warrant to access CSLI, case-specific exceptions may support a warrantless search of an individual's cell-site records under certain circumstances. "One well-recognized exception applies when ' "the exigencies of the situation" make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.' " *Kentucky v. King,* 563 U.S. 452, 460, 131 S.Ct. 1849, 179 L.Ed.2d 865 (2011) (quoting ***2223** *Mincey v. Arizona,* 437 U.S. 385, 394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978)). Such exigencies include the need to pursue a fleeing suspect, protect individuals who are threatened with imminent harm, or prevent the imminent destruction of evidence. 563 U.S., at 460, and n. 3, 131 S.Ct. 1849.

As a result, if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless collection of CSLI. Lower courts, for instance, have approved warrantless searches related to bomb threats, active shootings, and child abductions. Our decision today does not call into doubt warrantless access to CSLI in such circumstances. While police must get a warrant when collecting CSLI to assist in the mine-run criminal investigation, the rule we set forth does not limit their ability to respond to an ongoing emergency.

* * *

[20] As Justice Brandeis explained in his famous dissent, the Court is obligated—as "[s]ubtler and more far-reaching means of invading privacy have become

available to the Government"—to ensure that the "progress of science" does not erode Fourth Amendment protections. *Olmstead v. United States,* 277 U.S. 438, 473–474, 48 S.Ct. 564, 72 L.Ed. 944 (1928). Here the 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, "after consulting the lessons of history," drafted the Fourth Amendment to prevent. *Di Re,* 332 U.S., at 595, 68 S.Ct. 222.

We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment.

The judgment of the Court of Appeals is reversed, and the case is remanded for further proceedings consistent with this opinion.

It is so ordered.

Justice KENNEDY, with whom Justice THOMAS and Justice ALITO join, dissenting.

This case involves new technology, but the Court's stark departure from relevant Fourth Amendment precedents and principles is, in my submission, unnecessary and incorrect, requiring this respectful dissent.

The new rule the Court seems to formulate puts needed, reasonable, accepted, lawful, and congressionally authorized criminal investigations at serious risk in serious cases, often when law enforcement seeks to prevent the threat of violent crimes. And it places undue restrictions on the lawful and necessary enforcement powers exercised not only by the Federal Government, but also by law enforcement in every State and locality throughout the Nation. Adherence to this Court's longstanding precedents and analytic framework would have been the proper and prudent way to resolve this case.

The Court has twice held that individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). This is true even when the records contain personal and sensitive information. So when the Government uses a subpoena to obtain, for ***2224** example, bank records, telephone records, and credit card statements from the businesses that create and keep these records, the Government does not engage in a search of the business's customers within the meaning of the Fourth Amendment.

In this case petitioner challenges the Government's right to use compulsory process to obtain a now-common kind of business record: cell-site records held by cell phone service providers. The Government acquired the records through an investigative process enacted by Congress. Upon approval by a neutral magistrate, and based on the Government's duty to show reasonable necessity, it authorizes the disclosure of records and information that are under the control and ownership of the cell phone service provider, not its customer. Petitioner acknowledges that the Government may obtain a wide variety of business records using compulsory process, and he does not ask the Court to revisit its precedents. Yet he argues that, under those same precedents, the Government searched his records when it used court-approved compulsory process to obtain the cell-site information at issue here.

Cell-site records, however, are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process.

The Court today disagrees. It holds for the first time that by using compulsory process to obtain records of a business entity, the Government has not just engaged in an impermissible action, but has conducted a search of the business's customer. The Court further concludes that the search in this case was unreasonable and the Government needed to get a warrant to obtain more than six days of cell-site records.

In concluding that the Government engaged in a search, the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases. In doing so it draws an unprincipled and unworkable line between cell-site records on the one hand and financial and telephonic records on the other. According to today's majority opinion, the Government can acquire a record of

every credit card purchase and phone call a person makes over months or years without upsetting a legitimate expectation of privacy. But, in the Court's view, the Government crosses a constitutional line when it obtains a court's approval to issue a subpoena for more than six days of cell-site records in order to determine whether a person was within several hundred city blocks of a crime scene. That distinction is illogical and will frustrate principled application of the Fourth Amendment in many routine yet vital law enforcement operations.

It is true that the Cyber Age has vast potential both to expand and restrict individual freedoms in dimensions not contemplated in earlier times. See *Packingham v. North Carolina,* 582 U.S. ——, —— – ——, 137 S.Ct. 1730, 1735–1736, 198 L.Ed.2d 273 (2017). For the reasons that follow, however, there is simply no basis here for concluding that the Government interfered with information that the cell phone customer, either from a legal or commonsense standpoint, should have thought the law would deem owned or controlled by him.

I

Before evaluating the question presented it is helpful to understand the nature of cell-site records, how they are commonly ***2225** used by cell phone service providers, and their proper use by law enforcement.

When a cell phone user makes a call, sends a text message or e-mail, or gains access to the Internet, the cell phone establishes a radio connection to an antenna at a nearby cell site. The typical cell site covers a more-or-less circular geographic area around the site. It has three (or sometimes six) separate antennas pointing in different directions. Each provides cell service for a different 120–degree (or 60–degree) sector of the cell site's circular coverage area. So a cell phone activated on the north side of a cell site will connect to a different antenna than a cell phone on the south side.

Cell phone service providers create records each time a cell phone connects to an antenna at a cell site. For a phone call, for example, the provider records the date, time, and duration of the call; the phone numbers making and receiving the call; and, most relevant here, the cell site used to make the call, as well as the specific antenna that made the connection. The cell-site and antenna data points, together with the date and time of connection, are known as cell-site location information, or cell-site records. By linking an individual's cell phone to a particular 120– or 60–degree sector of a cell site's coverage area at a particular time, cell-site records reveal the general location of the cell phone user.

The location information revealed by cell-site records is imprecise, because an individual cell-site sector usually covers a large geographic area. The FBI agent who offered expert testimony about the cell-site records at issue here testified that a cell site in a city reaches between a half mile and two miles in all directions. That means a 60–degree sector covers between approximately one-eighth and two square miles (and a 120–degree sector twice that area). To put that in perspective, in urban areas cell-site records often would reveal the location of a cell phone user within an area covering between around a dozen and several hundred city blocks. In rural areas cell-site records can be up to 40 times more imprecise. By contrast, a Global Positioning System (GPS) can reveal an individual's location within around 15 feet.

Major cell phone service providers keep cell-site records for long periods of time. There is no law requiring them to do so. Instead, providers contract with their customers to collect and keep these records because they are valuable to the providers. Among other things, providers aggregate the records and sell them to third parties along with other information gleaned from cell phone usage. This data can be used, for example, to help a department store determine which of various prospective store locations is likely to get more foot traffic from middle-aged women who live in affluent zip codes. The market for cell phone data is now estimated to be in the billions of dollars. See Brief for Technology Experts as *Amici Curiae* 23.

Cell-site records also can serve an important investigative function, as the facts of this case demonstrate. Petitioner, Timothy Carpenter, along with a rotating group of accomplices, robbed at least six RadioShack and T–Mobile stores at gunpoint over a 2–year period. Five of those robberies occurred in the Detroit area, each crime at least four miles from the last. The sixth took place in Warren, Ohio, over 200 miles from Detroit.

The Government, of course, did not know all of these details in 2011 when it began investigating Carpenter. In April of that year police arrested four of Carpenter's co-conspirators. One of them confessed to committing nine robberies in Michigan and Ohio between December 2010 and March 2011. He identified 15 accomplices who had participated in at ***2226** least one of those robberies; named Carpenter as one of the accomplices; and provided Carpenter's cell phone number to the authorities. The suspect also warned that the other members of the conspiracy planned to commit more armed robberies in the immediate future.

The Government at this point faced a daunting task. Even if it could identify and apprehend the suspects, still it had to link each suspect in this changing criminal gang to specific robberies in order to bring charges and convict. And, of course, it was urgent that the Government take all necessary steps to stop the ongoing and dangerous crime spree.

Cell-site records were uniquely suited to this task. The geographic dispersion of the robberies meant that, if Carpenter's cell phone were within even a dozen to several hundred city blocks of one or more of the stores when the different robberies occurred, there would be powerful circumstantial evidence of his participation; and this would be especially so if his cell phone usually was not located in the sectors near the stores except during the robbery times.

To obtain these records, the Government applied to federal magistrate judges for disclosure orders pursuant to § 2703(d) of the Stored Communications Act. That Act authorizes a magistrate judge to issue an order requiring disclosure of cell-site records if the Government demonstrates "specific and articulable facts showing that there are reasonable grounds to believe" the records "are relevant and material to an ongoing criminal investigation." 18 U.S.C. §§ 2703(d), 2711(3). The full statutory provision is set out in the Appendix, *infra*.

From Carpenter's primary service provider, MetroPCS, the Government obtained records from between December 2010 and April 2011, based on its understanding that nine robberies had occurred in that timeframe. The Government also requested seven days of cell-site records from Sprint, spanning the time around the robbery in Warren, Ohio. It obtained two days of records.

These records confirmed that Carpenter's cell phone was in the general vicinity of four of the nine robberies, including the one in Ohio, at the times those robberies occurred.

II

The first Clause of the Fourth Amendment 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." The customary beginning point in any Fourth Amendment search case is whether the Government's actions constitute a "search" of the defendant's person, house, papers, or effects, within the meaning of the constitutional provision. If so, the next question is whether that search was reasonable.

Here the only question necessary to decide is whether the Government searched anything of Carpenter's when it used compulsory process to obtain cell-site records from Carpenter's cell phone service providers. This Court's decisions in *Miller* and *Smith* dictate that the answer is no, as every Court of Appeals to have considered the question has recognized. See *United States v. Thompson*, 866 F.3d 1149 (C.A.10 2017); *United States v. Graham*, 824 F.3d 421 (C.A.4 2016) (en banc); *United States v. Carpenter*, 819 F.3d 880 (C.A.6 2016); *United States v. Davis*, 785 F.3d 498 (C.A.11 2015) (en banc); *In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600 (C.A.5 2013).

A

Miller and *Smith* hold that individuals lack any protected Fourth Amendment interests ***2227** in records that are possessed, owned, and controlled only by a third party. In *Miller* federal law enforcement officers obtained four months of the defendant's banking records. 425 U.S., at 437–438, 96 S.Ct. 1619. And in *Smith* state police obtained records of the phone numbers dialed from the defendant's home phone. 442 U.S., at 737, 99 S.Ct. 2577. The Court held in both cases that the officers did not search anything belonging to the defendants within the meaning of the Fourth Amendment. The defendants could "assert neither ownership nor possession" of the records because the records were created, owned, and controlled by the companies. *Miller, supra*, at 440, 96 S.Ct. 1619; see *Smith, supra*, at 741, 99 S.Ct. 2577. And the defendants had no reasonable expectation of privacy in information they "voluntarily conveyed to the [companies] and exposed to their employees in the ordinary course of business." *Miller, supra*, at 442, 96 S.Ct. 1619; see *Smith*, 442 U.S., at 744, 99 S.Ct. 2577. Rather, the defendants "assumed the risk that the information would be divulged to police." *Id.*, at 745, 99 S.Ct. 2577.

Miller and *Smith* have been criticized as being based on too narrow a view of reasonable expectations of privacy. See, *e.g.*, Ashdown, The Fourth Amendment and the "Legitimate Expectation of Privacy," 34 Vand. L. Rev. 1289, 1313–1316 (1981). Those criticisms, however, are unwarranted. The principle established in *Miller* and *Smith* is correct for two reasons, the first relating to a defendant's attenuated interest in property owned by another, and the second relating to the safeguards inherent in the use of compulsory process.

First, *Miller* and *Smith* placed necessary limits on the

ability of individuals to assert Fourth Amendment interests in property to which they lack a "requisite connection." *Minnesota v. Carter,* 525 U.S. 83, 99, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (KENNEDY, J., concurring). Fourth Amendment rights, after all, are personal. The Amendment protects "[t]he right of the people to be secure in *their* ... persons, houses, papers, and effects"—not the persons, houses, papers, and effects of others. (Emphasis added.)

The concept of reasonable expectations of privacy, first announced in *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), sought to look beyond the "arcane distinctions developed in property and tort law" in evaluating whether a person has a sufficient connection to the thing or place searched to assert Fourth Amendment interests in it. *Rakas v. Illinois,* 439 U.S. 128, 143, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). Yet "property concepts" are, nonetheless, fundamental "in determining the presence or absence of the privacy interests protected by that Amendment." *Id.,* at 143–144, n. 12, 99 S.Ct. 421. This is so for at least two reasons. First, as a matter of settled expectations from the law of property, individuals often have greater expectations of privacy in things and places that belong to them, not to others. And second, the Fourth Amendment's protections must remain tethered to the text of that Amendment, which, again, protects only a person's own "persons, houses, papers, and effects."

Katz did not abandon reliance on property-based concepts. The Court in *Katz* analogized the phone booth used in that case to a friend's apartment, a taxicab, and a hotel room. 389 U.S., at 352, 359, 88 S.Ct. 507. So when the defendant "shu[t] the door behind him" and "pa[id] the toll," *id.,* at 352, 88 S.Ct. 507, he had a temporary interest in the space and a legitimate expectation that others would not intrude, much like the interest a hotel guest has in a hotel room, ***2228** *Stoner v. California,* 376 U.S. 483, 84 S.Ct. 889, 11 L.Ed.2d 856 (1964), or an overnight guest has in a host's home, *Minnesota v. Olson,* 495 U.S. 91, 110 S.Ct. 1684, 109 L.Ed.2d 85 (1990). The Government intruded on that space when it attached a listening device to the phone booth. *Katz,* 389 U.S., at 348, 88 S.Ct. 507. (And even so, the Court made it clear that the Government's search could have been reasonable had there been judicial approval on a case-specific basis, which, of course, did occur here. *Id.,* at 357–359, 88 S.Ct. 507.)

Miller and *Smith* set forth an important and necessary limitation on the *Katz* framework. They rest upon the commonsense principle that the absence of property law analogues can be dispositive of privacy expectations. The defendants in those cases could expect that the third-party businesses could use the records the companies collected, stored, and classified as their own for any number of business and commercial purposes. The businesses were not bailees or custodians of the records, with a duty to hold the records for the defendants' use. The defendants could make no argument that the records were their own papers or effects. See *Miller, supra,* at 440, 96 S.Ct. 1619 ("the documents subpoenaed here are not respondent's 'private papers' "); *Smith, supra,* at 741, 99 S.Ct. 2577 ("petitioner obviously cannot claim that his 'property' was invaded"). The records were the business entities' records, plain and simple. The defendants had no reason to believe the records were owned or controlled by them and so could not assert a reasonable expectation of privacy in the records.

The second principle supporting *Miller* and *Smith* is the longstanding rule that the Government may use compulsory process to compel persons to disclose documents and other evidence within their possession and control. See *United States v. Nixon,* 418 U.S. 683, 709, 94 S.Ct. 3090, 41 L.Ed.2d 1039 (1974) (it is an "ancient proposition of law" that "the public has a right to every man's evidence" (internal quotation marks and alterations omitted)). A subpoena is different from a warrant in its force and intrusive power. While a warrant allows the Government to enter and seize and make the examination itself, a subpoena simply requires the person to whom it is directed to make the disclosure. A subpoena, moreover, provides the recipient the "opportunity to present objections" before complying, which further mitigates the intrusion. *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186, 195, 66 S.Ct. 494, 90 L.Ed. 614 (1946).

For those reasons this Court has held that a subpoena for records, although a "constructive" search subject to Fourth Amendment constraints, need not comply with the procedures applicable to warrants—even when challenged by the person to whom the records belong. *Id.,* at 202, 208, 66 S.Ct. 494. Rather, a subpoena complies with the Fourth Amendment's reasonableness requirement so long as it is " 'sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.' " *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 415, 104 S.Ct. 769, 78 L.Ed.2d 567 (1984). Persons with no meaningful interests in the records sought by a subpoena, like the defendants in *Miller* and *Smith,* have no rights to object to the records' disclosure—much less to assert that the Government must obtain a warrant to compel disclosure of the records. See *Miller,* 425 U.S., at 444–446, 96 S.Ct. 1619; *SEC v. Jerry T. O'Brien, Inc.,* 467 U.S. 735, 742–743, 104 S.Ct. 2720, 81 L.Ed.2d 615 (1984).

Based on *Miller* and *Smith* and the principles underlying those cases, it is well established that subpoenas may be used to ***2229** obtain a wide variety of records held by businesses, even when the records contain private information. See 2 W. LaFave, Search and Seizure § 4.13 (5th ed. 2012). Credit cards are a prime example. State and federal law enforcement, for instance, often subpoena credit card statements to develop probable cause to prosecute crimes ranging from drug trafficking and distribution to healthcare fraud to tax evasion. See *United States v. Phibbs,* 999 F.2d 1053 (C.A.6 1993) (drug distribution); *McCune v. DOJ,* 592 Fed.Appx. 287 (C.A.5 2014) (healthcare fraud); *United States v. Green,* 305 F.3d 422 (C.A.6 2002) (drug trafficking and tax evasion); see also 12 U.S.C. §§ 3402(4), 3407 (allowing the Government to subpoena financial records if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry"). Subpoenas also may be used to obtain vehicle registration records, hotel records, employment records, and records of utility usage, to name just a few other examples. See 1 LaFave, *supra,* § 2.7(c).

And law enforcement officers are not alone in their reliance on subpoenas to obtain business records for legitimate investigations. Subpoenas also are used for investigatory purposes by state and federal grand juries, see *United States v. Dionisio,* 410 U.S. 1, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973), state and federal administrative agencies, see *Oklahoma Press, supra,* and state and federal legislative bodies, see *McPhaul v. United States,* 364 U.S. 372, 81 S.Ct. 138, 5 L.Ed.2d 136 (1960).

B

Carpenter does not question these traditional investigative practices. And he does not ask the Court to reconsider *Miller* and *Smith.* Carpenter argues only that, under *Miller* and *Smith,* the Government may not use compulsory process to acquire cell-site records from cell phone service providers.

There is no merit in this argument. Cell-site records, like all the examples just discussed, are created, kept, classified, owned, and controlled by cell phone service providers, which aggregate and sell this information to third parties. As in *Miller,* Carpenter can "assert neither ownership nor possession" of the records and has no control over them. 425 U.S., at 440, 96 S.Ct. 1619.

Carpenter argues that he has Fourth Amendment interests in the cell-site records because they are in essence his personal papers by operation of 47 U.S.C. § 222. That statute imposes certain restrictions on how providers may use "customer proprietary network information"—a term that encompasses cell-site records. §§ 222(c), (h)(1)(A). The statute in general prohibits providers from disclosing personally identifiable cell-site records to private third parties. § 222(c)(1). And it allows customers to request cell-site records from the provider. § 222(c)(2).

Carpenter's argument is unpersuasive, however, for § 222 does not grant cell phone customers any meaningful interest in cell-site records. The statute's confidentiality protections may be overridden by the interests of the providers or the Government. The providers may disclose the records "to protect the[ir] rights or property" or to "initiate, render, bill, and collect for telecommunications services." §§ 222(d)(1), (2). They also may disclose the records "as required by law"—which, of course, is how they were disclosed in this case. § 222(c)(1). Nor does the statute provide customers any practical control over the records. Customers do not create the records; they have no say in whether or for how long the records are stored; and they cannot require the records to be modified or destroyed. Even ***2230** their right to request access to the records is limited, for the statute "does not preclude a carrier from being reimbursed by the customers ... for the costs associated with making such disclosures." H.R.Rep. No. 104–204, pt. 1, p. 90 (1995). So in every legal and practical sense the "network information" regulated by § 222 is, under that statute, "proprietary" to the service providers, not Carpenter. The Court does not argue otherwise.

Because Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them. He could expect that a third party—the cell phone service provider—could use the information it collected, stored, and classified as its own for a variety of business and commercial purposes.

All this is not to say that *Miller* and *Smith* are without limits. *Miller* and *Smith* may not apply when the Government obtains the modern-day equivalents of an individual's own "papers" or "effects," even when those papers or effects are held by a third party. See *Ex parte Jackson,* 96 U.S. 727, 733, 24 L.Ed. 877 (1878) (letters held by mail carrier); *United States v. Warshak,* 631 F.3d 266, 283–288 (C.A.6 2010) (e-mails held by Internet service provider). As already discussed, however, this case does not involve property or a bailment of that sort. Here the Government's acquisition of cell-site records falls within the heartland of *Miller* and *Smith.*

In fact, Carpenter's Fourth Amendment objection is even weaker than those of the defendants in *Miller* and *Smith.*

Here the Government did not use a mere subpoena to obtain the cell-site records. It acquired the records only after it proved to a Magistrate Judge reasonable grounds to believe that the records were relevant and material to an ongoing criminal investigation. See 18 U.S.C. § 2703(d). So even if § 222 gave Carpenter some attenuated interest in the records, the Government's conduct here would be reasonable under the standards governing subpoenas. See *Donovan,* 464 U.S., at 415, 104 S.Ct. 769.

Under *Miller* and *Smith,* then, a search of the sort that requires a warrant simply did not occur when the Government used court-approved compulsory process, based on a finding of reasonable necessity, to compel a cell phone service provider, as owner, to disclose cell-site records.

III

The Court rejects a straightforward application of *Miller* and *Smith.* It concludes instead that applying those cases to cell-site records would work a "significant extension" of the principles underlying them, *ante,* at 2219, and holds that the acquisition of more than six days of cell-site records constitutes a search, *ante,* at 2217, n. 3.

In my respectful view the majority opinion misreads this Court's precedents, old and recent, and transforms *Miller* and *Smith* into an unprincipled and unworkable doctrine. The Court's newly conceived constitutional standard will cause confusion; will undermine traditional and important law enforcement practices; and will allow the cell phone to become a protected medium that dangerous persons will use to commit serious crimes.

A

The Court errs at the outset by attempting to sidestep *Miller* and *Smith.* The Court frames this case as following instead from *United States v. Knotts,* 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), and *United States v. Jones,* 565 U.S. 400, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). Those cases, the Court suggests, establish that ***2231** "individuals have a reasonable expectation of privacy in the whole of their physical movements." *Ante,* at 2214 - 2216, 2217.

Knotts held just the opposite: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." 460 U.S., at 281, 103 S.Ct. 1081. True, the Court in *Knotts* also suggested that "different constitutional principles may be applicable" to "dragnet-type law enforcement practices." *Id.,* at 284, 103 S.Ct. 1081. But by dragnet practices the Court was referring to " 'twenty-four hour surveillance of any citizen of this country ... without judicial knowledge or supervision.' " *Id.,* at 283, 103 S.Ct. 1081.

Those "different constitutional principles" mentioned in *Knotts,* whatever they may be, do not apply in this case. Here the Stored Communications Act requires a neutral judicial officer to confirm in each case that the Government has "reasonable grounds to believe" the cell-site records "are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). This judicial check mitigates the Court's concerns about " 'a too permeating police surveillance.' " *Ante,* at 2214 (quoting *United States v. Di Re,* 332 U.S. 581, 595, 68 S.Ct. 222, 92 L.Ed. 210 (1948)). Here, even more so than in *Knotts,* "reality hardly suggests abuse." 460 U.S., at 284, 103 S.Ct. 1081.

The Court's reliance on *Jones* fares no better. In *Jones* the Government installed a GPS tracking device on the defendant's automobile. The Court held the Government searched the automobile because it "physically occupied private property [of the defendant] for the purpose of obtaining information." 565 U.S., at 404, 132 S.Ct. 945. So in *Jones* it was "not necessary to inquire about the target's expectation of privacy in his vehicle's movements." *Grady v. North Carolina,* 575 U.S. ——, ——, 135 S.Ct. 1368, 1370, 191 L.Ed.2d 459 (2015) (*per curiam*).

Despite that clear delineation of the Court's holding in *Jones,* the Court today declares that *Jones* applied the " 'different constitutional principles' " alluded to in *Knotts* to establish that an individual has an expectation of privacy in the sum of his whereabouts. *Ante,* at 2215, 2217 - 2218. For that proposition the majority relies on the two concurring opinions in *Jones,* one of which stated that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring). But *Jones* involved direct governmental surveillance of a defendant's automobile without judicial authorization—specifically, GPS surveillance accurate within 50 to 100 feet. *Id.,* at 402–403, 132 S.Ct. 945. Even assuming that the different constitutional principles mentioned in *Knotts* would apply in a case like *Jones*—a proposition the Court was careful not to announce in *Jones, supra,* at 412–413, 132 S.Ct. 945—those principles are inapplicable here. Cases like this one, where the Government uses court-approved compulsory process to

obtain records owned and controlled by a third party, are governed by the two majority opinions in *Miller* and *Smith*.

B

The Court continues its analysis by misinterpreting *Miller* and *Smith*, and then it reaches the wrong outcome on these facts even under its flawed standard.

The Court appears, in my respectful view, to read *Miller* and *Smith* to establish a balancing test. For each "qualitatively different category" of information, the Court suggests, the privacy interests at stake must be weighed against the fact that the information has been disclosed to a third party. See ***2232** *ante*, at 2216, 2219 - 2220. When the privacy interests are weighty enough to "overcome" the third-party disclosure, the Fourth Amendment's protections apply. See *ante*, at 2220.

That is an untenable reading of *Miller* and *Smith*. As already discussed, the fact that information was relinquished to a third party was the entire basis for concluding that the defendants in those cases lacked a reasonable expectation of privacy. *Miller* and *Smith* do not establish the kind of category-by-category balancing the Court today prescribes.

But suppose the Court were correct to say that *Miller* and *Smith* rest on so imprecise a foundation. Still the Court errs, in my submission, when it concludes that cell-site records implicate greater privacy interests—and thus deserve greater Fourth Amendment protection—than financial records and telephone records.

Indeed, the opposite is true. A person's movements are not particularly private. As the Court recognized in *Knotts*, when the defendant there "traveled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination." 460 U.S., at 281–282, 103 S.Ct. 1081. Today expectations of privacy in one's location are, if anything, even less reasonable than when the Court decided *Knotts* over 30 years ago. Millions of Americans choose to share their location on a daily basis, whether by using a variety of location-based services on their phones, or by sharing their location with friends and the public at large via social media.

And cell-site records, as already discussed, disclose a person's location only in a general area. The records at issue here, for example, revealed Carpenter's location within an area covering between around a dozen and several hundred city blocks. "Areas of this scale might encompass bridal stores and Bass Pro Shops, gay bars and straight ones, a Methodist church and the local mosque." 819 F.3d 880, 889 (C.A.6 2016). These records could not reveal where Carpenter lives and works, much less his " 'familial, political, professional, religious, and sexual associations.' " *Ante*, at 2217 (quoting *Jones*, *supra*, at 415, 132 S.Ct. 945 (SOTOMAYOR, J., concurring)).

By contrast, financial records and telephone records do " 'revea[l] ... personal affairs, opinions, habits and associations.' " *Miller*, 425 U.S., at 451, 96 S.Ct. 1619 (Brennan, J., dissenting); see *Smith*, 442 U.S., at 751, 99 S.Ct. 2577 (Marshall, J., dissenting). What persons purchase and to whom they talk might disclose how much money they make; the political and religious organizations to which they donate; whether they have visited a psychiatrist, plastic surgeon, abortion clinic, or AIDS treatment center; whether they go to gay bars or straight ones; and who are their closest friends and family members. The troves of intimate information the Government can and does obtain using financial records and telephone records dwarfs what can be gathered from cell-site records.

Still, the Court maintains, cell-site records are "unique" because they are "comprehensive" in their reach; allow for retrospective collection; are "easy, cheap, and efficient compared to traditional investigative tools"; and are not exposed to cell phone service providers in a meaningfully voluntary manner. *Ante*, at 2216 - 2218, 2220, 2223. But many other kinds of business records can be so described. Financial records are of vast scope. Banks and credit card companies keep a comprehensive account of almost every transaction an individual makes on a daily basis. "With ***2233** just the click of a button, the Government can access each [company's] deep repository of historical [financial] information at practically no expense." *Ante*, at 2218. And the decision whether to transact with banks and credit card companies is no more or less voluntary than the decision whether to use a cell phone. Today, just as when *Miller* was decided, " 'it is impossible to participate in the economic life of contemporary society without maintaining a bank account.' " 425 U.S., at 451, 96 S.Ct. 1619 (BRENNAN, J., dissenting). But this Court, nevertheless, has held that individuals do not have a reasonable expectation of privacy in financial records.

Perhaps recognizing the difficulty of drawing the constitutional line between cell-site records and financial and telephonic records, the Court posits that the accuracy of cell-site records "is rapidly approaching GPS-level precision." *Ante*, at 2219. That is certainly plausible in the

era of cyber technology, yet the privacy interests associated with location information, which is often disclosed to the public at large, still would not outweigh the privacy interests implicated by financial and telephonic records.

Perhaps more important, those future developments are no basis upon which to resolve this case. In general, the Court "risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." *Ontario v. Quon,* 560 U.S. 746, 759, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010). That judicial caution, prudent in most cases, is imperative in this one.

Technological changes involving cell phones have complex effects on crime and law enforcement. Cell phones make crimes easier to coordinate and conceal, while also providing the Government with new investigative tools that may have the potential to upset traditional privacy expectations. See Kerr, An Equilibrium–Adjustment Theory of the Fourth Amendment, 125 Harv. L. Rev 476, 512–517 (2011). How those competing effects balance against each other, and how property norms and expectations of privacy form around new technology, often will be difficult to determine during periods of rapid technological change. In those instances, and where the governing legal standard is one of reasonableness, it is wise to defer to legislative judgments like the one embodied in § 2703(d) of the Stored Communications Act. See *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring). In § 2703(d) Congress weighed the privacy interests at stake and imposed a judicial check to prevent executive overreach. The Court should be wary of upsetting that legislative balance and erecting constitutional barriers that foreclose further legislative instructions. See *Quon, supra,* at 759, 130 S.Ct. 2619. The last thing the Court should do is incorporate an arbitrary and outside limit—in this case six days' worth of cell-site records—and use it as the foundation for a new constitutional framework. The Court's decision runs roughshod over the mechanism Congress put in place to govern the acquisition of cell-site records and closes off further legislative debate on these issues.

C

The Court says its decision is a "narrow one." *Ante,* at 2220. But its reinterpretation of *Miller* and *Smith* will have dramatic consequences for law enforcement, courts, and society as a whole.

Most immediately, the Court's holding that the Government must get a warrant to obtain more than six days of cell-site records limits the effectiveness of an important investigative tool for solving serious crimes. As this case demonstrates, cell-site records are uniquely suited to help ***2234** the Government develop probable cause to apprehend some of the Nation's most dangerous criminals: serial killers, rapists, arsonists, robbers, and so forth. See also, *e.g., Davis,* 785 F.3d, at 500–501 (armed robbers); Brief for Alabama et al. as *Amici Curiae* 21–22 (serial killer). These records often are indispensable at the initial stages of investigations when the Government lacks the evidence necessary to obtain a warrant. See *United States v. Pembrook,* 876 F.3d 812, 816–819 (C.A.6 2017). And the long-term nature of many serious crimes, including serial crimes and terrorism offenses, can necessitate the use of significantly more than six days of cell-site records. The Court's arbitrary 6–day cutoff has the perverse effect of nullifying Congress' reasonable framework for obtaining cell-site records in some of the most serious criminal investigations.

The Court's decision also will have ramifications that extend beyond cell-site records to other kinds of information held by third parties, yet the Court fails "to provide clear guidance to law enforcement" and courts on key issues raised by its reinterpretation of *Miller* and *Smith. Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2491, 189 L.Ed.2d 430 (2014).

First, the Court's holding is premised on cell-site records being a "distinct category of information" from other business records. *Ante,* at 2219. But the Court does not explain what makes something a distinct category of information. Whether credit card records are distinct from bank records; whether payment records from digital wallet applications are distinct from either; whether the electronic bank records available today are distinct from the paper and microfilm records at issue in *Miller*; or whether cell-phone call records are distinct from the home-phone call records at issue in *Smith,* are just a few of the difficult questions that require answers under the Court's novel conception of *Miller* and *Smith.*

Second, the majority opinion gives courts and law enforcement officers no indication how to determine whether any particular category of information falls on the financial-records side or the cell-site-records side of its newly conceived constitutional line. The Court's multifactor analysis—considering intimacy, comprehensiveness, expense, retrospectivity, and voluntariness—puts the law on a new and unstable foundation.

Third, even if a distinct category of information is deemed to be more like cell-site records than financial records, courts and law enforcement officers will have to guess how much of that information can be requested before a warrant is required. The Court suggests that less than seven days of location information may not require a warrant. See *ante,* at 2217, n. 3; see also *ante,* at 2220 - 2221 (expressing no opinion on "real-time CSLI," tower dumps, and security-camera footage). But the Court does not explain why that is so, and nothing in its opinion even alludes to the considerations that should determine whether greater or lesser thresholds should apply to information like IP addresses or website browsing history.

Fourth, by invalidating the Government's use of court-approved compulsory process in this case, the Court calls into question the subpoena practices of federal and state grand juries, legislatures, and other investigative bodies, as Justice ALITO's opinion explains. See *post,* at 2247 - 2257 (dissenting opinion). Yet the Court fails even to mention the serious consequences this will have for the proper administration of justice.

In short, the Court's new and uncharted course will inhibit law enforcement and "keep defendants and judges guessing for years to come." ***2235** *Riley,* 573 U.S., at ——, 134 S.Ct., at 2493 (internal quotation marks omitted).

* * *

This case should be resolved by interpreting accepted property principles as the baseline for reasonable expectations of privacy. Here the Government did not search anything over which Carpenter could assert ownership or control. Instead, it issued a court-authorized subpoena to a third party to disclose information it alone owned and controlled. That should suffice to resolve this case.

Having concluded, however, that the Government searched Carpenter when it obtained cell-site records from his cell phone service providers, the proper resolution of this case should have been to remand for the Court of Appeals to determine in the first instance whether the search was reasonable. Most courts of appeals, believing themselves bound by *Miller* and *Smith,* have not grappled with this question. And the Court's reflexive imposition of the warrant requirement obscures important and difficult issues, such as the scope of Congress' power to authorize the Government to collect new forms of information using processes that deviate from traditional warrant procedures, and how the Fourth Amendment's reasonableness requirement should apply when the Government uses compulsory process instead of engaging in an actual, physical search.

These reasons all lead to this respectful dissent.

APPENDIX

"§ 2703. Required disclosure of customer communications or records
"(d) REQUIREMENTS FOR COURT ORDER.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity 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. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider."

Justice THOMAS, dissenting.

This case should not turn on "whether" a search occurred. *Ante,* at 2223 - 2224. It should turn, instead, on *whose* property was searched. The Fourth Amendment guarantees individuals the right to be secure from unreasonable searches of "*their* persons, houses, papers, and effects." (Emphasis added.) In other words, "*each* person has the right to be secure against unreasonable searches ... in *his own* person, house, papers, and effects." *Minnesota v. Carter,* 525 U.S. 83, 92, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (Scalia, J., concurring). By obtaining the cell-site records of MetroPCS and Sprint, the Government did not search Carpenter's property. He did not create the records, he does not maintain them, he cannot control them, and he cannot destroy them. Neither the terms of his contracts nor any provision of law makes the records his. The records belong to MetroPCS and Sprint.

The Court concludes that, although the records are not Carpenter's, the Government must get a warrant because Carpenter had a reasonable "expectation of privacy"

***2236** in the location information that they reveal. *Ante,* at 2216 - 2217. I agree with Justice KENNEDY, Justice ALITO, Justice GORSUCH, and every Court of Appeals to consider the question that this is not the best reading of our precedents.

The more fundamental problem with the Court's opinion, however, is its use of the "reasonable expectation of privacy" test, which was first articulated by Justice Harlan in *Katz v. United States,* 389 U.S. 347, 360–361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (concurring opinion). The *Katz* test has no basis in the text or history of the Fourth Amendment. And, it invites courts to make judgments about policy, not law. Until we confront the problems with this test, *Katz* will continue to distort Fourth Amendment jurisprudence. I respectfully dissent.

I

Katz was the culmination of a series of decisions applying the Fourth Amendment to electronic eavesdropping. The first such decision was *Olmstead v. United States,* 277 U.S. 438, 48 S.Ct. 564, 72 L.Ed. 944 (1928), where federal officers had intercepted the defendants' conversations by tapping telephone lines near their homes. *Id.,* at 456–457, 48 S.Ct. 564. In an opinion by Chief Justice Taft, the Court concluded that this wiretap did not violate the Fourth Amendment. No "search" occurred, according to the Court, because the officers did not physically enter the defendants' homes. *Id.,* at 464–466, 48 S.Ct. 564. And neither the telephone lines nor the defendants' intangible conversations qualified as "persons, houses, papers, [or] effects" within the meaning of the Fourth Amendment. *Ibid.*[1] In the ensuing decades, this Court adhered to *Olmstead* and rejected Fourth Amendment challenges to various methods of electronic surveillance. See *On Lee v. United States,* 343 U.S. 747, 749–753, 72 S.Ct. 967, 96 L.Ed. 1270 (1952) (use of microphone to overhear conversations with confidential informant); *Goldman v. United States,* 316 U.S. 129, 131–132, 135–136, 62 S.Ct. 993, 86 L.Ed. 1322 (1942) (use of detectaphone to hear conversations in office next door).

In the 1960's, however, the Court began to retreat from *Olmstead.* In *Silverman v. United States,* 365 U.S. 505, 81 S.Ct. 679, 5 L.Ed.2d 734 (1961), for example, federal officers had eavesdropped on the defendants by driving a "spike mike" several inches into the house they were occupying. *Id.,* at 506–507, 81 S.Ct. 679. This was a "search," the Court held, because the "unauthorized physical penetration into the premises" was an "actual intrusion into a constitutionally protected area." *Id.,* at 509, 512, 81 S.Ct. 679. The Court did not mention *Olmstead* 's other holding that intangible conversations are not "persons, houses, papers, [or] effects." That omission was significant. The Court confirmed two years later that "[i]t follows from [*Silverman*] that the Fourth Amendment may protect against the overhearing of verbal statements as well as against the more traditional seizure of 'papers and effects.' " *Wong Sun v. United States,* 371 U.S. 471, 485, 83 S.Ct. 407, 9 L.Ed.2d 441 (1963); accord, ***2237** *Berger v. New York,* 388 U.S. 41, 51, 87 S.Ct. 1873, 18 L.Ed.2d 1040 (1967).

In *Katz,* the Court rejected *Olmstead* 's remaining holding—that eavesdropping is not a search absent a physical intrusion into a constitutionally protected area. The federal officers in *Katz* had intercepted the defendant's conversations by attaching an electronic device to the outside of a public telephone booth. 389 U.S., at 348, 88 S.Ct. 507. The Court concluded that this was a "search" because the officers "violated the privacy upon which [the defendant] justifiably relied while using the telephone booth." *Id.,* at 353, 88 S.Ct. 507. Although the device did not physically penetrate the booth, the Court overruled *Olmstead* and held that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion." 389 U.S., at 353, 88 S.Ct. 507. The Court did not explain what should replace *Olmstead* 's physical-intrusion requirement. It simply asserted that "the Fourth Amendment protects people, not places" and "what [a person] seeks to preserve as private ... may be constitutionally protected." 389 U.S., at 351, 88 S.Ct. 507.

Justice Harlan's concurrence in *Katz* attempted to articulate the standard that was missing from the majority opinion. While Justice Harlan agreed that " 'the Fourth Amendment protects people, not places,' " he stressed that "[t]he question ... is what protection it affords to those people," and "the answer ... requires reference to a 'place.' " *Id.,* at 361, 88 S.Ct. 507. Justice Harlan identified a "twofold requirement" to determine when the protections of the Fourth Amendment apply: "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' " *Ibid.*

Justice Harlan did not cite anything for this "expectation of privacy" test, and the parties did not discuss it in their briefs. The test appears to have been presented for the first time at oral argument by one of the defendant's lawyers. See Winn, *Katz* and the Origins of the "Reasonable Expectation of Privacy" Test, 40 McGeorge L. Rev. 1, 9–10 (2009). The lawyer, a recent law-school graduate, apparently had an "[e]piphany" while preparing

for oral argument. Schneider, *Katz v. United States*: The Untold Story, 40 McGeorge L. Rev. 13, 18 (2009). He conjectured that, like the "reasonable person" test from his Torts class, the Fourth Amendment should turn on "whether a reasonable person ... could have expected his communication to be private." *Id.*, at 19. The lawyer presented his new theory to the Court at oral argument. See, *e.g.*, Tr. of Oral Arg. in *Katz v. United States*, O.T. 1967, No. 35, p. 5 (proposing a test of "whether or not, objectively speaking, the communication was intended to be private"); *id.*, at 11 ("We propose a test using a way that's not too dissimilar from the tort 'reasonable man' test"). After some questioning from the Justices, the lawyer conceded that his test should also require individuals to subjectively expect privacy. See *id.*, at 12. With that modification, Justice Harlan seemed to accept the lawyer's test almost verbatim in his concurrence.

Although the majority opinion in *Katz* had little practical significance after Congress enacted the Omnibus Crime Control and Safe Streets Act of 1968, Justice Harlan's concurrence profoundly changed our Fourth Amendment jurisprudence. It took only one year for the full Court to adopt his two-pronged test. See *Terry v. Ohio*, 392 U.S. 1, 10, 88 S.Ct. 1868, 20 L.Ed.2d 889 (1968). And by 1979, the Court was describing Justice Harlan's test as the "lodestar" for determining whether ***2238** a "search" had occurred. *Smith v. Maryland*, 442 U.S. 735, 739, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). Over time, the Court minimized the subjective prong of Justice Harlan's test. See Kerr, *Katz* Has Only One Step: The Irrelevance of Subjective Expectations, 82 U. Chi. L. Rev. 113 (2015). That left the objective prong—the "reasonable expectation of privacy" test that the Court still applies today. See *ante*, at 2213 - 2214; *United States v. Jones*, 565 U.S. 400, 406, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012).

II

Under the *Katz* test, a "search" occurs whenever "government officers violate a person's 'reasonable expectation of privacy.' " *Jones, supra*, at 406, 132 S.Ct. 945. The most glaring problem with this test is that it has "no plausible foundation in the text of the Fourth Amendment." *Carter*, 525 U.S., at 97, 119 S.Ct. 469 (opinion of Scalia, J.). The Fourth Amendment, as relevant here, protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches." By defining "search" to mean "any violation of a reasonable expectation of privacy," the *Katz* test misconstrues virtually every one of these words.

A

The *Katz* test distorts the original meaning of "searc[h]"—the word in the Fourth Amendment that it purports to define, see *ante*, at 2213 - 2214; *Smith, supra*. Under the *Katz* test, the government conducts a search anytime it violates someone's "reasonable expectation of privacy." That is not a normal definition of the word "search."

At the founding, "search" did not mean a violation of someone's reasonable expectation of privacy. The word was probably not a term of art, as it does not appear in legal dictionaries from the era. And its ordinary meaning was the same as it is today: " '[t]o look over or through for the purpose of finding something; to explore; to examine by inspection; as, to *search* the house for a book; to *search* the wood for a thief.' " *Kyllo v. United States*, 533 U.S. 27, 32, n. 1, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (quoting N. Webster, An American Dictionary of the English Language 66 (1828) (reprint 6th ed. 1989)); accord, 2 S. Johnson, A Dictionary of the English Language (5th ed. 1773) ("Inquiry by looking into every suspected place"); N. Bailey, An Universal Etymological English Dictionary (22d ed. 1770) ("a seeking after, a looking for, & c."); 2 J. Ash, The New and Complete Dictionary of the English Language (2d ed. 1795) ("An enquiry, an examination, the act of seeking, an enquiry by looking into every suspected place; a quest; a pursuit"); T. Sheridan, A Complete Dictionary of the English Language (6th ed. 1796) (similar). The word "search" was not associated with "reasonable expectation of privacy" until Justice Harlan coined that phrase in 1967. The phrase "expectation(s) of privacy" does not appear in the pre-*Katz* federal or state case reporters, the papers of prominent Founders,[2] early congressional documents and debates,[3] collections of early American English texts,[4] or early American newspapers. ***2239** [5]

B

The *Katz* test strays even further from the text by focusing on the concept of "privacy." The word "privacy" does not appear in the Fourth Amendment (or anywhere else in the Constitution for that matter). Instead, the Fourth Amendment references "[t]he right of the people to be secure." It then qualifies that right by limiting it to "persons" and three specific types of property: "houses, papers, and effects." By connecting the right to be secure to these four specific objects, "[t]he text of the Fourth

Amendment reflects its close connection to property." *Jones, supra,* at 405, 132 S.Ct. 945. "[P]rivacy," by contrast, "was not part of the political vocabulary of the [founding]. Instead, liberty and privacy rights were understood largely in terms of property rights." Cloud, Property Is Privacy: Locke and Brandeis in the Twenty–First Century, 55 Am. Crim. L. Rev. 37, 42 (2018).

Those who ratified the Fourth Amendment were quite familiar with the notion of security in property. Security in property was a prominent concept in English law. See, *e.g.,* 3 W. Blackstone, Commentaries on the Laws of England 288 (1768) ("[E]very man's house is looked upon by the law to be his castle"); 3 E. Coke, Institutes of Laws of England 162 (6th ed. 1680) ("[F]or a man[']s house is his Castle, & domus sua cuique est tutissimum refugium [each man's home is his safest refuge]"). The political philosophy of John Locke, moreover, "permeated the 18th-century political scene in America." *Obergefell v. Hodges,* 576 U.S. ——, ——, 135 S.Ct. 2584, 2634, 192 L.Ed.2d 609 (2015) (THOMAS, J., dissenting). For Locke, every individual had a property right "in his own person" and in anything he "removed from the common state [of] Nature" and "mixed his labour with." Second Treatise of Civil Government § 27 (1690). Because property is "very unsecure" in the state of nature, § 123, individuals form governments to obtain "a secure enjoyment of their properties." § 95. Once a government is formed, however, it cannot be given "a power to destroy that which every one designs to secure"; it cannot legitimately "endeavour to take away, and destroy the property of the people," or exercise "an absolute power over [their] lives, liberties, and estates." § 222.

The concept of security in property recognized by Locke and the English legal tradition appeared throughout the materials that inspired the Fourth Amendment. In *Entick v. Carrington,* 19 How. St. Tr. 1029 (C.P. 1765)—a heralded decision that the founding generation considered "the true and ultimate expression of constitutional law," *Boyd v. United States,* 116 U.S. 616, 626, 6 S.Ct. 524, 29 L.Ed. 746 (1886)—Lord Camden explained that "[t]he great end, for which men entered into society, was to secure their property." 19 How. St. Tr., at 1066. The American colonists echoed this reasoning in their "widespread hostility" to the Crown's writs of assistance[6]—a practice that inspired the Revolution and became "[t]he driving force behind the adoption of the [Fourth] Amendment." ***2240** *United States v. Verdugo–Urquidez,* 494 U.S. 259, 266, 110 S.Ct. 1056, 108 L.Ed.2d 222 (1990). Prominent colonists decried the writs as destroying " 'domestic security' " by permitting broad searches of homes. M. Smith, The Writs of Assistance Case 475 (1978) (quoting a 1772 Boston town meeting); see also *id.,* at 562 (complaining that " 'every householder in this province, will necessarily become *less secure* than he was before this writ' " (quoting a 1762 article in the Boston Gazette)); *id.,* at 493 (complaining that the writs were " 'expressly contrary to the common law, which ever regarded a man's *house* as his castle, or a place of perfect security' " (quoting a 1768 letter from John Dickinson)). John Otis, who argued the famous Writs of Assistance case, contended that the writs violated " 'the fundamental Principl[e] of Law' " that " '[a] Man who is quiet, is as secure in his House, as a Prince in his Castle.' " *Id.,* at 339 (quoting John Adam's notes). John Adams attended Otis' argument and later drafted Article XIV of the Massachusetts Constitution,[7] which served as a model for the Fourth Amendment. See Clancy, The Framers' Intent: John Adams, His Era, and the Fourth Amendment, 86 Ind. L.J. 979, 982 (2011); Donahue, The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181, 1269 (2016) (Donahue). Adams agreed that "[p]roperty must be secured, or liberty cannot exist." Discourse on Davila, in 6 The Works of John Adams 280 (C. Adams ed. 1851).

Of course, the founding generation understood that, by securing their property, the Fourth Amendment would often protect their privacy as well. See, *e.g., Boyd, supra,* at 630, 6 S.Ct. 524 (explaining that searches of houses invade "the privacies of life"); *Wilkes v. Wood,* 19 How. St. Tr. 1153, 1154 (C.P. 1763) (argument of counsel contending that seizures of papers implicate "our most private concerns"). But the Fourth Amendment's attendant protection of privacy does not justify *Katz* 's elevation of privacy as the *sine qua non* of the Amendment. See T. Clancy, The Fourth Amendment: Its History and Interpretation § 3.4.4, p. 78 (2008) ("[The *Katz* test] confuse[s] the reasons for exercising the protected right with the right itself. A purpose of exercising one's Fourth Amendment rights might be the desire for privacy, but the individual's motivation is not the right protected"); cf. *United States v. Gonzalez–Lopez,* 548 U.S. 140, 145, 126 S.Ct. 2557, 165 L.Ed.2d 409 (2006) (rejecting "a line of reasoning that 'abstracts from the right to its purposes, and then eliminates the right' "). As the majority opinion in *Katz* recognized, the Fourth Amendment "cannot be translated into a general constitutional 'right to privacy,' " as its protections "often have nothing to do with privacy at all." 389 U.S., at 350, 88 S.Ct. 507. Justice Harlan's focus on privacy in his concurrence—an opinion that was issued between *Griswold v. Connecticut,* 381 U.S. 479, 85 S.Ct. 1678, 14 L.Ed.2d 510 (1965), and *Roe v. Wade,* 410 U.S. 113, 93 S.Ct. 705, 35 L.Ed.2d 147 (1973)—reflects privacy's status as the organizing constitutional idea of the 1960's

and 1970's. The organizing constitutional idea of the founding era, by contrast, was property.

***2241** C

In shifting the focus of the Fourth Amendment from property to privacy, the *Katz* test also reads the words "persons, houses, papers, and effects" out of the text. At its broadest formulation, the *Katz* test would find a search "*wherever* an individual may harbor a reasonable 'expectation of privacy.' " *Terry,* 392 U.S., at 9, 88 S.Ct. 1868 (emphasis added). The Court today, for example, does not ask whether cell-site location records are "persons, houses, papers, [or] effects" within the meaning of the Fourth Amendment.[8] Yet "persons, houses, papers, and effects" cannot mean "anywhere" or "anything." *Katz* 's catchphrase that "the Fourth Amendment protects people, not places," is not a serious attempt to reconcile the constitutional text. See *Carter,* 525 U.S., at 98, n. 3, 119 S.Ct. 469 (opinion of Scalia, J.). The Fourth Amendment obviously protects people; "[t]he question ... is what protection it affords to those people." *Katz,* 389 U.S., at 361, 88 S.Ct. 507 (Harlan, J., concurring). The Founders decided to protect the people from unreasonable searches and seizures of four specific things—persons, houses, papers, and effects. They identified those four categories as "the objects of privacy protection to which the *Constitution* would extend, leaving further expansion to the good judgment ... of the people through their representatives in the legislature." *Carter, supra,* at 97–98, 119 S.Ct. 469 (opinion of Scalia, J.).

This limiting language was important to the founders. Madison's first draft of the Fourth Amendment used a different phrase: "their persons, their houses, their papers, and their *other property*." 1 Annals of Cong. 452 (1789) (emphasis added). In one of the few changes made to Madison's draft, the House Committee of Eleven changed "other property" to "effects." See House Committee of Eleven Report (July 28, 1789), in N. Cogan, The Complete Bill of Rights 334 (2d ed. 2015). This change might have narrowed the Fourth Amendment by clarifying that it does not protect real property (other than houses). See *Oliver v. United States,* 466 U.S. 170, 177, and n. 7, 104 S.Ct. 1735, 80 L.Ed.2d 214 (1984); Davies, Recovering the Original Fourth Amendment, 98 Mich. L. Rev. 547, 709–714 (1999) (Davies). Or the change might have broadened the Fourth Amendment by clarifying that it protects commercial goods, not just personal possessions. See Donahue 1301. Or it might have done both. Whatever its ultimate effect, the change reveals that the Founders understood the phrase "persons, houses, papers, and effects" to be an important measure of the Fourth Amendment's overall scope. See Davies 710. The *Katz* test, however, displaces and renders that phrase entirely "superfluous." *Jones,* 565 U.S., at 405, 132 S.Ct. 945.

D

"[P]ersons, houses, papers, and effects" are not the only words that the *Katz* test reads out of the Fourth Amendment. The Fourth Amendment specifies that the people have a right to be secure from unreasonable searches of "their" persons, houses, papers, and effects. Although phrased in the plural, "[t]he obvious meaning of ['their'] is that *each* person has the right to be secure against unreasonable searches ***2242** and seizures in *his own* person, house, papers, and effects." *Carter, supra,* at 92, 119 S.Ct. 469 (opinion of Scalia, J.); see also *District of Columbia v. Heller,* 554 U.S. 570, 579, 128 S.Ct. 2783, 171 L.Ed.2d 637 (2008) (explaining that the Constitution uses the plural phrase "the people" to "refer to individual rights, not 'collective' rights"). Stated differently, the word "their" means, at the very least, that individuals do not have Fourth Amendment rights in *someone else's* property. See *Carter, supra,* at 92–94, 119 S.Ct. 469 (opinion of Scalia, J.). Yet, under the *Katz* test, individuals can have a reasonable expectation of privacy in another person's property. See, *e.g., Carter,* 525 U.S., at 89, 119 S.Ct. 469 (majority opinion) ("[A] person may have a legitimate expectation of privacy in the house of someone else"). Until today, our precedents have not acknowledged that individuals can claim a reasonable expectation of privacy in someone else's business records. See *ante,* at 2224 (KENNEDY, J., dissenting). But the Court erases that line in this case, at least for cell-site location records. In doing so, it confirms that the *Katz* test does not necessarily require an individual to prove that the government searched *his* person, house, paper, or effect.

Carpenter attempts to argue that the cell-site records are, in fact, his "papers," see Brief for Petitioner 32–35; Reply Brief 14–15, but his arguments are unpersuasive, see *ante,* at 2229 - 2230 (opinion of KENNEDY, J.); *post,* at 2257 - 2259 (ALITO, J., dissenting). Carpenter stipulated below that the cell-site records are the business records of Sprint and MetroPCS. See App. 51. He cites no property law in his briefs to this Court, and he does not explain how he has a property right in the companies' records under the law of any jurisdiction at any point in American history. If someone stole these records from Sprint or MetroPCS, Carpenter does not argue that he could recover in a traditional tort action. Nor do his contracts with Sprint and MetroPCS make the records his, even though such

provisions could exist in the marketplace. Cf., *e.g.*, Google Terms of Service, https://policies.google.com/terms ("Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours").

Instead of property, tort, or contract law, Carpenter relies on the federal Telecommunications Act of 1996 to demonstrate that the cell site records are his papers. The Telecommunications Act generally bars cell-phone companies from disclosing customers' cell site location information to the public. See 47 U.S.C. § 222(c). This is sufficient to make the records his, Carpenter argues, because the Fourth Amendment merely requires him to identify a source of "positive law" that "protects against access by the public without consent." Brief for Petitioner 32–33 (citing Baude & Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1825–1826 (2016); emphasis deleted).

Carpenter is mistaken. To come within the text of the Fourth Amendment, Carpenter must prove that the cell-site records are *his* ; positive law is potentially relevant only insofar as it answers that question. The text of the Fourth Amendment cannot plausibly be read to mean "any violation of positive law" any more than it can plausibly be read to mean "any violation of a reasonable expectation of privacy."

Thus, the Telecommunications Act is insufficient because it does not give Carpenter a property right in the cell-site records. Section 222, titled "Privacy of customer ***2243** information," protects customers' privacy by preventing cell-phone companies from disclosing sensitive information about them. The statute creates a "duty to protect the confidentiality" of information relating to customers, § 222(a), and creates "[p]rivacy requirements" that limit the disclosure of that information, § 222(c)(1). Nothing in the text pre-empts state property law or gives customers a property interest in the companies' business records (assuming Congress even has that authority).[9] Although § 222 "protects the interests of individuals against wrongful uses or disclosures of personal data, the rationale for these legal protections has not historically been grounded on a perception that people have property rights in personal data as such." Samuelson, Privacy as Intellectual Property? 52 Stan. L. Rev. 1125, 1130–1131 (2000) (footnote omitted). Any property rights remain with the companies.

The *Katz* test comes closer to the text of the Fourth Amendment when it asks whether an expectation of privacy is "reasonable," but it ultimately distorts that term as well. The Fourth Amendment forbids "unreasonable searches." In other words, reasonableness determines the legality of a search, not "whether a search ... within the meaning of the Constitution has *occurred*." *Carter*, 525 U.S., at 97, 119 S.Ct. 469 (opinion of Scalia, J.) (internal quotation marks omitted).

Moreover, the *Katz* test invokes the concept of reasonableness in a way that would be foreign to the ratifiers of the Fourth Amendment. Originally, the word "unreasonable" in the Fourth Amendment likely meant "against reason"—as in "against the reason of the common law." See Donahue 1270–1275; Davies 686–693; *California v. Acevedo*, 500 U.S. 565, 583, 111 S.Ct. 1982, 114 L.Ed.2d 619 (1991) (Scalia, J., concurring in judgment). At the founding, searches and seizures were regulated by a robust body of common-law rules. See generally W. Cuddihy, The Fourth Amendment: Origins and Original Meaning 602–1791 (2009); *e.g.*, *Wilson v. Arkansas*, 514 U.S. 927, 931–936, 115 S.Ct. 1914, 131 L.Ed.2d 976 (1995) (discussing the common-law knock-and-announce rule). The search-and-seizure practices that the Founders feared most—such as general warrants—were already illegal under the common law, and jurists such as Lord Coke described violations of the common law as "against reason." See Donahue 1270–1271, and n. 513. Locke, Blackstone, Adams, and other influential figures shortened the phrase "against reason" to "unreasonable." See *id.*, at 1270–1275. Thus, by prohibiting "unreasonable" searches and seizures in the Fourth Amendment, the Founders ensured that the newly created Congress could not use legislation to abolish the established common-law rules of search and seizure. See T. Cooley, Constitutional Limitations *303 (2d ed. 1871); 3 J. Story, Commentaries on the ***2244** Constitution of the United States § 1895, p. 748 (1833).

Although the Court today maintains that its decision is based on "Founding-era understandings," *ante*, at 2214, the Founders would be puzzled by the Court's conclusion as well as its reasoning. The Court holds that the Government unreasonably searched Carpenter by subpoenaing the cell-site records of Sprint and MetroPCS without a warrant. But the Founders would not recognize the Court's "warrant requirement." *Ante*, at 2222. The common law required warrants for some types of searches and seizures, but not for many others. The relevant rule depended on context. See *Acevedo*, *supra*, at 583–584, 111 S.Ct. 1982 (opinion of Scalia, J.); Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 763–770 (1994); Davies 738–739. In cases like this one, a

E

subpoena for third-party documents was not a "search" to begin with, and the common law did not limit the government's authority to subpoena third parties. See *post,* at 2247 - 2253 (ALITO, J., dissenting). Suffice it to say, the Founders would be confused by this Court's transformation of their common-law protection of property into a "warrant requirement" and a vague inquiry into "reasonable expectations of privacy."

III

That the *Katz* test departs so far from the text of the Fourth Amendment is reason enough to reject it. But the *Katz* test also has proved unworkable in practice. Jurists and commentators tasked with deciphering our jurisprudence have described the *Katz* regime as "an unpredictable jumble," "a mass of contradictions and obscurities," "all over the map," "riddled with inconsistency and incoherence," "a series of inconsistent and bizarre results that [the Court] has left entirely undefended," "unstable," "chameleon-like," " 'notoriously unhelpful,' " "a conclusion rather than a starting point for analysis," "distressingly unmanageable," "a dismal failure," "flawed to the core," "unadorned fiat," and "inspired by the kind of logic that produced Rube Goldberg's bizarre contraptions."[10] Even Justice Harlan, four years after penning his concurrence in *Katz,* confessed that the test encouraged "the substitution of words for analysis." *United States v. White,* 401 U.S. 745, 786, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971) (dissenting opinion).

***2245** After 50 years, it is still unclear what question the *Katz* test is even asking. This Court has steadfastly declined to elaborate the relevant considerations or identify any meaningful constraints. See, *e.g., ante,* at 2213 - 2214 ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection"); *O'Connor v. Ortega,* 480 U.S. 709, 715, 107 S.Ct. 1492, 94 L.Ed.2d 714 (1987) (plurality opinion) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable"); *Oliver,* 466 U.S., at 177, 104 S.Ct. 1735 ("No single factor determines whether an individual legitimately may claim under the Fourth Amendment that a place should be free of government intrusion").

Justice Harlan's original formulation of the *Katz* test appears to ask a descriptive question: Whether a given expectation of privacy is "one that society is prepared to recognize as 'reasonable.' " 389 U.S., at 361, 88 S.Ct. 507. As written, the *Katz* test turns on society's actual, current views about the reasonableness of various expectations of privacy.

But this descriptive understanding presents several problems. For starters, it is easily circumvented. If, for example, "the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," individuals could not realistically expect privacy in their homes. *Smith,* 442 U.S., at 740, n. 5, 99 S.Ct. 2577; see also Chemerinsky, Rediscovering Brandeis's Right to Privacy, 45 Brandeis L.J. 643, 650 (2007) ("[Under *Katz,* t]he government seemingly can deny privacy just by letting people know in advance not to expect any"). A purely descriptive understanding of the *Katz* test also risks "circular[ity]." *Kyllo,* 533 U.S., at 34, 121 S.Ct. 2038. While this Court is supposed to base its decisions on society's expectations of privacy, society's expectations of privacy are, in turn, shaped by this Court's decisions. See Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 S.Ct. Rev. 173, 188 ("[W]hether [a person] will or will not have [a reasonable] expectation [of privacy] will depend on what the legal rule is").

To address this circularity problem, the Court has insisted that expectations of privacy must come from outside its Fourth Amendment precedents, "either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *Rakas v. Illinois,* 439 U.S. 128, 144, n. 12, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978). But the Court's supposed reliance on "real or personal property law" rings hollow. The whole point of *Katz* was to " 'discredi[t]' " the relationship between the Fourth Amendment and property law, 389 U.S., at 353, 88 S.Ct. 507, and this Court has repeatedly downplayed the importance of property law under the *Katz* test, see, *e.g., United States v. Salvucci,* 448 U.S. 83, 91, 100 S.Ct. 2547, 65 L.Ed.2d 619 (1980) ("[P]roperty rights are neither the beginning nor the end of this Court's inquiry [under *Katz*]"); *Rawlings v. Kentucky,* 448 U.S. 98, 105, 100 S.Ct. 2556, 65 L.Ed.2d 633 (1980) ("[This Court has] emphatically rejected the notion that 'arcane' concepts of property law ought to control the ability to claim the protections of the Fourth Amendment"). Today, for example, the Court makes no mention of property law, except to reject its relevance. See *ante,* at 2214, and n. 1.

As for "understandings that are recognized or permitted in society," this Court has never answered even the most basic questions about what this means. See Kerr, ***2246** Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 504–505 (2007). For example, our precedents do not explain who is included in "society," how we know what they "recogniz[e] or permi[t]," and

how much of society must agree before something constitutes an "understanding."

Here, for example, society might prefer a balanced regime that prohibits the Government from obtaining cell-site location information unless it can persuade a neutral magistrate that the information bears on an ongoing criminal investigation. That is precisely the regime Congress created under the Stored Communications Act and Telecommunications Act. See 47 U.S.C. § 222(c)(1); 18 U.S.C. §§ 2703(c)(1)(B), (d). With no sense of irony, the Court invalidates this regime today—the one that society actually created "in the form of its elected representatives in Congress." 819 F.3d 880, 890 (2016).

Truth be told, this Court does not treat the *Katz* test as a descriptive inquiry. Although the *Katz* test is phrased in descriptive terms about society's views, this Court treats it like a normative question—whether a particular practice *should* be considered a search under the Fourth Amendment. Justice Harlan thought this was the best way to understand his test. See *White,* 401 U.S., at 786, 91 S.Ct. 1122 (dissenting opinion) (explaining that courts must assess the "desirability" of privacy expectations and ask whether courts "should" recognize them by "balanc[ing]" the "impact on the individual's sense of security ... against the utility of the conduct as a technique of law enforcement"). And a normative understanding is the only way to make sense of this Court's precedents, which bear the hallmarks of subjective policymaking instead of neutral legal decisionmaking. "[T]he only thing the past three decades have established about the *Katz* test" is that society's expectations of privacy "bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable." *Carter,* 525 U.S., at 97, 119 S.Ct. 469 (opinion of Scalia, J.). Yet, "[t]hough we know ourselves to be eminently reasonable, self-awareness of eminent reasonableness is not really a substitute for democratic election." *Sosa v. Alvarez–Machain,* 542 U.S. 692, 750, 124 S.Ct. 2739, 159 L.Ed.2d 718 (2004) (Scalia, J., concurring in part and concurring in judgment).

* * *

In several recent decisions, this Court has declined to apply the *Katz* test because it threatened to narrow the original scope of the Fourth Amendment. See *Grady v. North Carolina,* 575 U.S. ——, ——, 135 S.Ct. 1368, 1370, 191 L.Ed.2d 459 (2015) (*per curiam*); *Florida v. Jardines,* 569 U.S. 1, 5, 133 S.Ct. 1409, 185 L.Ed.2d 495 (2013); *Jones,* 565 U.S., at 406–407, 132 S.Ct. 945. But as today's decision demonstrates, *Katz* can also be invoked to expand the Fourth Amendment beyond its original scope. This Court should not tolerate errors in either direction. "The People, through ratification, have already weighed the policy tradeoffs that constitutional rights entail." *Luis v. United States,* 578 U.S. ——, ——, 136 S.Ct. 1083, 1101, 194 L.Ed.2d 256 (2016) (THOMAS, J., concurring in judgment). Whether the rights they ratified are too broad or too narrow by modern lights, this Court has no authority to unilaterally alter the document they approved.

Because the *Katz* test is a failed experiment, this Court is dutybound to reconsider it. Until it does, I agree with my dissenting colleagues' reading of our precedents. Accordingly, I respectfully dissent.

Justice ALITO, with whom Justice THOMAS joins, dissenting.

I share the Court's concern about the effect of new technology on personal privacy, ***2247** but I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely.

First, the Court ignores the basic distinction between an actual search (dispatching law enforcement officers to enter private premises and root through private papers and effects) and an order merely requiring a party to look through its own records and produce specified documents. The former, which intrudes on personal privacy far more deeply, requires probable cause; the latter does not. Treating an order to produce like an actual search, as today's decision does, is revolutionary. It violates both the original understanding of the Fourth Amendment and more than a century of Supreme Court precedent. Unless it is somehow restricted to the particular situation in the present case, the Court's move will cause upheaval. Must every grand jury subpoena *duces tecum* be supported by probable cause? If so, investigations of terrorism, political corruption, white-collar crime, and many other offenses will be stymied. And what about subpoenas and other document-production orders issued by administrative agencies? See, *e.g.,* 15 U.S.C. § 57b–1(c) (Federal Trade Commission); §§ 77s(c), 78u(a)-(b) (Securities and Exchange Commission); 29 U.S.C. § 657(b) (Occupational Safety and Health Administration); 29 C.F.R. § 1601.16(a)(2) (2017) (Equal Employment Opportunity Commission).

Second, the Court allows a defendant to object to the

search of a third party's property. This also is revolutionary. The Fourth Amendment protects "[t]he right of the people to be secure in *their* persons, houses, papers, and effects" (emphasis added), not the persons, houses, papers, and effects of others. Until today, we have been careful to heed this fundamental feature of the Amendment's text. This was true when the Fourth Amendment was tied to property law, and it remained true after *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967), broadened the Amendment's reach.

By departing dramatically from these fundamental principles, the Court destabilizes long-established Fourth Amendment doctrine. We will be making repairs—or picking up the pieces—for a long time to come.

I

Today the majority holds that a court order requiring the production of cell-site records may be issued only after the Government demonstrates probable cause. See *ante,* at 2220 - 2221. That is a serious and consequential mistake. The Court's holding is based on the premise that the order issued in this case was an actual "search" within the meaning of the Fourth Amendment, but that premise is inconsistent with the original meaning of the Fourth Amendment and with more than a century of precedent.

A

The order in this case was the functional equivalent of a subpoena for documents, and there is no evidence that these writs were regarded as "searches" at the time of the founding. Subpoenas *duces tecum* and other forms of compulsory document production were well known to the founding generation. Blackstone dated the first writ of subpoena to the reign of King Richard II in the late 14th century, and by the end of the 15th century, the use of such writs had "become the daily practice of the [Chancery] court." 3 W. Blackstone, ***2248** Commentaries on the Laws of England 53 (G. Tucker ed. 1803) (Blackstone). Over the next 200 years, subpoenas would grow in prominence and power in tandem with the Court of Chancery, and by the end of Charles II's reign in 1685, two important innovations had occurred.

First, the Court of Chancery developed a new species of subpoena. Until this point, subpoenas had been used largely to compel attendance and oral testimony from witnesses; these subpoenas correspond to today's subpoenas *ad testificandum*. But the Court of Chancery also improvised a new version of the writ that tacked onto a regular subpoena an order compelling the witness to bring certain items with him. By issuing these so-called subpoenas *duces tecum,* the Court of Chancery could compel the production of papers, books, and other forms of physical evidence, whether from the parties to the case or from third parties. Such subpoenas were sufficiently commonplace by 1623 that a leading treatise on the practice of law could refer in passing to the fee for a "*Sub poena of Ducas tecum* " (seven shillings and two pence) without needing to elaborate further. T. Powell, The Attourneys Academy 79 (1623). Subpoenas *duces tecum* would swell in use over the next century as the rules for their application became ever more developed and definite. See, *e.g.,* 1 G. Jacob, The Compleat Chancery–Practiser 290 (1730) ("The *Subpoena duces tecum* is awarded when the Defendant has confessed by his Answer that he hath such Writings in his Hands as are prayed by the Bill to be discovered or brought into Court").

Second, although this new species of subpoena had its origins in the Court of Chancery, it soon made an appearance in the work of the common-law courts as well. One court later reported that "[t]he Courts of Common law ... employed the same or similar means ... from the time of Charles the Second at least." *Amey v. Long,* 9 East. 473, 484, 103 Eng. Rep. 653, 658 (K.B. 1808).

By the time Blackstone published his Commentaries on the Laws of England in the 1760's, the use of subpoenas *duces tecum* had bled over substantially from the courts of equity to the common-law courts. Admittedly, the transition was still incomplete: In the context of jury trials, for example, Blackstone complained about "the want of a compulsive power for the production of books and papers belonging to the parties." Blackstone 381; see also, *e.g., Entick v. Carrington,* 19 State Trials 1029, 1073 (K.B. 1765) ("I wish some cases had been shewn, where the law forceth evidence out of the owner's custody by process. [But] where the adversary has by force or fraud got possession of your own proper evidence, there is no way to get it back but by action"). But Blackstone found some comfort in the fact that at least those documents "[i]n the hands of third persons ... can generally be obtained by rule of court, or by adding a clause of requisition to the writ of *subpoena,* which is then called a *subpoena duces tecum.*" Blackstone 381; see also, *e.g., Leeds v. Cook,* 4 Esp. 256, 257, 170 Eng. Rep. 711 (N.P. 1803) (third-party subpoena *duces tecum*); *Rex v. Babb,* 3 T.R. 579, 580, 100 Eng. Rep. 743, 744 (K.B. 1790) (third-party document production). One of the primary questions outstanding, then, was whether common-law courts would remedy the "defect[s]" identified by the

Commentaries, and allow parties to use subpoenas *duces tecum* not only with respect to third parties but also with respect to each other. Blackstone 381.

That question soon found an affirmative answer on both sides of the Atlantic. In the United States, the First Congress established the federal court system in the ***2249** Judiciary Act of 1789. As part of that Act, Congress authorized "all the said courts of the United States ... in the trial of actions at law, on motion and due notice thereof being given, to require the parties to produce books or writings in their possession or power, which contain evidence pertinent to the issue, in cases and under circumstances where they might be compelled to produce the same by the ordinary rules of proceeding in chancery." § 15, 1 Stat. 82. From that point forward, federal courts in the United States could compel the production of documents regardless of whether those documents were held by parties to the case or by third parties.

In Great Britain, too, it was soon definitively established that common-law courts, like their counterparts in equity, could subpoena documents held either by parties to the case or by third parties. After proceeding in fits and starts, the King's Bench eventually held in *Amey v. Long* that the "writ of subpoena duces tecum [is] a writ of compulsory obligation and effect in the law." 9 East., at 486, 103 Eng. Rep., at 658. Writing for a unanimous court, Lord Chief Justice Ellenborough explained that "[t]he right to resort to means competent to compel the production of written, as well as oral, testimony seems essential to the very existence and constitution of a Court of Common Law." *Id.*, at 484, 103 Eng. Rep., at 658. Without the power to issue subpoenas *duces tecum,* the Lord Chief Justice observed, common-law courts "could not possibly proceed with due effect." *Ibid.*

The prevalence of subpoenas *duces tecum* at the time of the founding was not limited to the civil context. In criminal cases, courts and prosecutors were also using the writ to compel the production of necessary documents. In *Rex v. Dixon,* 3 Burr. 1687, 97 Eng. Rep. 1047 (K.B. 1765), for example, the King's Bench considered the propriety of a subpoena *duces tecum* served on an attorney named Samuel Dixon. Dixon had been called "to give evidence before the grand jury of the county of Northampton" and specifically "to produce three vouchers ... in order to found a prosecution by way of indictment against [his client] Peach ... for forgery." *Id.*, at 1687, 97 Eng. Rep., at 1047–1048. Although the court ultimately held that Dixon had not needed to produce the vouchers on account of attorney-client privilege, none of the justices expressed the slightest doubt about the general propriety of subpoenas *duces tecum* in the criminal context. See *id.*, at 1688, 97 Eng. Rep., at 1048. As Lord Chief Justice Ellenborough later explained, "[i]n that case no objection was taken to the writ, but to the special circumstances under which the party possessed the papers; so that the Court may be considered as recognizing the general obligation to obey writs of that description in other cases." *Amey, supra,* at 485, 103 Eng. Rep., at 658; see also 4 J. Chitty, Practical Treatise on the Criminal Law 185 (1816) (template for criminal subpoena *duces tecum*).

As *Dixon* shows, subpoenas *duces tecum* were routine in part because of their close association with grand juries. Early American colonists imported the grand jury, like so many other common-law traditions, and they quickly flourished. See *United States v. Calandra,* 414 U.S. 338, 342–343, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974). Grand juries were empaneled by the federal courts almost as soon as the latter were established, and both they and their state counterparts actively exercised their wide-ranging common-law authority. See R. Younger, The People's Panel 47–55 (1963). Indeed, "the Founders thought the grand jury so essential ... that they provided in the Fifth Amendment that federal prosecution for serious crimes can only be instituted by 'a presentment or ***2250** indictment of a Grand Jury.' " *Calandra, supra,* at 343, 94 S.Ct. 613.

Given the popularity and prevalence of grand juries at the time, the Founders must have been intimately familiar with the tools they used—including compulsory process—to accomplish their work. As a matter of tradition, grand juries were "accorded wide latitude to inquire into violations of criminal law," including the power to "compel the production of evidence or the testimony of witnesses as [they] conside[r] appropriate." *Ibid.* Long before national independence was achieved, grand juries were already using their broad inquisitorial powers not only to present and indict criminal suspects but also to inspect public buildings, to levy taxes, to supervise the administration of the laws, to advance municipal reforms such as street repair and bridge maintenance, and in some cases even to propose legislation. Younger, *supra,* at 5–26. Of course, such work depended entirely on grand juries' ability to access any relevant documents.

Grand juries continued to exercise these broad inquisitorial powers up through the time of the founding. See *Blair v. United States,* 250 U.S. 273, 280, 39 S.Ct. 468, 63 L.Ed. 979 (1919) ("At the foundation of our Federal Government the inquisitorial function of the grand jury and the compulsion of witnesses were

recognized as incidents of the judicial power"). In a series of lectures delivered in the early 1790's, Justice James Wilson crowed that grand juries were "the peculiar boast of the common law" thanks in part to their wide-ranging authority: "All the operations of government, and of its ministers and officers, are within the compass of their view and research." 2 J. Wilson, The Works of James Wilson 534, 537 (R. McCloskey ed. 1967). That reflected the broader insight that "[t]he grand jury's investigative power must be broad if its public responsibility is adequately to be discharged." *Calandra, supra,* at 344, 94 S.Ct. 613.

Compulsory process was also familiar to the founding generation in part because it reflected "the ancient proposition of law" that " ' "the public ... has a right to every man's evidence." ' " *United States v. Nixon,* 418 U.S. 683, 709, 94 S.Ct. 3090, 41 L.Ed.2d 1039 (1974); see also *ante,* at 2228 (KENNEDY, J., dissenting). As early as 1612, "Lord Bacon is reported to have declared that 'all subjects, without distinction of degrees, owe to the King tribute and service, not only of their deed and hand, but of their knowledge and discovery.' " *Blair, supra,* at 279–280, 39 S.Ct. 468. That duty could be "onerous at times," yet the Founders considered it "necessary to the administration of justice according to the forms and modes established in our system of government." *Id.,* at 281, 39 S.Ct. 468; see also *Calandra, supra,* at 345, 94 S.Ct. 613.

B

Talk of kings and common-law writs may seem out of place in a case about cell-site records and the protections afforded by the Fourth Amendment in the modern age. But this history matters, not least because it tells us what was on the minds of those who ratified the Fourth Amendment and how they understood its scope. That history makes it abundantly clear that the Fourth Amendment, as originally understood, did not apply to the compulsory production of documents at all.

The Fourth Amendment does not regulate all methods by which the Government obtains documents. Rather, it prohibits only those "searches and seizures" of "persons, houses, papers, and effects" that are "unreasonable." Consistent with that language, "at least until the latter half of the 20th century" "our Fourth Amendment jurisprudence was tied to common-law trespass." ***2251** *United States v. Jones,* 565 U.S. 400, 405, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). So by its terms, the Fourth Amendment does not apply to the compulsory production of documents, a practice that involves neither any physical intrusion into private space nor any taking of property by agents of the state. Even Justice Brandeis—a stalwart proponent of construing the Fourth Amendment liberally—acknowledged that "under any ordinary construction of language," "there is no 'search' or 'seizure' when a defendant is required to produce a document in the orderly process of a court's procedure." *Olmstead v. United States,* 277 U.S. 438, 476, 48 S.Ct. 564, 72 L.Ed. 944 (1928) (dissenting opinion).[1]

Nor is there any reason to believe that the Founders intended the Fourth Amendment to regulate courts' use of compulsory process. American colonists rebelled against the Crown's physical invasions of their persons and their property, not against its acquisition of information by any and all means. As Justice Black once put it, "[t]he Fourth Amendment was aimed directly at the abhorred practice of breaking in, ransacking and searching homes and other buildings and seizing people's personal belongings without warrants issued by magistrates." *Katz,* 389 U.S., at 367, 88 S.Ct. 507 (dissenting opinion). More recently, we have acknowledged 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." *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2494, 189 L.Ed.2d 430 (2014).

General warrants and writs of assistance were noxious not because they allowed the Government to acquire evidence in criminal investigations, but because of the *means* by which they permitted the Government to acquire that evidence. Then, as today, searches could be quite invasive. Searches generally begin with officers "mak[ing] nonconsensual entries into areas not open to the public." *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 414, 104 S.Ct. 769, 78 L.Ed.2d 567 (1984). Once there, officers are necessarily in a position to observe private spaces generally shielded from the public and discernible only with the owner's consent. Private area after private area becomes exposed to the officers' eyes as they rummage through the owner's property in their hunt for the object or objects of the search. If they are searching for documents, officers may additionally have to rifle through many other papers—potentially filled with the most intimate details of a person's thoughts and life—before they find the specific information ***2252** they are seeking. See *Andresen v. Maryland,* 427 U.S. 463, 482, n. 11, 96 S.Ct. 2737, 49 L.Ed.2d 627 (1976). If anything sufficiently incriminating comes into view, officers seize it. *Horton v. California,* 496 U.S. 128, 136–137, 110 S.Ct. 2301, 110 L.Ed.2d 112 (1990). Physical destruction always lurks as an underlying

possibility; "officers executing search warrants on occasion must damage property in order to perform their duty." *Dalia v. United States,* 441 U.S. 238, 258, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979); see, *e.g., United States v. Ramirez,* 523 U.S. 65, 71–72, 118 S.Ct. 992, 140 L.Ed.2d 191 (1998) (breaking garage window); *United States v. Ross,* 456 U.S. 798, 817–818, 102 S.Ct. 2157, 72 L.Ed.2d 572 (1982) (ripping open car upholstery); *Brown v. Battle Creek Police Dept.,* 844 F.3d 556, 572 (C.A.6 2016) (shooting and killing two pet dogs); *Lawmaster v. Ward,* 125 F.3d 1341, 1350, n. 3 (C.A.10 1997) (breaking locks).

Compliance with a subpoena *duces tecum* requires none of that. A subpoena *duces tecum* permits a subpoenaed individual to conduct the search for the relevant documents himself, without law enforcement officers entering his home or rooting through his papers and effects. As a result, subpoenas avoid the many incidental invasions of privacy that necessarily accompany any actual search. And it was *those* invasions of privacy—which, although incidental, could often be extremely intrusive and damaging—that led to the adoption of the Fourth Amendment.

Neither this Court nor any of the parties have offered the slightest bit of historical evidence to support the idea that the Fourth Amendment originally applied to subpoenas *duces tecum* and other forms of compulsory process. That is telling, for as I have explained, these forms of compulsory process were a feature of criminal (and civil) procedure well known to the Founders. The Founders would thus have understood that holding the compulsory production of documents to the same standard as actual searches and seizures would cripple the work of courts in civil and criminal cases alike. It would be remarkable to think that, despite that knowledge, the Founders would have gone ahead and sought to impose such a requirement. It would be even more incredible to believe that the Founders would have imposed that requirement through the inapt vehicle of an amendment directed at different concerns. But it would blink reality entirely to argue that this entire process happened without anyone saying *the least thing about it*—not during the drafting of the Bill of Rights, not during any of the subsequent ratification debates, and not for most of the century that followed. If the Founders thought the Fourth Amendment applied to the compulsory production of documents, one would imagine that there would be *some* founding-era evidence of the Fourth Amendment being applied to the compulsory production of documents. Cf. *Free Enterprise Fund v. Public Company Accounting Oversight Bd.,* 561 U.S. 477, 505, 130 S.Ct. 3138, 177 L.Ed.2d 706 (2010); *Printz v. United States,* 521 U.S. 898, 905, 117 S.Ct. 2365, 138 L.Ed.2d 914 (1997). Yet none has been brought to our attention.

C

Of course, our jurisprudence has not stood still since 1791. We now evaluate subpoenas *duces tecum* and other forms of compulsory document production under the Fourth Amendment, although we employ a reasonableness standard that is less demanding than the requirements for a warrant. But the road to that doctrinal destination was anything but smooth, and our initial missteps—and the subsequent struggle to extricate ourselves from their consequences—should provide an object ***2253** lesson for today's majority about the dangers of holding compulsory process to the same standard as actual searches and seizures.

For almost a century after the Fourth Amendment was enacted, this Court said and did nothing to indicate that it might regulate the compulsory production of documents. But that changed temporarily when the Court decided *Boyd v. United States,* 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746 (1886), the first—and, until today, the only—case in which this Court has ever held the compulsory production of documents to the same standard as actual searches and seizures.

The *Boyd* Court held that a court order compelling a company to produce potentially incriminating business records violated both the Fourth and the Fifth Amendments. The Court acknowledged that "certain aggravating incidents of actual search and seizure, such as forcible entry into a man's house and searching amongst his papers, are wanting" when the Government relies on compulsory process. *Id.,* at 622, 6 S.Ct. 524. But it nevertheless asserted that the Fourth Amendment ought to "be liberally construed," *id.,* at 635, 6 S.Ct. 524, and further reasoned that compulsory process "effects the sole object and purpose of search and seizure" by "forcing from a party evidence against himself," *id.,* at 622, 6 S.Ct. 524. "In this regard," the Court concluded, "the Fourth and Fifth Amendments run almost into each other." *Id.,* at 630, 6 S.Ct. 524. Having equated compulsory process with actual searches and seizures and having melded the Fourth Amendment with the Fifth, the Court then found the order at issue unconstitutional because it compelled the production of property to which the Government did not have superior title. See *id.,* at 622–630, 6 S.Ct. 524.

In a concurrence joined by Chief Justice Waite, Justice Miller agreed that the order violated the Fifth Amendment, *id.,* at 639, 6 S.Ct. 524, but he strongly protested the majority's invocation of the Fourth

Amendment. He explained: "[T]here is no reason why this court should assume that the action of the court below, in requiring a party to produce certain papers ..., authorizes an unreasonable search or seizure of the house, papers, or effects of that party. There is in fact no search and no seizure." *Ibid.* "If the mere service of a notice to produce a paper ... is a search," Justice Miller concluded, "then a change has taken place in the meaning of words, which has not come within my reading, and which I think was unknown at the time the Constitution was made." *Id.*, at 641, 6 S.Ct. 524.

Although *Boyd* was replete with stirring rhetoric, its reasoning was confused from start to finish in a way that ultimately made the decision unworkable. See 3 W. LaFave, J. Israel, N. King, & O. Kerr, Criminal Procedure § 8.7(a) (4th ed. 2015). Over the next 50 years, the Court would gradually roll back *Boyd* 's erroneous conflation of compulsory process with actual searches and seizures.

That effort took its first significant stride in *Hale v. Henkel,* 201 U.S. 43, 26 S.Ct. 370, 50 L.Ed. 652 (1906), where the Court found it "quite clear" and "conclusive" that "the search and seizure clause of the Fourth Amendment was not intended to interfere with the power of courts to compel, through a *subpoena duces tecum,* the production, upon a trial in court, of documentary evidence." *Id.*, at 73, 26 S.Ct. 370. Without that writ, the Court recognized, "it would be 'utterly impossible to carry on the administration of justice.' " *Ibid.*

Hale, however, did not entirely liberate subpoenas *duces tecum* from Fourth ***2254** Amendment constraints. While refusing to treat such subpoenas as the equivalent of actual searches, *Hale* concluded that they must not be unreasonable. And it held that the subpoena *duces tecum* at issue was "far too sweeping in its terms to be regarded as reasonable." *Id.*, at 76, 26 S.Ct. 370. The *Hale* Court thus left two critical questions unanswered: Under the Fourth Amendment, what makes the compulsory production of documents "reasonable," and how does that standard differ from the one that governs actual searches and seizures?

The Court answered both of those questions definitively in *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186, 66 S.Ct. 494, 90 L.Ed. 614 (1946), where we held that the Fourth Amendment regulates the compelled production of documents, but less stringently than it does full-blown searches and seizures. *Oklahoma Press* began by admitting that the Court's opinions on the subject had "perhaps too often ... been generative of heat rather than light," "mov[ing] with variant direction" and sometimes having "highly contrasting" "emphasis and tone." *Id.*, at 202, 66 S.Ct. 494. "The primary source of misconception concerning the Fourth Amendment's function" in this context, the Court explained, "lies perhaps in the identification of cases involving so-called 'figurative' or 'constructive' search with cases of actual search and seizure." *Ibid.* But the Court held that "the basic distinction" between the compulsory production of documents on the one hand, and actual searches and seizures on the other, meant that two different standards had to be applied. *Id.*, at 204, 66 S.Ct. 494.

Having reversed *Boyd* 's conflation of the compelled production of documents with actual searches and seizures, the Court then set forth the relevant Fourth Amendment standard for the former. When it comes to "the production of corporate or other business records," the Court held that the Fourth Amendment "at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be 'particularly described,' if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant." *Oklahoma Press, supra,* at 208, 66 S.Ct. 494. Notably, the Court held that a showing of probable cause was not necessary so long as "the investigation is authorized by Congress, is for a purpose Congress can order, and the documents sought are relevant to the inquiry." *Id.*, at 209, 66 S.Ct. 494.

Since *Oklahoma Press,* we have consistently hewed to that standard. See, *e.g., Lone Steer, Inc.,* 464 U.S., at 414–415, 104 S.Ct. 769; *United States v. Miller,* 425 U.S. 435, 445–446, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976); *California Bankers Assn. v. Shultz,* 416 U.S. 21, 67, 94 S.Ct. 1494, 39 L.Ed.2d 812 (1974); *United States v. Dionisio,* 410 U.S. 1, 11–12, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973); *See v. Seattle,* 387 U.S. 541, 544, 87 S.Ct. 1737, 18 L.Ed.2d 943 (1967); *United States v. Powell,* 379 U.S. 48, 57–58, 85 S.Ct. 248, 13 L.Ed.2d 112 (1964); *McPhaul v. United States,* 364 U.S. 372, 382–383, 81 S.Ct. 138, 5 L.Ed.2d 136 (1960); *United States v. Morton Salt Co.,* 338 U.S. 632, 652–653, 70 S.Ct. 357, 94 L.Ed. 401 (1950); cf. *McLane Co. v. EEOC,* 581 U.S. ——, ——, 137 S.Ct. 1159, 1169–1170, 197 L.Ed.2d 500 (2017). By applying *Oklahoma Press* and thereby respecting "the traditional distinction between a search warrant and a subpoena," *Miller, supra,* at 446, 96 S.Ct. 1619, this Court has reinforced "the basic compromise" between "the public interest" in every man's evidence and the private interest "of men to be free from officious meddling." *Oklahoma Press, supra,* at 213, 66 S.Ct. 494.

***2255 D**

Today, however, the majority inexplicably ignores the settled rule of *Oklahoma Press* in favor of a resurrected version of *Boyd*. That is mystifying. This should have been an easy case regardless of whether the Court looked to the original understanding of the Fourth Amendment or to our modern doctrine.

As a matter of original understanding, the Fourth Amendment does not regulate the compelled production of documents at all. Here the Government received the relevant cell-site records pursuant to a court order compelling Carpenter's cell service provider to turn them over. That process is thus immune from challenge under the original understanding of the Fourth Amendment.

As a matter of modern doctrine, this case is equally straightforward. As Justice KENNEDY explains, no search or seizure of Carpenter or his property occurred in this case. *Ante,* at 2226 - 2235; see also Part II, *infra*. But even if the majority were right that the Government "searched" Carpenter, it would at most be a "figurative or constructive search" governed by the *Oklahoma Press* standard, not an "actual search" controlled by the Fourth Amendment's warrant requirement.

And there is no doubt that the Government met the *Oklahoma Press* standard here. Under *Oklahoma Press,* a court order must " 'be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome.' " *Lone Steer, Inc., supra,* at 415, 104 S.Ct. 769. Here, the type of order obtained by the Government almost necessarily satisfies that standard. The Stored Communications Act allows a court to issue the relevant type of order "only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that ... the records ... sough[t] are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). And the court "may quash or modify such order" if the provider objects that the "records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider." *Ibid.* No such objection was made in this case, and Carpenter does not suggest that the orders contravened the *Oklahoma Press* standard in any other way.

That is what makes the majority's opinion so puzzling. It decides that a "search" of Carpenter occurred within the meaning of the Fourth Amendment, but then it leaps straight to imposing requirements that—until this point—have governed only *actual* searches and seizures. See *ante,* at 2220 - 2221. Lost in its race to the finish is any real recognition of the century's worth of precedent it jeopardizes. For the majority, this case is apparently no different from one in which Government agents raided Carpenter's home and removed records associated with his cell phone.

Against centuries of precedent and practice, all that the Court can muster is the observation that "this Court has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy." *Ante,* at 2221. Frankly, I cannot imagine a concession more damning to the Court's argument than that. As the Court well knows, the reason that we have never seen such a case is because—until today—defendants categorically had no "reasonable expectation of privacy" and no property interest in records belonging to third parties. See Part II, *infra*. By implying otherwise, the Court tries the nice trick of seeking shelter under the cover of precedents that it simultaneously perforates.

***2256** Not only that, but even if the Fourth Amendment permitted someone to object to the subpoena of a third party's records, the Court cannot explain why that individual should be entitled to *greater* Fourth Amendment protection than the party actually being subpoenaed. When parties are subpoenaed to turn over their records, after all, they will at most receive the protection afforded by *Oklahoma Press* even though they will own and have a reasonable expectation of privacy in the records at issue. Under the Court's decision, however, the Fourth Amendment will extend greater protections to someone else who is not being subpoenaed and does not own the records. That outcome makes no sense, and the Court does not even attempt to defend it.

We have set forth the relevant Fourth Amendment standard for subpoenaing business records many times over. Out of those dozens of cases, the majority cannot find even one that so much as suggests an exception to the *Oklahoma Press* standard for sufficiently personal information. Instead, we have always "described the constitutional requirements" for compulsory process as being " 'settled' " and as applying categorically to all " 'subpoenas [of] corporate books or records.' " *Lone Steer, Inc.,* 464 U.S., at 415, 104 S.Ct. 769 (internal quotation marks omitted). That standard, we have held, is "*the most* " protection the Fourth Amendment gives "to the production of corporate records and papers." *Oklahoma Press,* 327 U.S., at 208, 66 S.Ct. 494 (emphasis added).[2]

Although the majority announces its holding in the context of the Stored Communications Act, nothing stops its logic from sweeping much further. The Court has offered no meaningful limiting principle, and none is

apparent. Cf. Tr. of Oral Arg. 31 (Carpenter's counsel admitting that "a grand jury subpoena ... would be held to the same standard as any other subpoena or subpoena-like request for [cell-site] records").

Holding that subpoenas must meet the same standard as conventional searches will seriously damage, if not destroy, their utility. Even more so than at the founding, today the Government regularly uses subpoenas *duces tecum* and other forms of compulsory process to carry out its essential functions. See, *e.g., Dionisio,* 410 U.S., at 11–12, 93 S.Ct. 764 (grand jury subpoenas); *McPhaul,* 364 U.S., at 382–383, 81 S.Ct. 138 (legislative subpoenas); *Oklahoma Press, supra,* at 208–209, 66 S.Ct. 494 (administrative subpoenas). Grand juries, for example, have long "compel[led] the production of evidence" in order to determine "*whether* there is probable cause to believe a crime has been committed." *Calandra,* 414 U.S., at 343, 94 S.Ct. 613 (emphasis added). Almost by definition, then, grand juries will be unable at first to demonstrate "the probable cause required for a warrant." *Ante,* at 2221 (majority opinion); see also *Oklahoma Press, supra,* at 213, 66 S.Ct. 494. If they are required to do so, the effects are as predictable as they are alarming: Many investigations will sputter out at the start, and a host of criminals will be able to evade law enforcement's reach.

"To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence." *Nixon,* 418 U.S., at 709, 94 S.Ct. 3090. For over a hundred years, we have understood that holding ***2257** subpoenas to the same standard as actual searches and seizures "would stop much if not all of investigation in the public interest at the threshold of inquiry." *Oklahoma Press, supra,* at 213, 66 S.Ct. 494. Today a skeptical majority decides to put that understanding to the test.

II

Compounding its initial error, the Court also holds that a defendant has the right under the Fourth Amendment to object to the search of a third party's property. This holding flouts the clear text of the Fourth Amendment, and it cannot be defended under either a property-based interpretation of that Amendment or our decisions applying the reasonable-expectations-of-privacy test adopted in *Katz,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576. By allowing Carpenter to object to the search of a third party's property, the Court threatens to revolutionize a second and independent line of Fourth Amendment doctrine.

A

It bears repeating that the Fourth Amendment guarantees "[t]he right of the people to be secure in *their* persons, houses, papers, and effects." (Emphasis added.) The Fourth Amendment does not confer rights with respect to the persons, houses, papers, and effects of others. Its language makes clear that "Fourth Amendment rights are personal," *Rakas v. Illinois,* 439 U.S. 128, 140, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978), and as a result, this Court has long insisted that they "may not be asserted vicariously," *id.,* at 133, 99 S.Ct. 421. It follows that a "person who is aggrieved ... only through the introduction of damaging evidence secured by a search of a third person's premises or property has not had any of his Fourth Amendment rights infringed." *Id.,* at 134, 99 S.Ct. 421.

In this case, as Justice KENNEDY cogently explains, the cell-site records obtained by the Government belong to Carpenter's cell service providers, not to Carpenter. See *ante,* at 2229 - 2230. Carpenter did not create the cell-site records. Nor did he have possession of them; at all relevant times, they were kept by the providers. Once Carpenter subscribed to his provider's service, he had no right to prevent the company from creating or keeping the information in its records. Carpenter also had no right to demand that the providers destroy the records, no right to prevent the providers from destroying the records, and, indeed, no right to modify the records in any way whatsoever (or to prevent the providers from modifying the records). Carpenter, in short, has no meaningful control over the cell-site records, which are created, maintained, altered, used, and eventually destroyed by his cell service providers.

Carpenter responds by pointing to a provision of the Telecommunications Act that requires a provider to disclose cell-site records when a customer so requests. See 47 U.S.C. § 222(c)(2). But a statutory disclosure requirement is hardly sufficient to give someone an ownership interest in the documents that must be copied and disclosed. Many statutes confer a right to obtain copies of documents without creating any property right.[3]

***2258** Carpenter's argument is particularly hard to swallow because nothing in the Telecommunications Act precludes cell service providers from charging customers a fee for accessing cell-site records. See *ante,* at 2229 - 2230 (KENNEDY, J., dissenting). It would be very strange if the owner of records were required to pay in order to inspect his own property.

Nor does the Telecommunications Act give Carpenter a property right in the cell-site records simply because they are subject to confidentiality restrictions. See 47 U.S.C. § 222(c)(1) (without a customer's permission, a cell service provider may generally "use, disclose, or permit access to individually identifiable [cell-site records]" only with respect to "its provision" of telecommunications services). Many federal statutes impose similar restrictions on private entities' use or dissemination of information in their own records without conferring a property right on third parties.[4]

***2259** It would be especially strange to hold that the Telecommunication Act's confidentiality provision confers a property right when the Act creates an express exception for any disclosure of records that is "required by law." 47 U.S.C. § 222(c)(1). So not only does Carpenter lack " 'the most essential and beneficial' " of the " 'constituent elements' " of property, *Dickman v. Commissioner,* 465 U.S. 330, 336, 104 S.Ct. 1086, 79 L.Ed.2d 343 (1984)—*i.e.,* the right to use the property to the exclusion of others—but he cannot even exclude the party he would most like to keep out, namely, the Government.[5]

For all these reasons, there is no plausible ground for maintaining that the information at issue here represents Carpenter's "papers" or "effects."[6]

B

In the days when this Court followed an exclusively property-based approach to the Fourth Amendment, the distinction between an individual's Fourth Amendment rights and those of a third party was clear cut. We first asked whether the object of the search—say, a house, papers, or effects—belonged to the defendant, and, if it did, whether the Government had committed a "trespass" in acquiring the evidence at issue. *Jones,* 565 U.S., at 411, n. 8, 132 S.Ct. 945.

When the Court held in *Katz* that "property rights are not the sole measure of Fourth Amendment violations," *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992), the sharp boundary between personal and third-party rights was tested. Under *Katz,* a party may invoke the Fourth Amendment whenever law enforcement officers violate the party's "justifiable" or "reasonable" expectation of privacy. See 389 U.S., at 353, 88 S.Ct. 507; see also *id.,* at 361, 88 S.Ct. 507 (Harlan, J., concurring) (applying the Fourth Amendment where "a person [has] exhibited an actual (subjective) expectation of privacy" and where that "expectation [is] one that society is prepared to recognize as 'reasonable' "). Thus freed from ***2260** the limitations imposed by property law, parties began to argue that they had a reasonable expectation of privacy in items owned by others. After all, if a trusted third party took care not to disclose information about the person in question, that person might well have a reasonable expectation that the information would not be revealed.

Efforts to claim Fourth Amendment protection against searches of the papers and effects of others came to a head in *Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71, where the defendant sought the suppression of two banks' microfilm copies of his checks, deposit slips, and other records. The defendant did not claim that he owned these documents, but he nonetheless argued that "analysis of ownership, property rights and possessory interests in the determination of Fourth Amendment rights ha[d] been severely impeached" by *Katz* and other recent cases. See Brief for Respondent in *United States v. Miller,* O.T.1975, No. 74–1179, p. 6. Turning to *Katz,* he then argued that he had a reasonable expectation of privacy in the banks' records regarding his accounts. Brief for Respondent in No. 74–1179, at 6; see also *Miller, supra,* at 442–443, 96 S.Ct. 1619.

Acceptance of this argument would have flown in the face of the Fourth Amendment's text, and the Court rejected that development. Because Miller gave up "dominion and control" of the relevant information to his bank, *Rakas,* 439 U.S., at 149, 99 S.Ct. 421, the Court ruled that he lost any protected Fourth Amendment interest in that information. See *Miller, supra,* at 442–443, 96 S.Ct. 1619. Later, in *Smith v. Maryland,* 442 U.S. 735, 745, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), the Court reached a similar conclusion regarding a telephone company's records of a customer's calls. As Justice KENNEDY concludes, *Miller* and *Smith* are thus best understood as placing "necessary limits on the ability of individuals to assert Fourth Amendment interests in property to which they lack a 'requisite connection.' " *Ante,* at 2227.

The same is true here, where Carpenter indisputably lacks any meaningful property-based connection to the cell-site records owned by his provider. Because the records are not Carpenter's in any sense, Carpenter may not seek to use the Fourth Amendment to exclude them.

By holding otherwise, the Court effectively allows Carpenter to object to the "search" of a third party's property, not recognizing the revolutionary nature of this change. The Court seems to think that *Miller* and *Smith* invented a new "doctrine"—"the third-party doctrine"—and the Court refuses to "extend" this product

of the 1970's to a new age of digital communications. *Ante,* at 2216 - 2217, 2220. But the Court fundamentally misunderstands the role of *Miller* and *Smith.* Those decisions did not forge a new doctrine; instead, they rejected an argument that would have disregarded the clear text of the Fourth Amendment and a formidable body of precedent.

In the end, the Court never explains how its decision can be squared with the fact that the Fourth Amendment protects only "[t]he right of the people to be secure in *their* persons, houses, papers, and effects." (Emphasis added.)

* * *

Although the majority professes a desire not to " 'embarrass the future,' " *ante,* at 2220, we can guess where today's decision will lead.

One possibility is that the broad principles that the Court seems to embrace will be applied across the board. All subpoenas *duces tecum* and all other orders compelling ***2261** the production of documents will require a demonstration of probable cause, and individuals will be able to claim a protected Fourth Amendment interest in any sensitive personal information about them that is collected and owned by third parties. Those would be revolutionary developments indeed.

The other possibility is that this Court will face the embarrassment of explaining in case after case that the principles on which today's decision rests are subject to all sorts of qualifications and limitations that have not yet been discovered. If we take this latter course, we will inevitably end up "mak[ing] a crazy quilt of the Fourth Amendment." *Smith, supra,* at 745, 99 S.Ct. 2577.

All of this is unnecessary. In the Stored Communications Act, Congress addressed the specific problem at issue in this case. The Act restricts the misuse of cell-site records by cell service providers, something that the Fourth Amendment cannot do. The Act also goes beyond current Fourth Amendment case law in restricting access by law enforcement. It permits law enforcement officers to acquire cell-site records only if they meet a heightened standard and obtain a court order. If the American people now think that the Act is inadequate or needs updating, they can turn to their elected representatives to adopt more protective provisions. Because the collection and storage of cell-site records affects nearly every American, it is unlikely that the question whether the current law requires strengthening will escape Congress's notice.

Legislation is much preferable to the development of an entirely new body of Fourth Amendment caselaw for many reasons, including the enormous complexity of the subject, the need to respond to rapidly changing technology, and the Fourth Amendment's limited scope. The Fourth Amendment restricts the conduct of the Federal Government and the States; it does not apply to private actors. But today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans. If today's decision encourages the public to think that this Court can protect them from this looming threat to their privacy, the decision will mislead as well as disrupt. And if holding a provision of the Stored Communications Act to be unconstitutional dissuades Congress from further legislation in this field, the goal of protecting privacy will be greatly disserved.

The desire to make a statement about privacy in the digital age does not justify the consequences that today's decision is likely to produce.

Justice GORSUCH, dissenting.

In the late 1960s this Court suggested for the first time that a search triggering the Fourth Amendment occurs when the government violates an "expectation of privacy" that "society is prepared to recognize as 'reasonable.' " *Katz v. United States,* 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring). Then, in a pair of decisions in the 1970s applying the *Katz* test, the Court held that a "reasonable expectation of privacy" *doesn't* attach to information shared with "third parties." See *Smith v. Maryland,* 442 U.S. 735, 743–744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); *United States v. Miller,* 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). By these steps, the Court came to conclude, the Constitution does nothing to limit investigators from searching records you've entrusted to your bank, accountant, and maybe even your doctor.

***2262** What's left of the Fourth Amendment? Today we use the Internet to do most everything. Smartphones make it easy to keep a calendar, correspond with friends, make calls, conduct banking, and even watch the game. Countless Internet companies maintain records about us and, increasingly, *for* us. Even our most private documents—those that, in other eras, we would have locked safely in a desk drawer or destroyed—now reside on third party servers. *Smith* and *Miller* teach that the police can review all of this material, on the theory that no one reasonably expects any of it will be kept private. But

no one believes that, if they ever did.

What to do? It seems to me we could respond in at least three ways. The first is to ignore the problem, maintain *Smith* and *Miller*, and live with the consequences. If the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it. The second choice is to set *Smith* and *Miller* aside and try again using the *Katz* "reasonable expectation of privacy" jurisprudence that produced them. The third is to look for answers elsewhere.

*

Start with the first option. *Smith* held that the government's use of a pen register to record the numbers people dial on their phones doesn't infringe a reasonable expectation of privacy because that information is freely disclosed to the third party phone company. 442 U.S., at 743–744, 99 S.Ct. 2577. *Miller* held that a bank account holder enjoys no reasonable expectation of privacy in the bank's records of his account activity. That's true, the Court reasoned, "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." 425 U.S., at 443, 96 S.Ct. 1619. Today the Court suggests that *Smith* and *Miller* distinguish between *kinds* of information disclosed to third parties and require courts to decide whether to "extend" those decisions to particular classes of information, depending on their sensitivity. See *ante*, at 2216 - 2221. But as the Sixth Circuit recognized and Justice KENNEDY explains, no balancing test of this kind can be found in *Smith* and *Miller*. See *ante*, at 2231 - 2232 (dissenting opinion). Those cases announced a categorical rule: Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it. And even if *Smith* and *Miller* did permit courts to conduct a balancing contest of the kind the Court now suggests, it's still hard to see how that would help the petitioner in this case. Why is someone's location when using a phone so much more sensitive than who he was talking to (*Smith*) or what financial transactions he engaged in (*Miller*)? I do not know and the Court does not say.

The problem isn't with the Sixth Circuit's application of *Smith* and *Miller* but with the cases themselves. Can the government demand a copy of all your e-mails from Google or Microsoft without implicating your Fourth Amendment rights? Can it secure your DNA from 23andMe without a warrant or probable cause? *Smith* and *Miller* say yes it can—at least without running afoul of *Katz*. But that result strikes most lawyers and judges today—me included—as pretty unlikely. In the years since its adoption, countless scholars, too, have come to conclude that the "third-party doctrine is not only wrong, but horribly wrong." Kerr, The Case for the Third–Party Doctrine, 107 Mich. L. Rev. 561, 563, n. 5, 564 (2009) (collecting criticisms but defending the doctrine (footnotes omitted)). The reasons are obvious. "As an empirical statement about subjective ***2263** expectations of privacy," the doctrine is "quite dubious." Baude & Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1872 (2016). People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private. Meanwhile, if the third party doctrine is supposed to represent a normative assessment of when a person should expect privacy, the notion that the answer might be "never" seems a pretty unattractive societal prescription. *Ibid.*

What, then, is the explanation for our third party doctrine? The truth is, the Court has never offered a persuasive justification. The Court has said that by conveying information to a third party you " 'assum[e] the risk' " it will be revealed to the police and therefore lack a reasonable expectation of privacy in it. *Smith, supra,* at 744, 99 S.Ct. 2577. But assumption of risk doctrine developed in tort law. It generally applies when "by contract or otherwise [one] expressly agrees to accept a risk of harm" or impliedly does so by "manifest[ing] his willingness to accept" that risk and thereby "take[s] his chances as to harm which may result from it." Restatement (Second) of Torts §§ 496B, 496C(1), and Comment *b* (1965); see also 1 D. Dobbs, P. Hayden, & E. Bublick, Law of Torts §§ 235–236, pp. 841–850 (2d ed. 2017). That rationale has little play in this context. Suppose I entrust a friend with a letter and he promises to keep it secret until he delivers it to an intended recipient. In what sense have I agreed to bear the risk that he will turn around, break his promise, and spill its contents to someone else? More confusing still, what have I done to "manifest my willingness to accept" the risk that the government will pry the document from my friend and read it *without* his consent?

One possible answer concerns knowledge. I know that my friend *might* break his promise, or that the government *might* have some reason to search the papers in his possession. But knowing about a risk doesn't mean you assume responsibility for it. Whenever you walk down the sidewalk you know a car may negligently or recklessly veer off and hit you, but that hardly means you accept the consequences and absolve the driver of any damage he

may do to you. Epstein, Privacy and the Third Hand: Lessons From the Common Law of Reasonable Expectations, 24 Berkeley Tech. L.J. 1199, 1204 (2009); see W. Keeton, D. Dobbs, R. Keeton, & D. Owen, Prosser & Keeton on Law of Torts 490 (5th ed.1984).

Some have suggested the third party doctrine is better understood to rest on consent than assumption of risk. "So long as a person knows that they are disclosing information to a third party," the argument goes, "their choice to do so is voluntary and the consent valid." Kerr, *supra,* at 588. I confess I still don't see it. Consenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government.* Perhaps there are exceptions, like when the third party is an undercover government agent. See Murphy, The Case Against the Case Against the Third–Party Doctrine: A Response to Epstein and Kerr, 24 Berkeley Tech. L.J. 1239, 1252 (2009); cf. *Hoffa v. United States,* 385 U.S. 293, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966). But otherwise this conception of consent appears to be just assumption of risk relabeled—you've "consented" to whatever risks are foreseeable.

Another justification sometimes offered for third party doctrine is clarity. You (and the police) know exactly how much protection you have in information confided ***2264** to others: none. As rules go, "the king always wins" is admirably clear. But the opposite rule would be clear too: Third party disclosures *never* diminish Fourth Amendment protection (call it "the king always loses"). So clarity alone cannot justify the third party doctrine.

In the end, what do *Smith* and *Miller* add up to? A doubtful application of *Katz* that lets the government search almost whatever it wants whenever it wants. The Sixth Circuit had to follow that rule and faithfully did just that, but it's not clear why we should.

*

There's a second option. What if we dropped *Smith* and *Miller* 's third party doctrine and retreated to the root *Katz* question whether there is a "reasonable expectation of privacy" in data held by third parties? Rather than solve the problem with the third party doctrine, I worry this option only risks returning us to its source: After all, it was *Katz* that produced *Smith* and *Miller* in the first place.

Katz's problems start with the text and original understanding of the Fourth Amendment, as Justice THOMAS thoughtfully explains today. *Ante,*at 2237 - 2244 (dissenting opinion). The Amendment's protections do not depend on the breach of some abstract "expectation of privacy" whose contours are left to the judicial imagination. Much more concretely, it protects your "person," and your "houses, papers, and effects." Nor does your right to bring a Fourth Amendment claim depend on whether a judge happens to agree that your subjective expectation to privacy is a "reasonable" one. Under its plain terms, the Amendment grants you the right to invoke its guarantees whenever one of your protected things (your person, your house, your papers, or your effects) is unreasonably searched or seized. Period.

History too holds problems for *Katz*. Little like it can be found in the law that led to the adoption of the Fourth Amendment or in this Court's jurisprudence until the late 1960s. The Fourth Amendment came about in response to a trio of 18th century cases "well known to the men who wrote and ratified the Bill of Rights, [and] famous throughout the colonial population." Stuntz, The Substantive Origins of Criminal Procedure, 105 Yale L.J. 393, 397 (1995). The first two were English cases invalidating the Crown's use of general warrants to enter homes and search papers. *Entick v. Carrington,* 19 How. St. Tr. 1029 (K.B. 1765); *Wilkes v. Wood,* 19 How. St. Tr. 1153 (K.B. 1763); see W. Cuddihy, The Fourth Amendment: Origins and Original Meaning 439–487 (2009); *Boyd v. United States,* 116 U.S. 616, 625–630, 6 S.Ct. 524, 29 L.Ed. 746 (1886). The third was American: the Boston Writs of Assistance Case, which sparked colonial outrage at the use of writs permitting government agents to enter houses and business, breaking open doors and chests along the way, to conduct searches and seizures—and to force third parties to help them. Stuntz, *supra,* at 404–409; M. Smith, The Writs of Assistance Case (1978). No doubt the colonial outrage engendered by these cases rested in part on the government's intrusion upon privacy. But the framers chose not to protect privacy in some ethereal way dependent on judicial intuitions. They chose instead to protect privacy in particular places and things—"persons, houses, papers, and effects"—and against particular threats—"unreasonable" governmental "searches and seizures." See *Entick, supra,* at 1066 ("Papers are the owner's goods and chattels; they are his dearest property; and so far from enduring a seizure, that they will hardly bear an inspection"); see also *ante,* at 2235 - 2246 (THOMAS, J., dissenting).

***2265** Even taken on its own terms, *Katz* has never been sufficiently justified. In fact, we still don't even know what its "reasonable expectation of privacy" test *is*. Is it supposed to pose an empirical question (what privacy expectations do people *actually* have) or a normative one

(what expectations *should* they have)? Either way brings problems. If the test is supposed to be an empirical one, it's unclear why judges rather than legislators should conduct it. Legislators are responsive to their constituents and have institutional resources designed to help them discern and enact majoritarian preferences. Politically insulated judges come armed with only the attorneys' briefs, a few law clerks, and their own idiosyncratic experiences. They are hardly the representative group you'd expect (or want) to be making empirical judgments for hundreds of millions of people. Unsurprisingly, too, judicial judgments often fail to reflect public views. See Slobogin & Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society," 42 Duke L.J. 727, 732, 740–742 (1993). Consider just one example. Our cases insist that the seriousness of the offense being investigated does *not* reduce Fourth Amendment protection. *Mincey v. Arizona,* 437 U.S. 385, 393–394, 98 S.Ct. 2408, 57 L.Ed.2d 290 (1978). Yet scholars suggest that most people *are* more tolerant of police intrusions when they investigate more serious crimes. See Blumenthal, Adya, & Mogle, The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy," 11 U. Pa. J. Const. L. 331, 352–353 (2009). And I very much doubt that this Court would be willing to adjust its *Katz* cases to reflect these findings even if it believed them.

Maybe, then, the *Katz* test should be conceived as a normative question. But if that's the case, why (again) do judges, rather than legislators, get to determine whether society *should be* prepared to recognize an expectation of privacy as legitimate? Deciding what privacy interests *should be* recognized often calls for a pure policy choice, many times between incommensurable goods—between the value of privacy in a particular setting and society's interest in combating crime. Answering questions like that calls for the exercise of raw political will belonging to legislatures, not the legal judgment proper to courts. See The Federalist No. 78, p. 465 (C. Rossiter ed. 1961) (A. Hamilton). When judges abandon legal judgment for political will we not only risk decisions where "reasonable expectations of privacy" come to bear "an uncanny resemblance to those expectations of privacy" shared by Members of this Court. *Minnesota v. Carter,* 525 U.S. 83, 97, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (Scalia, J., concurring). We also risk undermining public confidence in the courts themselves.

My concerns about *Katz* come with a caveat. *Sometimes,* I accept, judges may be able to discern and describe existing societal norms. See, *e.g., Florida v. Jardines,* 569 U.S. 1, 8, 133 S.Ct. 1409, 185 L.Ed.2d 495 (2013) (inferring a license to enter on private property from the " 'habits of the country' " (quoting *McKee v. Gratz,* 260 U.S. 127, 136, 43 S.Ct. 16, 67 L.Ed. 167 (1922))); Sachs, Finding Law, 107 Cal. L. Rev. (forthcoming 2019), online at https://ssrn.com/abstract=3064443 (as last visited June 19, 2018). That is particularly true when the judge looks to positive law rather than intuition for guidance on social norms. See *Byrd v. United States,* 584 U.S. ——, —— – ——, 138 S.Ct. 1518, 1527, —— L.Ed.2d —— (2018) ("general property-based concept[s] guid[e] the resolution of this case"). So there may be *some* occasions where *Katz* is capable of principled application— ***2266** though it may simply wind up approximating the more traditional option I will discuss in a moment. Sometimes it may also be possible to apply *Katz* by analogizing from precedent when the line between an existing case and a new fact pattern is short and direct. But so far this Court has declined to tie itself to any significant restraints like these. See *ante,* at 2214, n. 1 ("[W]hile property rights are often informative, our cases by no means suggest that such an interest is 'fundamental' or 'dispositive' in determining which expectations of privacy are legitimate").

As a result, *Katz* has yielded an often unpredictable—and sometimes unbelievable—jurisprudence. *Smith* and *Miller* are only two examples; there are many others. Take *Florida v. Riley,* 488 U.S. 445, 109 S.Ct. 693, 102 L.Ed.2d 835 (1989), which says that a police helicopter hovering 400 feet above a person's property invades no reasonable expectation of privacy. Try that one out on your neighbors. Or *California v. Greenwood,* 486 U.S. 35, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988), which holds that a person has no reasonable expectation of privacy in the garbage he puts out for collection. In that case, the Court said that the homeowners forfeited their privacy interests because "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public." *Id.,* at 40, 108 S.Ct. 1625 (footnotes omitted). But the habits of raccoons don't prove much about the habits of the country. I doubt, too, that most people spotting a neighbor rummaging through their garbage would think they lacked reasonable grounds to confront the rummager. Making the decision all the stranger, California state law expressly *protected* a homeowner's property rights in discarded trash. *Id.,* at 43, 108 S.Ct. 1625. Yet rather than defer to that as evidence of the people's habits and reasonable expectations of privacy, the Court substituted its own curious judgment.

Resorting to *Katz* in data privacy cases threatens more of the same. Just consider. The Court today says that judges should use *Katz* 's reasonable expectation of privacy test to decide what Fourth Amendment rights people have in

cell-site location information, explaining that "no single rubric definitively resolves which expectations of privacy are entitled to protection." *Ante,* at 2213 - 2214. But then it offers a twist. Lower courts should be sure to add two special principles to their *Katz* calculus: the need to avoid "arbitrary power" and the importance of "plac[ing] obstacles in the way of a too permeating police surveillance." *Ante,* at 2214 (internal quotation marks omitted). While surely laudable, these principles don't offer lower courts much guidance. The Court does not tell us, for example, how far to carry either principle or how to weigh them against the legitimate needs of law enforcement. At what point does access to electronic data amount to "arbitrary" authority? When does police surveillance become "too permeating"? And what sort of "obstacles" should judges "place" in law enforcement's path when it does? We simply do not know.

The Court's application of these principles supplies little more direction. The Court declines to say whether there is any sufficiently limited period of time "for which the Government may obtain an individual's historical [location information] free from Fourth Amendment scrutiny." *Ante,* at 2217, n. 3; see *ante,* at 2216 - 2219. But then it tells us that access to seven days' worth of information *does* trigger Fourth Amendment scrutiny—even though here the carrier "produced only two days of records." *Ante,* at 2217, n. 3. Why is the relevant fact the seven days of ***2267** information the government *asked for* instead of the two days of information the government *actually saw* ? Why seven days instead of ten or three or one? And in what possible sense did the government "search" five days' worth of location information it was never even sent? We do not know.

Later still, the Court adds that it can't say whether the Fourth Amendment is triggered when the government collects "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)." *Ante,* at 2220. But what distinguishes historical data from real-time data, or seven days of a single person's data from a download of *everyone* 's data over some indefinite period of time? Why isn't a tower dump the *paradigmatic* example of "too permeating police surveillance" and a dangerous tool of "arbitrary" authority—the touchstones of the majority's modified *Katz* analysis? On what possible basis could such mass data collection survive the Court's test while collecting a single person's data does not? Here again we are left to guess. At the same time, though, the Court offers some firm assurances. It tells us its decision does *not* "call into question conventional surveillance techniques and tools, such as security cameras." *Ibid.* That, however, just raises more questions for lower courts to sort out about what techniques qualify as "conventional" and why those techniques would be okay *even if* they lead to "permeating police surveillance" or "arbitrary police power."

Nor is this the end of it. After finding a reasonable expectation of privacy, the Court says there's still more work to do. Courts must determine whether to "extend" *Smith* and *Miller* to the circumstances before them. *Ante,* at 2216, 2219 - 2220. So apparently *Smith* and *Miller* aren't quite left for dead; they just no longer have the clear reach they once did. How do we measure their new reach? The Court says courts now must conduct a *second Katz*-like balancing inquiry, asking whether the fact of disclosure to a third party outweighs privacy interests in the "category of information" so disclosed. *Ante,* at 2218, 2219 - 2220. But how are lower courts supposed to weigh these radically different interests? Or assign values to different categories of information? All we know is that historical cell-site location information (for seven days, anyway) escapes *Smith* and *Miller* 's shorn grasp, while a lifetime of bank or phone records does not. As to any other kind of information, lower courts will have to stay tuned.

In the end, our lower court colleagues are left with two amorphous balancing tests, a series of weighty and incommensurable principles to consider in them, and a few illustrative examples that seem little more than the product of judicial intuition. In the Court's defense, though, we have arrived at this strange place not because the Court has misunderstood *Katz.* Far from it. We have arrived here because this is where *Katz* inevitably leads.

*

There is another way. From the founding until the 1960s, the right to assert a Fourth Amendment claim didn't depend on your ability to appeal to a judge's personal sensibilities about the "reasonableness" of your expectations or privacy. It was tied to the law. *Jardines,* 569 U.S., at 11, 133 S.Ct. 1409; *United States v. Jones,* 565 U.S. 400, 405, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012). The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures." True to those words and their original understanding, the traditional approach ***2268** asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment. Though now often lost in *Katz* 's shadow, this traditional understanding persists. *Katz* only "supplements, rather than displaces the

traditional property-based understanding of the Fourth Amendment." *Byrd,* 584 U.S., at ——, 138 S.Ct., at 1526 (internal quotation marks omitted); *Jardines, supra,* at 11, 133 S.Ct. 1409 (same); *Soldal v. Cook County,* 506 U.S. 56, 64, 113 S.Ct. 538, 121 L.Ed.2d 450 (1992) (*Katz* did not "snuf[f] out the previously recognized protection for property under the Fourth Amendment").

Beyond its provenance in the text and original understanding of the Amendment, this traditional approach comes with other advantages. Judges are supposed to decide cases based on "democratically legitimate sources of law"—like positive law or analogies to items protected by the enacted Constitution—rather than "their own biases or personal policy preferences." Pettys, Judicial Discretion in Constitutional Cases, 26 J.L. & Pol. 123, 127 (2011). A Fourth Amendment model based on positive legal rights "carves out significant room for legislative participation in the Fourth Amendment context," too, by asking judges to consult what the people's representatives have to say about their rights. Baude & Stern, 129 Harv. L. Rev., at 1852. Nor is this approach hobbled by *Smith* and *Miller,* for those cases are just *limitations* on *Katz,* addressing only the question whether individuals have a reasonable expectation of privacy in materials they share with third parties. Under this more traditional approach, Fourth Amendment protections for your papers and effects do not automatically disappear just because you share them with third parties.

Given the prominence *Katz* has claimed in our doctrine, American courts are pretty rusty at applying the traditional approach to the Fourth Amendment. We know that if a house, paper, or effect is yours, you have a Fourth Amendment interest in its protection. But what kind of legal interest is sufficient to make something *yours* ? And what source of law determines that? Current positive law? The common law at 1791, extended by analogy to modern times? Both? See *Byrd, supra,* at ——— – ———, 138 S.Ct., at 1531 (THOMAS, J., concurring); cf. Re, The Positive Law Floor, 129 Harv. L. Rev. Forum 313 (2016). Much work is needed to revitalize this area and answer these questions. I do not begin to claim all the answers today, but (unlike with *Katz*) at least I have a pretty good idea what the questions *are*. And it seems to me a few things can be said.

First, the fact that a third party has access to or possession of your papers and effects does not necessarily eliminate your interest in them. Ever hand a private document to a friend to be returned? Toss your keys to a valet at a restaurant? Ask your neighbor to look after your dog while you travel? You would not expect the friend to share the document with others; the valet to lend your car to his buddy; or the neighbor to put Fido up for adoption. Entrusting your stuff to others is a *bailment.* A bailment is the "delivery of personal property by one person (the *bailor*) to another (the *bailee*) who holds the property for a certain purpose." Black's Law Dictionary 169 (10th ed. 2014); J. Story, Commentaries on the Law of Bailments § 2, p. 2 (1832) ("a bailment is a delivery of a thing in trust for some special object or purpose, and upon a contract, expressed or implied, to conform to the object or purpose of the trust"). A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the "implication[s] from their ***2269** conduct" if they don't. 8 C.J. S., Bailments § 36, pp. 468–469 (2017). A bailee who uses the item in a different way than he's supposed to, or against the bailor's instructions, is liable for conversion. *Id.,* § 43, at 481; see *Goad v. Harris,* 207 Ala. 357, 92 So. 546 (1922); *Knight v. Seney,* 290 Ill. 11, 17, 124 N.E. 813, 815–816 (1919); *Baxter v. Woodward,* 191 Mich. 379, 385, 158 N.W. 137, 139 (1916). This approach is quite different from *Smith* and *Miller* 's (counter)-intuitive approach to reasonable expectations of privacy; where those cases extinguish Fourth Amendment interests once records are given to a third party, property law may preserve them.

Our Fourth Amendment jurisprudence already reflects this truth. In *Ex parte Jackson,* 96 U.S. 727, 24 L.Ed. 877 (1878), this Court held that sealed letters placed in the mail are "as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles." *Id.,* at 733. The reason, drawn from the Fourth Amendment's text, was that "[t]he constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to *their papers,* thus closed against inspection, *wherever they may be.*" *Ibid.* (emphasis added). It did not matter that letters were bailed to a third party (the government, no less). The sender enjoyed the same Fourth Amendment protection as he does "when papers are subjected to search in one's own household." *Ibid.*

These ancient principles may help us address modern data cases too. Just because you entrust your data—in some cases, your modern-day papers and effects—to a third party may not mean you lose any Fourth Amendment interest in its contents. Whatever may be left of *Smith* and *Miller,* few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest. See *ante,* at 2230 (KENNEDY, J.,

dissenting) (noting that enhanced Fourth Amendment protection may apply when the "modern-day equivalents of an individual's own 'papers' or 'effects' ... are held by a third party" through "bailment"); *ante,* at 2259, n. 6 (ALITO, J., dissenting) (reserving the question whether Fourth Amendment protection may apply in the case of "bailment" or when "someone has entrusted papers he or she owns ... to the safekeeping of another"); *United States v. Warshak,* 631 F.3d 266, 285–286 (C.A.6 2010) (relying on an analogy to *Jackson* to extend Fourth Amendment protection to e-mail held by a third party service provider).

Second, I doubt that complete ownership or exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right. Where houses are concerned, for example, individuals can enjoy Fourth Amendment protection without fee simple title. Both the text of the Amendment and the common law rule support that conclusion. "People call a house 'their' home when legal title is in the bank, when they rent it, and even when they merely occupy it rent free." *Carter,* 525 U.S., at 95–96, 119 S.Ct. 469 (Scalia, J., concurring). That rule derives from the common law. *Oystead v. Shed,* 13 Mass. 520, 523 (1816) (explaining, citing "[t]he very learned judges, *Foster, Hale,* and *Coke,*" that the law "would be as much disturbed by a forcible entry to arrest a boarder or a servant, who had acquired, by contract, express or implied, a right to enter the house at all times, and to remain in it as long as they please, as if the object were to arrest the master of the house or his children"). That is why tenants and resident family members—though they have no legal title—have standing to complain ***2270** about searches of the houses in which they live. *Chapman v. United States,* 365 U.S. 610, 616–617, 81 S.Ct. 776, 5 L.Ed.2d 828 (1961), *Bumper v. North Carolina,* 391 U.S. 543, 548, n. 11, 88 S.Ct. 1788, 20 L.Ed.2d 797 (1968).

Another point seems equally true: just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections in it. Not infrequently one person comes into possession of someone else's property without the owner's consent. Think of the finder of lost goods or the policeman who impounds a car. The law recognizes that the goods and the car still belong to their true owners, for "where a person comes into lawful possession of the personal property of another, even though there is no formal agreement between the property's owner and its possessor, the possessor will become a constructive bailee when justice so requires." *Christensen v. Hoover,* 643 P.2d 525, 529 (Colo.1982) (en banc); Laidlaw, Principles of Bailment, 16 Cornell L.Q. 286 (1931). At least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern life, and in that way the fact that we store data with third parties may amount to a sort of involuntary bailment too. See *ante,* at 2217 - 2218 (majority opinion); *Riley v. California,* 573 U.S. ——, ——, 134 S.Ct. 2473, 2484, 189 L.Ed.2d 430 (2014).

Third, positive law may help provide detailed guidance on evolving technologies without resort to judicial intuition. State (or sometimes federal) law often creates rights in both tangible and intangible things. See *Ruckelshaus v. Monsanto Co.,* 467 U.S. 986, 1001, 104 S.Ct. 2862, 81 L.Ed.2d 815 (1984). In the context of the Takings Clause we often ask whether those state-created rights are sufficient to make something someone's property for constitutional purposes. See *id.,* at 1001–1003, 104 S.Ct. 2862; *Louisville Joint Stock Land Bank v. Radford,* 295 U.S. 555, 590–595, 55 S.Ct. 854, 79 L.Ed. 1593 (1935). A similar inquiry may be appropriate for the Fourth Amendment. Both the States and federal government are actively legislating in the area of third party data storage and the rights users enjoy. See, *e.g.,* Stored Communications Act, 18 U.S.C. § 2701 *et seq.*; Tex. Prop.Code Ann. § 111.004(12) (West 2017) (defining "[p]roperty" to include "property held in any digital or electronic medium"). State courts are busy expounding common law property principles in this area as well. *E.g., Ajemian v. Yahoo!, Inc.,* 478 Mass. 169, 170, 84 N.E.3d 766, 768 (2017) (e-mail account is a "form of property often referred to as a 'digital asset' "); *Eysoldt v. ProScan Imaging,* 194 Ohio App.3d 630, 638, 2011–Ohio–2359, 957 N.E.2d 780, 786 (2011) (permitting action for conversion of web account as intangible property). If state legislators or state courts say that a digital record has the attributes that normally make something property, that may supply a sounder basis for judicial decisionmaking than judicial guesswork about societal expectations.

Fourth, while positive law may help establish a person's Fourth Amendment interest there may be some circumstances where positive law cannot be used to defeat it. *Ex parte Jackson* reflects that understanding. There this Court said that "[n]o law of Congress" could authorize letter carriers "to invade the secrecy of letters." 96 U.S., at 733. So the post office couldn't impose a regulation dictating that those mailing letters surrender all legal interests in them once they're deposited in a mailbox. If that is right, *Jackson* suggests the existence of a constitutional floor below which Fourth Amendment rights may not descend. Legislatures cannot ***2271** pass laws declaring your house or papers to be your property except to the extent the police wish to search them without cause. As the Court has previously explained, "we must 'assur[e] preservation of that degree of privacy

against government that existed when the Fourth Amendment was adopted.' " *Jones,* 565 U.S., at 406, 132 S.Ct. 945 (quoting *Kyllo v. United States,* 533 U.S. 27, 34, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001)). Nor does this mean protecting only the specific rights known at the founding; it means protecting their modern analogues too. So, for example, while thermal imaging was unknown in 1791, this Court has recognized that using that technology to look inside a home constitutes a Fourth Amendment "search" of that "home" no less than a physical inspection might. *Id.,* at 40, 121 S.Ct. 2038.

Fifth, this constitutional floor may, in some instances, bar efforts to circumvent the Fourth Amendment's protection through the use of subpoenas. No one thinks the government can evade *Jackson* 's prohibition on opening sealed letters without a warrant simply by issuing a subpoena to a postmaster for "all letters sent by John Smith" or, worse, "all letters sent by John Smith concerning a particular transaction." So the question courts will confront will be this: What other kinds of records are sufficiently similar to letters in the mail that the same rule should apply?

It may be that, as an original matter, a subpoena requiring the recipient to produce records wasn't thought of as a "search or seizure" by the government implicating the Fourth Amendment, see *ante,* at 2247 - 2253 (opinion of ALITO, J.), but instead as an act of compelled self-incrimination implicating the Fifth Amendment, see *United States v. Hubbell,* 530 U.S. 27, 49–55, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) (THOMAS, J., dissenting); Nagareda, Compulsion "To Be a Witness" and the Resurrection of Boyd, 74 N.Y.U. L. Rev. 1575, 1619, and n. 172 (1999). But the common law of searches and seizures does not appear to have confronted a case where private documents equivalent to a mailed letter were entrusted to a bailee and then subpoenaed. As a result, "[t]he common-law rule regarding subpoenas for documents held by third parties entrusted with information from the target is ... unknown and perhaps unknowable." Dripps, Perspectives on The Fourth Amendment Forty Years Later: Toward the Realization of an Inclusive Regulatory Model, 100 Minn. L. Rev. 1885, 1922 (2016). Given that (perhaps insoluble) uncertainty, I am content to adhere to *Jackson* and its implications for now.

To be sure, we must be wary of returning to the doctrine of *Boyd v. United States,* 116 U.S. 616, 6 S.Ct. 524, 29 L.Ed. 746. *Boyd* invoked the Fourth Amendment to restrict the use of subpoenas even for ordinary business records and, as Justice ALITO notes, eventually proved unworkable. See *ante,* at 2253 (dissenting opinion); 3 W. LaFave, J. Israel, N. King, & O. Kerr, Criminal Procedure § 8.7(a), pp. 185–187 (4th ed. 2015). But if we were to overthrow *Jackson* too and deny Fourth Amendment protection to *any* subpoenaed materials, we would do well to reconsider the scope of the Fifth Amendment while we're at it. Our precedents treat the right against self-incrimination as applicable only to testimony, not the production of incriminating evidence. See *Fisher v. United States,* 425 U.S. 391, 401, 96 S.Ct. 1569, 48 L.Ed.2d 39 (1976). But there 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. Nagareda, *supra,* at 1605–1623; *Rex v. Purnell,* 96 Eng. Rep. 20 (K.B. 1748); Slobogin, Privacy at Risk 145 (2007).

***2272 ***

What does all this mean for the case before us? To start, I cannot fault the Sixth Circuit for holding that *Smith* and *Miller* extinguish any *Katz*-based Fourth Amendment interest in third party cell-site data. That is the plain effect of their categorical holdings. Nor can I fault the Court today for its implicit but unmistakable conclusion that the rationale of *Smith* and *Miller* is wrong; indeed, I agree with that. The Sixth Circuit was powerless to say so, but this Court can and should. At the same time, I do not agree with the Court's decision today to keep *Smith* and *Miller* on life support and supplement them with a new and multilayered inquiry that seems to be only *Katz*-squared. Returning there, I worry, promises more trouble than help. Instead, I would look to a more traditional Fourth Amendment approach. Even if *Katz* may still supply one way to prove a Fourth Amendment interest, it has never been the only way. Neglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment.

Our case offers a cautionary example. It seems to me entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law. Yes, the telephone carrier holds the information. But 47 U.S.C. § 222 designates a customer's cell-site location information as "customer proprietary network information" (CPNI), § 222(h)(1)(A), and gives customers certain rights to control use of and access to CPNI about themselves. The statute generally forbids a carrier to "use, disclose, or permit access to individually identifiable" CPNI without the customer's consent, except as needed to provide the customer's telecommunications services. § 222(c)(1). It also requires the carrier to disclose CPNI "upon affirmative written request by the customer, to any person designated by the customer." § 222(c)(2). Congress even

afforded customers a private cause of action for damages against carriers who violate the Act's terms. § 207. Plainly, customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use. Those interests might even rise to the level of a property right.

The problem is that we do not know anything more. Before the district court and court of appeals, Mr. Carpenter pursued only a *Katz* "reasonable expectations" argument. He did not invoke the law of property or any analogies to the common law, either there or in his petition for certiorari. Even in his merits brief before this Court, Mr. Carpenter's discussion of his positive law rights in cell-site data was cursory. He offered no analysis, for example, of what rights state law might provide him in addition to those supplied by § 222. In these circumstances, I cannot help but conclude—reluctantly—that Mr. Carpenter forfeited perhaps his most promising line of argument.

Unfortunately, too, this case marks the second time this Term that individuals have forfeited Fourth Amendment arguments based on positive law by failing to preserve them. See *Byrd,* 584 U.S., at ——, 138 S.Ct., at 1526. Litigants have had fair notice since at least *United States v. Jones* (2012) and *Florida v. Jardines* (2013) that arguments like these may vindicate Fourth Amendment interests even where *Katz* arguments do not. Yet the arguments have gone unmade, leaving courts to the usual *Katz* handwaving. These omissions do not serve the development of a sound or fully protective Fourth Amendment jurisprudence.

All Citations

138 S.Ct. 2206, 201 L.Ed.2d 507, 86 USLW 4491, 18 Cal. Daily Op. Serv. 6081, 2018 Daily Journal D.A.R. 6026, 27 Fla. L. Weekly Fed. S 415

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, 50 L.Ed. 499.

1 Justice KENNEDY believes that there is such a rubric—the "property-based concepts" that *Katz* purported to move beyond. *Post,* at 2224 (dissenting opinion). But while property rights are often informative, our cases by no means suggest that such an interest is "fundamental" or "dispositive" in determining which expectations of privacy are legitimate. *Post,* at 2227 - 2228. Justice THOMAS (and to a large extent Justice GORSUCH) would have us abandon *Katz* and return to an exclusively property-based approach. *Post,* at 2235 - 2236, 2244 - 2246 (THOMAS J., dissenting); *post,* at 2264 - 2266 (GORSUCH, J., dissenting). *Katz* of course "discredited" the "premise that property interests control," 389 U.S., at 353, 88 S.Ct. 507, and we have repeatedly emphasized that privacy interests do not rise or fall with property rights, see, *e.g., United States v. Jones,* 565 U.S. 400, 411, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012) (refusing to "make trespass the exclusive test"); *Kyllo v. United States,* 533 U.S. 27, 32, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property."). Neither party has asked the Court to reconsider *Katz* in this case.

2 Justice KENNEDY argues that this case is in a different category from *Jones* and the dragnet-type practices posited in *Knotts* because the disclosure of the cell-site records was subject to "judicial authorization." *Post,* at 2230 - 2232. That line of argument conflates the threshold question whether a "search" has occurred with the separate matter of whether the search was reasonable. The subpoena process set forth in the Stored Communications Act does not determine a target's expectation of privacy. And in any event, neither *Jones* nor *Knotts* purported to resolve the question of what authorization may be required to conduct such electronic surveillance techniques. But see *Jones,* 565 U.S., at 430, 132 S.Ct. 945 (ALITO, J., concurring in judgment) (indicating that longer term GPS tracking may require a warrant).

3 The parties suggest as an alternative to their primary submissions that the acquisition of CSLI becomes a search only if it extends beyond a limited period. See Reply Brief 12 (proposing a 24–hour cutoff); Brief for United States 55–56 (suggesting a seven-day cutoff). As part of its argument, the Government treats the seven days of CSLI requested from Sprint as the pertinent period, even though Sprint produced only two days of records. Brief for United States 56. Contrary to Justice KENNEDY's assertion, *post,* at 2233, we need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient for our purposes today to hold that accessing seven days of CSLI constitutes a Fourth Amendment search.

4 Justice GORSUCH faults us for not promulgating a complete code addressing the manifold situations that may be

presented by this new technology—under a constitutional provision turning on what is "reasonable," no less. *Post,* at 2266 - 2268. Like Justice GORSUCH, we "do not begin to claim all the answers today," *post,* at 2268, and therefore decide no more than the case before us.

5 See *United States v. Dionisio,* 410 U.S. 1, 14, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973) ("No person can have a reasonable expectation that others will not know the sound of his voice"); *Donovan v. Lone Steer, Inc.,* 464 U.S. 408, 411, 415, 104 S.Ct. 769, 78 L.Ed.2d 567 (1984) (payroll and sales records); *California Bankers Assn. v. Shultz,* 416 U.S. 21, 67, 94 S.Ct. 1494, 39 L.Ed.2d 812 (1974) (Bank Secrecy Act reporting requirements); *See v. Seattle,* 387 U.S. 541, 544, 87 S.Ct. 1737, 18 L.Ed.2d 943 (1967) (financial books and records); *United States v. Powell,* 379 U.S. 48, 49, 57, 85 S.Ct. 248, 13 L.Ed.2d 112 (1964) (corporate tax records); *McPhaul v. United States,* 364 U.S. 372, 374, 382, 81 S.Ct. 138, 5 L.Ed.2d 136 (1960) (books and records of an organization); *United States v. Morton Salt Co.,* 338 U.S. 632, 634, 651–653, 70 S.Ct. 357, 94 L.Ed. 401 (1950) (Federal Trade Commission reporting requirement); *Oklahoma Press Publishing Co. v. Walling,* 327 U.S. 186, 189, 204–208, 66 S.Ct. 494, 90 L.Ed. 614 (1946) (payroll records); *Hale v. Henkel,* 201 U.S. 43, 45, 75, 26 S.Ct. 370, 50 L.Ed. 652 (1906) (corporate books and papers).

1 Justice Brandeis authored the principal dissent in *Olmstead.* He consulted the "underlying purpose," rather than "the words of the [Fourth] Amendment," to conclude that the wiretap was a search. 277 U.S., at 476, 48 S.Ct. 564. In Justice Brandeis' view, the Framers "recognized the significance of man's spiritual nature, of his feelings and of his intellect" and "sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations." *Id.,* at 478, 48 S.Ct. 564. Thus, "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed," should constitute an unreasonable search under the Fourth Amendment. *Ibid.*

2 National Archives, Library of Congress, Founders Online, https://founders.archives.gov (all Internet materials as last visited June 18, 2018).

3 A Century of Lawmaking For A New Nation, U.S. Congressional Documents and Debates, 1774–1875 (May 1, 2003), https://memory.loc.gov/ammem/amlaw/lawhome.html.

4 Corpus of Historical American English, https://corpus.byu.edu/coha; Google Books (American), https://googlebooks.byu.edu/x.asp; Corpus of Founding Era American English, https://lawncl.byu.edu/cofea.

5 Readex, America's Historical Newspapers (2018), https://www.readex.com/content/americas-historical-newspapers.

6 Writs of assistance were "general warrants" that gave "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." *Stanford v. Texas,* 379 U.S. 476, 481, 85 S.Ct. 506, 13 L.Ed.2d 431 (1965).

7 "Every subject has a right to be secure from all unreasonable searches and seizures of his person, his house, his papers, and all his possessions. All warrants, therefore, are contrary to right, if the cause or foundation of them be not previously supported by oath or affirmation, and if the order in the warrant to a civil officer, to make search in suspected places, or to arrest one or more suspected persons, or to seize their property, be not accompanied with a special designation of the person or objects of search, arrest, or seizure; and no warrant ought to be issued but in cases, and with the formalities prescribed by the laws." Mass. Const., pt. I, Art. XIV (1780).

8 The answer to that question is not obvious. Cell-site location records are business records that mechanically collect the interactions between a person's cell phone and the company's towers; they are not private papers and do not reveal the contents of any communications. Cf. Schnapper, Unreasonable Searches and Seizures of Papers, 71 Va. L. Rev. 869, 923–924 (1985) (explaining that business records that do not reveal "personal or speech-related confidences" might not satisfy the original meaning of "papers").

9 Carpenter relies on an order from the Federal Communications Commission (FCC), which weakly states that " '*[t]o the extent* [a customer's location information] is property, ... it is better understood as belonging to the customer, not the carrier.' " Brief for Petitioner 34, and n. 23 (quoting 13 FCC Rcd. 8061, 8093 ¶ 43 (1998); emphasis added). But this order was vacated by the Court of Appeals for the Tenth Circuit. *U.S. West, Inc. v. FCC,* 182 F.3d 1224, 1240 (1999). Notably, the carrier in that case argued that the FCC's regulation of customer information was a taking of *its* property. See *id.,* at 1230. Although the panel majority had no occasion to address this argument, see *id.,* at 1239, n. 14, the dissent concluded that the carrier had failed to prove the information was "property" at all, see *id.,* at 1247–1248 (opinion of Briscoe, J.).

10 Kugler & Strahilevitz, Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory, 2015 S.Ct.

Rev. 205, 261; Bradley, Two Models of the Fourth Amendment, 83 Mich. L. Rev. 1468 (1985); Kerr, Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 505 (2007); Solove, Fourth Amendment Pragmatism, 51 Boston College L. Rev. 1511 (2010); Wasserstom & Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 29 (1988); Colb, What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy, 55 Stan. L. Rev. 119, 122 (2002); Clancy, The Fourth Amendment: Its History and Interpretation § 3.3.4, p. 65 (2008); *Minnesota v. Carter,* 525 U.S. 83, 97, 119 S.Ct. 469, 142 L.Ed.2d 373 (1998) (Scalia, J., dissenting); *State v. Campbell,* 306 Ore. 157, 164, 759 P.2d 1040, 1044 (1988); Wilkins, Defining the "Reasonable Expectation of Privacy": an Emerging Tripartite Analysis, 40 Vand. L. Rev. 1077, 1107 (1987); Yeager, Search, Seizure and the Positive Law: Expectations of Privacy Outside the Fourth Amendment, 84 J.Crim. L. & C. 249, 251 (1993); Thomas, Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment, 80 Notre Dame L. Rev. 1451, 1500 (2005); *Rakas v. Illinois,* 439 U.S. 128, 165, 99 S.Ct. 421, 58 L.Ed.2d 387 (1978) (White, J., dissenting); Cloud, Rube Goldberg Meets the Constitution: The Supreme Court, Technology, and the Fourth Amendment, 72 Miss. L.J. 5, 7 (2002).

1 Any other interpretation of the Fourth Amendment's text would run into insuperable problems because it would apply not only to subpoenas *duces tecum* but to all other forms of compulsory process as well. If the Fourth Amendment applies to the compelled production of documents, then it must also apply to the compelled production of testimony—an outcome that we have repeatedly rejected and which, if accepted, would send much of the field of criminal procedure into a tailspin. See, *e.g., United States v. Dionisio,* 410 U.S. 1, 9, 93 S.Ct. 764, 35 L.Ed.2d 67 (1973) ("It is clear that a subpoena to appear before a grand jury is not a 'seizure' in the Fourth Amendment sense, even though that summons may be inconvenient or burdensome"); *United States v. Calandra,* 414 U.S. 338, 354, 94 S.Ct. 613, 38 L.Ed.2d 561 (1974) ("Grand jury questions ... involve no independent governmental invasion of one's person, house, papers, or effects"). As a matter of original understanding, a subpoena *duces tecum* no more effects a "search" or "seizure" of papers within the meaning of the Fourth Amendment than a subpoena *ad testificandum* effects a "search" or "seizure" of a person.

2 All that the Court can say in response is that we have "been careful not to uncritically extend existing precedents" when confronting new technologies. *Ante,* at 2222. But applying a categorical rule categorically does not "extend" precedent, so the Court's statement ends up sounding a lot like a tacit admission that it is overruling our precedents.

3 See, *e.g.,* Freedom of Information Act, 5 U.S.C. § 552(a) ("Each agency shall make available to the public information as follows ..."); Privacy Act, 5 U.S.C. § 552a(d)(1) ("Each agency that maintains a system of records shall ... upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof ..."); Fair Credit Reporting Act, 15 U.S.C. § 1681j(a)(1)(A) ("All consumer reporting agencies ... shall make all disclosures pursuant to section 1681g of this title once during any 12-month period upon request of the consumer and without charge to the consumer"); Right to Financial Privacy Act of 1978, 12 U.S.C. § 3404(c) ("The customer has the right ... to obtain a copy of the record which the financial institution shall keep of all instances in which the customer's record is disclosed to a Government authority pursuant to this section, including the identity of the Government authority to which such disclosure is made"); Government in the Sunshine Act, 5 U.S.C. § 552b(f)(2) ("Copies of such transcript, or minutes, or a transcription of such recording disclosing the identity of each speaker, shall be furnished to any person at the actual cost of duplication or transcription"); Cable Act, 47 U.S.C. § 551(d) ("A cable subscriber shall be provided access to all personally identifiable information regarding that subscriber which is collected and maintained by a cable operator"); Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g(a)(1)(A) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy of denying, or which effectively prevents, the parents of students who are or have been in attendance at a school of such agency or at such institution, as the case may be, the right to inspect and review the education records of their children.... Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made").

4 See, *e.g.,* Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g(b)(1) ("No funds shall be made available under any applicable program to any educational agency or institution which has a policy or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information ...) of students without the written consent of their parents to any individual, agency, or organization ..."); Video Privacy Protection Act, 18 U.S.C. § 2710(b)(1) ("A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (d)"); Driver Privacy Protection Act, 18 U.S.C. § 2721(a)(1) ("A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity ... personal information ..."); Fair Credit Reporting Act, 15 U.S.C. § 1681b(a) ("[A]ny consumer reporting agency may furnish a consumer report under the following circumstances and no other .."); Right

to Financial Privacy Act, 12 U.S.C. § 3403(a) ("No financial institution, or officer, employees, or agent of a financial institution, may provide to any Government authority access to or copies of, or the information contained in, the financial records of any customer except in accordance with the provisions of this chapter"); Patient Safety and Quality Improvement Act, 42 U.S.C. § 299b–22(b) ("Notwithstanding any other provision of Federal, State, or local law, and subject to subsection (c) of this section, patient safety work product shall be confidential and shall not be disclosed"); Cable Act, 47 U.S.C. § 551(c)(1) ("[A] cable operator shall not disclose personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber concerned and shall take such actions as are necessary to prevent unauthorized access to such information by a person other than the subscriber or cable operator").

5 Carpenter also cannot argue that he owns the cell-site records merely because they fall into the category of records referred to as "customer proprietary network information." 47 U.S.C. § 222(c). Even assuming labels alone can confer property rights, nothing in this particular label indicates whether the "information" is "proprietary" to the "customer" or to the provider of the "network." At best, the phrase "customer proprietary network information" is ambiguous, and context makes clear that it refers to the *provider* 's information. The Telecommunications Act defines the term to include all "information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." 47 U.S.C. § 222(h)(1)(A). For Carpenter to be right, he must own not only the cell-site records in this case, but also records relating to, for example, the "technical configuration" of his subscribed service—records that presumably include such intensely personal and private information as transmission wavelengths, transport protocols, and link layer system configurations.

6 Thus, this is not a case in which someone has entrusted papers that he or she owns to the safekeeping of another, and it does not involve a bailment. Cf. *post,* at 2268 - 2269 (GORSUCH, J., dissenting).

End of Document

KeyCite Yellow Flag - Negative Treatment
Distinguished by Hashem v. Hunterdon County, D.N.J., September 29, 2016

804 F.3d 277
United States Court of Appeals,
Third Circuit.

Syed Farhaj HASSAN; The Council of Imams in New Jersey; Muslim Students Association of the U.S. and Canada, Inc.; All Body Shop Inside & Outside; Unity Beef Sausage Company; Muslim Foundation Inc.; Moiz Mohammed; Jane Doe; Soofia Tahir; Zaimah Abdur-Rahim; Abdul-Hakim Abdullah, Appellants
v.
The CITY OF NEW YORK.

No. 14-1688.
|
Argued Jan. 13, 2015.
|
Opinion Filed Oct. 13, 2015.
|
As Amended Feb. 2, 2016.

Synopsis
Background: Persons associated with Islam commenced action against municipality pursuant to § 1983 and *Monell* alleging violation of their rights under Free Exercise and Establishment Clauses and Equal Protection Clause as result of police surveillance program. The United States District Court for the District of New Jersey, William J. Martini, J., 2014 WL 654604, dismissed the action. Plaintiffs appealed.

Holdings: The Court of Appeals, Ambro, Circuit Judge, held that:

[1] discriminatory classification, where citizen's right to equal treatment was at stake, qualified as actual injury for standing purposes;

[2] persons associated with Islam who claimed to be targets of police surveillance program had been affected in personal and individual way, as required to satisfy injury in fact for standing;

[3] causal connection existed between police surveillance program targeting persons associated with Islam and those persons targeted who had alleged harm from program;

[4] redressability, as required for standing, was satisfied;

[5] plaintiffs plausibly alleged surveillance program with facially discriminatory classification;

[6] invidious motive was not necessary element of discriminatory intent;

[7] on issue of first impression, religious-based classifications were subject to heightened scrutiny; and

[8] municipality's assurance that police surveillance was justified by national-security and public-safety concerns did not satisfy its burden of producing evidence to overcome heightened scrutiny's presumption of violation of equal protection.

Reversed and remanded.

Roth, Circuit Judge, filed concurring opinion.

West Headnotes (38)

[1] **Federal Civil Procedure**
In general; injury or interest

Standing to sue is required for jurisdiction in a federal forum; derived from Article III of the Constitution, it is the threshold inquiry in every case, one for which the party invoking federal jurisdiction bears the burden of proof. U.S.C.A. Const. Art. 3, § 2, cl. 1.

[2] **Federal Civil Procedure**
In general; injury or interest

When analyzing standing, a court must assume that the party asserting federal jurisdiction is correct on the legal merits of his claim, that a decision on the merits would be favorable, and that the requested relief would be granted; in

other words, to withstand a "facial attack" at the motion-to-dismiss stage, a plaintiff need only plausibly allege facts establishing each constitutional requirement. U.S.C.A. Const. Art. 3, § 2, cl. 1.

3 Cases that cite this headnote

[3] **Federal Civil Procedure**
In general; injury or interest

A plaintiff alleges injury-in-fact, as required for standing, when it claims that it has, or is in imminent danger of having, suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural and hypothetical. U.S.C.A. Const. Art. 3, § 2, cl. 1.

1 Cases that cite this headnote

[4] **Federal Civil Procedure**
In general; injury or interest

When analyzing standing, the burden for alleging injury in fact is low, requiring nothing more than an identifiable trifle of harm. U.S.C.A. Const. Art. 3, § 2, cl. 1.

1 Cases that cite this headnote

[5] **Constitutional Law**
Criminal Law
Constitutional Law
Criminal Law

Persons of or associated with the Islamic faith suffered injury-in-fact as result of police surveillance program designed to monitor the lives of Muslims, their businesses, houses of worship, organizations, and schools, as required to give them Article III standing to challenge the constitutionality of the program under the establishment and free exercise clauses of the First Amendment and the equal protection clause of the Fourteenth Amendment; discriminatory classification alone was sufficient, even if it did not involve a tangible benefit or overt condemnation of the Muslim religion. U.S.C.A. Const. Art. 3, § 2, cl. 1; U.S.C.A. Const.Amends. 1, 14.

2 Cases that cite this headnote

[6] **Constitutional Law**
Freedom of Religion and Conscience

The First Amendment's guarantee of freedom of religion includes freedom from religious discrimination. U.S.C.A. Const.Amend. 1.

[7] **Constitutional Law**
Freedom of Speech, Expression, and Press
Constitutional Law
Religion

The Religion Clauses and the Equal Protection Clause as applied to religion all speak with one voice on this point: absent the most unusual circumstances, one's religion ought not affect one's legal rights or duties or benefits. U.S.C.A. Const.Amends. 1, 14.

[8] **Federal Civil Procedure**
Rights of third parties or public

Only a complainant who possesses something more than a general interest in the proper execution of the laws is in a position to secure judicial intervention; but where a plaintiff is asserting his or her own equality right, a claim of discrimination, even where it affects a broad class, is not an abstract concern or generalized grievance for standing purposes. U.S.C.A. Const. Art. 3, § 2, cl. 1.

1 Cases that cite this headnote

[9] **Constitutional Law**
Criminal Law
Constitutional Law
Criminal Law

Persons associated with Islam who claimed to be targets of police surveillance program had been affected in personal and individual way, as required to satisfy injury in fact for standing to bring action against municipality pursuant to § 1983 and *Monell* on allegations of violation of their rights under Free Exercise and Establishment Clauses and Equal Protection Clause; even if program injured hundreds or thousands of other persons, individualized nature of asserted rights and interests at stake was not changed. U.S.C.A. Const. Art. 3, § 2, cl. 1; U.S.C.A. Const.Amends. 1, 14; 42 U.S.C.A. § 1983.

1 Cases that cite this headnote

[10] **Constitutional Law**
Criminal Law
Constitutional Law
Criminal Law

Causal connection existed between police surveillance program targeting persons associated with Islam and those persons targeted who had alleged harm from program, as required to satisfy injury in fact for standing to bring action against municipality pursuant to § 1983 and *Monell* on allegations of violation of their rights under Free Exercise and Establishment Clauses and Equal Protection Clause; even if those persons did not realize they had been targeted, discrimination itself was legally cognizable injury and collateral consequences of discrimination could count as Article III injury. U.S.C.A. Const. Art. 3, § 2, cl. 1; U.S.C.A. Const.Amends. 1, 14; 42 U.S.C.A. § 1983.

1 Cases that cite this headnote

[11] **Federal Civil Procedure**
Causation; redressability

There is room for concurrent causation in the analysis of standing; an indirect causal relationship will suffice, so long as there is a fairly traceable connection. U.S.C.A. Const. Art. 3, § 2, cl. 1.

[12] **Federal Civil Procedure**
Causation; redressability

Redressability, as required for standing, requires a plaintiff to show that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision. U.S.C.A. Const. Art. 3, § 2, cl. 1.

[13] **Federal Civil Procedure**
Causation; redressability

Redressability, as required for standing, is easily established in a case where the alleged injury arises from an identifiable discriminatory policy; while a court cannot predict the exact nature of the possible relief without a full development of the facts, an order enjoining the policy and requiring non-discriminatory investigation and enforcement would redress the injury. U.S.C.A. Const. Art. 3, § 2, cl. 1.

1 Cases that cite this headnote

[14] **Constitutional Law**
Criminal Law
Constitutional Law

Criminal Law

Redressability, as required for standing to bring claims under Free Exercise and Establishment Clauses and Equal Protection Clause, was satisfied by past harms from police surveillance program targeting persons associated with Islam; targeted persons could recover compensatory damages for out-of-pocket losses or emotional distress, or they could obtain public declaration that they were right and were improperly treated, along with nominal damages to serve as symbolic vindication of their constitutional rights. U.S.C.A. Const. Art. 3, § 2, cl. 1; U.S.C.A. Const.Amends. 1, 14; Restatement (Second) of Torts § 901.

1 Cases that cite this headnote

[15] **Constitutional Law**
Particular claims

Persons associated with Islam stated equal protection civil rights claim based on police surveillance program with facially discriminatory classification, where those persons alleged specifics about program, including when it was conceived, where municipality implemented it, why it was employed, and they articulated variety of methods by which surveillance was carried out. U.S.C.A. Const.Amend. 14; 42 U.S.C.A. § 1983.

[16] **Constitutional Law**
Investigation in general; searches

A claim of selective investigation by the police draws on ordinary equal protection standards; as with other equal-protection claims, a court asks whether the municipality intentionally discriminates against a reasonably identifiable group and whether that intentional discrimination is nonetheless legally justified. U.S.C.A. Const.Amend. 14.

2 Cases that cite this headnote

[17] **Constitutional Law**
Intentional or purposeful action requirement

To state an equal-protection claim, plaintiffs must allege intentional discrimination. U.S.C.A. Const.Amend. 14.

28 Cases that cite this headnote

[18] **Constitutional Law**
Intentional or purposeful action requirement

An equal-protection claim based on a policy of intentional discrimination may be based on a policy that has not been reduced to a written form. U.S.C.A. Const.Amend. 14.

5 Cases that cite this headnote

[19] **Constitutional Law**
Investigation in general; searches

Although a lack of reasonable suspicion does not afford a presumption that a law-enforcement officer initiated an investigation on the basis of a protected characteristic, it is certainly one factor that may be considered by a finder of fact on an equal-protection claim based on a policy of intentional discrimination through selective investigation. U.S.C.A. Const.Amend. 14.

2 Cases that cite this headnote

[20] **Constitutional Law**
Investigation in general; searches
Criminal Law
Prevention and Investigation of Crime

Invidious motive was not necessary element of discriminatory intent, on equal protection claim of selective investigation by police; state actor only had to mean to single out plaintiff because of protected characteristic itself. U.S.C.A. Const.Amend. 14.

6 Cases that cite this headnote

[21] **Constitutional Law**
Investigation in general; searches

While the absence of a legitimate motive may bear on whether the challenged surveillance survives the appropriate level of equal-protection scrutiny on claim of selective investigation by police, intentional discrimination need not be motivated by ill will, enmity, or hostility to contravene the Equal Protection Clause. U.S.C.A. Const.Amend. 14.

1 Cases that cite this headnote

[22] **Constitutional Law**
Intentional or purposeful action requirement

On an equal protection claim, once a plaintiff demonstrates treatment different from others with whom he or she is similarly situated and that the unequal treatment is the result of intentional discrimination, the adequacy of the reasons for that discrimination are separately assessed at equal protection's second step under the appropriate standard of review. U.S.C.A. Const.Amend. 14.

13 Cases that cite this headnote

[23] **Constitutional Law**
Differing levels set forth or compared

At a minimum, intentional discrimination against any "identifiable group" is subject to rational-basis review on an equal protection claim, which requires the classification to be rationally related to a legitimate governmental purpose; however, where a "quasi-suspect" or "suspect" classification is at issue, the challenged action must survive "intermediate scrutiny" or "strict scrutiny." U.S.C.A. Const.Amend. 14.

6 Cases that cite this headnote

[24] **Constitutional Law**
Intermediate scrutiny in general

On an equal protection claim, intermediate scrutiny, applicable to quasi-suspect classes like gender and illegitimacy, requires a classification to be substantially related to an important governmental objective. U.S.C.A. Const.Amend. 14.

1 Cases that cite this headnote

[25] **Constitutional Law**
Strict scrutiny and compelling interest in general

On an equal protection claim, strict scrutiny, applicable to suspect classes like race and nationality, requires the classification to be narrowly tailored to further a compelling governmental interest. U.S.C.A. Const.Amend. 14.

1 Cases that cite this headnote

[26] **Constitutional Law**
Strict or heightened scrutiny; compelling interest

"Strict scrutiny" is triggered in the case of a "fundamental right."

[27] **Constitutional Law**
Free Exercise of Religion

The right to free exercise of religion is fundamental. U.S.C.A. Const.Amend. 1.

1 Cases that cite this headnote

[28] **Courts**
Dicta

Supreme Court dicta requires serious consideration, especially when is encountered with a decades-long succession of statements from the Court.

1 Cases that cite this headnote

[29] **Constitutional Law**
Religion

Intentional discrimination based on religious affiliation must survive heightened equal-protection review. U.S.C.A. Const.Amend. 14.

3 Cases that cite this headnote

[30] **Constitutional Law**
Intermediate scrutiny in general
Constitutional Law
Strict scrutiny and compelling interest in general

In designating a particular classification as "suspect" or "quasi-suspect" under the Equal Protection Clause, a variety of factors are considered that are grouped around the central idea of whether the discrimination embodies a gross unfairness that is so sufficiently inconsistent with the ideals of equal protection to term it "invidious"; among these are whether the class is defined by an immutable trait that frequently bears no relation to ability to perform or contribute to society and whether the class has been saddled with unique disabilities because of prejudice or inaccurate stereotypes, but experience, not abstract logic, must be the primary guide. U.S.C.A. Const.Amend. 14.

1 Cases that cite this headnote

[31] **Constitutional Law**
Heightened Levels of Scrutiny

A classification is more likely to receive heightened equal protection scrutiny if it discriminates against individuals based on a characteristic that they either cannot realistically change or ought not be compelled to change because it is fundamental to their identities. U.S.C.A. Const.Amend. 14.

[32] **Constitutional Law**
Differing levels set forth or compared

Under the equal protection clause, the higher the scrutiny required, the more persuasive must be the governmental objective and the snugger the means-ends fit; thus, while it usually matters little for purposes of rational-basis review that a governmental interest is not exceedingly important or that other means are better suited to the achievement of governmental ends, heightened scrutiny demands a much stronger justification and a much tighter relationship between the means employed and the ends served. U.S.C.A. Const.Amend. 14.

[33] **Constitutional Law**
Equal protection

On an equal protection claim, while the rational-basis standard usually puts the burden of proof on the classification's opponent and permits a court to hypothesize interests that might support the governmental distinctions, the burden of justification under both intermediate and strict scrutiny is demanding and rests entirely on the government. U.S.C.A. Const.Amend. 14.

1 Cases that cite this headnote

[34] **Constitutional Law**
Criminal Law
Criminal Law
Prevention and Investigation of Crime

Municipality's assurance that police surveillance of persons associated with Islam was justified by national-security and public-safety concerns did not satisfy its burden of producing evidence to overcome heightened scrutiny's presumption of violation of equal protection. U.S.C.A. Const.Amend. 14.

[35] **Civil Rights**
Weight and Sufficiency of Evidence

On an equal protection claim, heightened scrutiny requires substantiation of the relationship between the asserted justification and discriminatory means employed by objective evidence; mere speculation or conjecture is insufficient as are appeals to common sense which might be inflected by stereotypes. U.S.C.A. Const.Amend. 14.

[36] **Constitutional Law**
Strict scrutiny and compelling interest in general

On an equal protection claim, while a classification does not fail rational-basis review because it is not made with mathematical nicety or because in practice it results in some inequality, strict scrutiny requires that the classification at issue "fit" with greater precision than any alternative means. U.S.C.A. Const.Amend. 14.

[37] **Civil Rights**
Criminal law enforcement; prisons

Opinion of state attorney general that police surveillance program did not violate state law was not relevant to issue of whether program violated federal constitution.

[38] **Constitutional Law**
Criminal Law
Criminal Law
Prevention and Investigation of Crime

Absence of subjective hostility by government was not relevant to issue of whether government violated Establishment Clause or Free Exercise Clause through police surveillance of persons associated with Islam. U.S.C.A. Const.Amend. 1.

Attorneys and Law Firms

***282** Baher A. Azmy, Esquire, (Argued), Ghita Schwarz, Esquire, Omar Farah, Esquire, Center for Constitutional Rights, New York, N.Y., Glenn Katon, Esquire, Farhana Khera, Esquire, Adil Haq, Esquire, Muslim Advocates, Oakland, CA, Lawrence S. Lustberg, Esquire, Joseph A. Pace, Esquire, Portia Dolores Pedro, Esquire, Gibbons, Newark, NJ, Counsel for Appellants.

Zachary W. Carter, Corporation Counsel of the City of New York, Richard P. Dearing, Esquire, Peter G. Farrell, Esquire, (Argued), Celeste Koeleveld, Esquire, Alexis Leist, Esquire, Anthony DiSenso, Esquire, William Oates, Esquire, Cheryl Shammas, Esquire, Odile Farrell, Esquire, New York City Law Department, New York, N.Y., Counsel for Appellee.

Ayesha N. Khan, Esquire, Gregory M. Lipper, Esquire, Alexander J. Luchenitser, Esquire, Americans United for Separation of Church and State, Washington, DC, Counsel for Amicus Appellant, Americans United for Separation of Church and State.

Benjamin C. Block, Esquire, William Murray, Esquire, Covington & Burling LLP, Washington, DC, Stephen J. Schulhofer, Esquire, New York, N.Y., Robert L. Rusky, Esquire, San Francisco, CA, Counsel for Amicus Appellants, Karen Korematsu, Jay Hirabayashi, Holly Yasui.

***283** Brian D. Boyle, Esquire, Walter E. Dellinger, III, Esquire, Deanna M. Rice, Esquire, Nausheen Hassan, Esquire, O'Melveny & Myers LLP, Washington, DC, Counsel for Amicus Appellants, 100 Blacks in Law Enforcement Who Care, Chris Burbank, Eric Adams.

Gregory J. Wallance, Esquire, W. Stewart Wallace, Esquire, Kaye Scholer LLP, New York, N.Y., Michael Robertson, Esquire, Kaye Scholer LLP, Washington, DC, Counsel for Amicus Appellants, Asian American Legal Defense and Education Fund, American Arab Anti–Discrimination Committee, Universal Muslim Association of America Advocacy, South Asian Americans Leading Together, Shia Rights Watch, New Jersey Muslim Lawyers Association, National Network for Arab American Communities, National Lawyers Guild New York City Chapter, Muslim Public Affairs Council, Muslim Legal Fund of America, Muslim Consultative Network, Muslim Bar Association of New York, Muslim American Civil Liberties Coalition, Creating Law Enforcement Accountability and Responsibility, Arab American Association of New York, Asian Americans Advancing Justice–Asian Law Caucus, South Asian Organization, Project SALAM.

Ronald K. Chen, Esquire, Rutgers University Constitutional Rights Clinic, Newark, NJ, Edward Barocas, Esquire, Jeanne LoCicero, Esquire, Alexander Shalom, Esquire, American Civil Liberties Union of New Jersey Foundation, Newark, NJ, Counsel for Amicus Appellants, American Civil Liberties Union of New Jersey, LatinoJustice PRLDEF, Mexican American Legal Defense and Educational Fund, Bill of Rights Defense Committee, Garden State Bar, Association, Hispanic Bar Association of New Jersey, Association of Black Women Lawyers of New Jersey.

Bruce D. Brown, Esquire, Gregg P. Leslie, Esquire, Jamie T. Schuman, Esquire, Reporters Committee for Freedom of the Press, Arlington, VA, Jennifer A. Borg, Esquire, North Jersey Media Group Inc., Woodland Park, NJ, Counsel for Amicus Appellants, Reporters Committee for Freedom of the Press, North Jersey Media Group Inc.

Michael W. Price, Esquire, Faiza Patel, Esquire, Brennan Center for Justice at NYU School of Law, New York, N.Y., Counsel for Amicus Appellant, Brennan Center for Justice at New York University School of Law

Allen P. Pegg, Esquire, Hogan Lovells U.S. LLP, Miami, FL, Counsel for Amicus Appellants, Sikh Coalition, Interfaith Alliance Foundation, National Council of the Churches of Christ in the USA, Union for Reform Judaism, Central Conference of American Rabbis, Women of Reform Judaism, Islamic Society of North America, Bend the Arc: A Jewish Partnership for Justice, Hindu Temple Society of North America, Auburn Theological Seminary, National Council of Jewish Women, Universal Muslim Association of America, American Humanist Association, Sikh American Legal Defense and Education Fund, Muslim Alliance in North America National Religious Campaign Against Torture, Reconstructionist Rabbinical Association, Imam Mahdi Association of Marjaeya, Muslims for Peace, T'ruah: The Rabbinic Call for Human Rights, Ta'leef Collective, Muslim Congress, Unitarian Universalist Legislative Ministry of New Jersey, Queens Federation of Churches, Inc., Northern California Islamic Council, Council of Islamic Organization of Greater Chicago, Islamic Shura Council of Southern California.

Before: AMBRO, FUENTES, and ROTH, Circuit Judges.

***284** OPINION OF THE COURT

AMBRO, Circuit Judge.

TABLE OF CONTENTS

I. INTRODUCTION

Plaintiffs appeal the dismissal of their civil-rights suit against the City of New York (the "City"). They claim to be targets of a wide-ranging surveillance program that the New York City Police Department (the "NYPD") began in the wake of the September 11, 2001 terrorist attacks (the "Program"). Plaintiffs allege that the Program is based on the false and stigmatizing premise that Muslim religious identity "is a permissible proxy for criminality, and that Muslim individuals, businesses, and institutions can therefore be subject to pervasive surveillance not visited upon individuals, businesses, and institutions of any other religious faith or the public at large." First Am. Compl. ¶ 6 (the "Complaint" or "Compl."). They bring this lawsuit "to affirm the principle that individuals may not be singled out for intrusive investigation and pervasive surveillance that cause them continuing harm simply because they profess a certain faith." *Id.* ¶ 8.

In its narrowest form, this appeal raises two questions: Do Plaintiffs—themselves allegedly subject to a discriminatory surveillance program—have standing to sue in federal court to vindicate their religious-liberty and equal-protection rights? If so, taking Plaintiffs' non-conclusory allegations as true, have they stated valid claims under the First and Fourteenth Amendments to our Constitution? Both of these questions, which we answer yes, seem straightforward enough. Lurking beneath the surface, however, are questions about equality, religious liberty, the role of ***285** courts in safeguarding our Constitution, and the protection of our civil liberties and rights equally during wartime and in peace.

II. BACKGROUNDA. Plaintiffs' Allegations

Lead Plaintiff Syed Faraj Hassan and others of or associated with the Islamic faith (collectively "Plaintiffs") assert that, since January 2002, the City has through the NYPD conducted the Program in secret "to monitor the lives of Muslims, their businesses, houses of worship, organizations, and schools in New York City and surrounding states, particularly New Jersey." *See* Pls.' Br. 2 (citing Compl. ¶¶ 36, 38). As this case comes before us on the City's Motion to Dismiss, we must take all facts alleged in Plaintiffs' Complaint as true and draw all reasonable inferences that arise therefrom in their favor. *See* Fed.R.Civ.P. 12(b)(6).

1. The Program

Plaintiffs contend that the NYPD launched the Program following the September 11, 2001 terrorist attacks with the goal of "infiltra[ting] and monitor[ing] Muslim life in and around New York City." Compl. ¶ 2. They claim that it "target[s] Muslim entities and individuals in New Jersey for investigation solely because they are Muslim or believed to be Muslim" rather than "based upon evidence

of wrongdoing." *Id.* ¶¶ 7, 47. Plaintiffs claim that the Program, going on its tenth year when the Complaint was filed, "has never generated a single lead." *Id.* ¶ 2.

Per the Complaint, the NYPD "uses a variety of methods to spy on Muslims." *Id.* ¶ 39. Among the techniques that it employs are to "snap pictures, take video, and collect license plate numbers of [mosque] congregants" and to "mount surveillance cameras on light poles, aimed at mosques," which "[o]fficers can [then] control [remotely] ... with their computers" and which generate footage used "to help identify worshippers." *Id.* ¶ 46. Plaintiffs also allege the NYPD sends "undercover officers"—some of which are called "mosque crawlers" and "rakers"—into mosques, student organizations, businesses, and neighborhoods that "it believes to be heavily Muslim." *Id.* ¶¶ 47, 49–50. By "monitor[ing] sermons and conversations in mosques" and "surveil[ling] locations such as bookstores, bars, cafes, and nightclubs," officers "document[ ] ... American Muslim life" in "painstaking detail[ ]" and "report back to the NYPD." *Id.* ¶ 47.

While Plaintiffs believe that some of this surveillance activity is passive (such as "tak[ing] video and photographs at mosques, Muslim-owned businesses, and schools," *id.* ¶ 39, and recording "the subject of conversations overheard at mosques," *id.* ¶ 47), in other cases NYPD officers more actively engage with the persons monitored. One alleged spying method of the latter type is to "sen [d] undercover officers to [Muslim-affiliated] locations to engage in pretextual conversations to elicit information from proprietors and patrons." *Id.* ¶ 39. Officers also "sometimes pose" as members of certain groups and organizations under investigation. *Id.* ¶ 50. The Complaint illustrates one such example where an NYPD "officer ... went on a rafting trip with a [ ] [Muslim Students Association (MSA)] and monitored and recorded how often the student participants on the trip prayed" and their "discuss[ion of] religious topics." *Id.*

Not only does the alleged Program "utilize[ ] numerous forms of surveillance," *id.* ¶ 45, but that surveillance is also widespread. Plaintiffs claim, for instance, that the NYPD "has strived to have an informant inside every mosque within a 250–mile radius of New York City" and has ***286** "place[d] informants or undercover officers in all or virtually all MSAs" at "colleges and universities in New York, New Jersey, Connecticut, and Pennsylvania ... without any indication whatsoever of criminal activity or any connection whatsoever to wrongdoing." *Id.* ¶¶ 47, 49. In all, the NYPD has allegedly "surveill[ed] ... at least twenty mosques, fourteen restaurants, eleven retail stores, two grade schools and two [MSAs], in addition to an untold number of individuals who own, operate, and visit those establishments." *Id.* ¶ 3.

Plaintiffs claim that, in addition to singling out organizations and businesses for surveillance that in some way are visibly or openly affiliated with Islam (such as mosques or businesses with prayer mats or other Islamic identifications), "the Program also intentionally targets Muslims by using ethnicity as a proxy for faith." *Id.* ¶ 40. Plaintiffs aver, for instance, that the NYPD "has designated twenty-eight countries ... constitut[ing] about 80% of the world's Muslim population" and "American Black Muslim" as "ancestries of interest." *Id.* ¶ 41. But the Program is still decidedly focused on religion. Thus, rather than "surveil all people and establishments with 'ancestries of interest,' " the NYPD "expressly chooses to exclude people and establishments with such 'ancestries' if they are not Muslim." *Id.* ¶ 42. This includes "Egyptians if they are Coptic Christians, Syrians if they are Jewish, or Albanians if they are Catholic or Orthodox Christian." *Id.* Conversely, Plaintiffs claim that the NYPD has examined other immigrant communities in Newark, New Jersey "for the presence of Muslims," such as the "Portuguese and Brazilian immigrant communities" notwithstanding that "Portugal and Brazil [are] ... not found on [the NYPD's] list of twenty-eight 'ancestries.' " *Id.* ¶ 44.

2. Reports and Informational Databases

Plaintiffs allege that the Program has resulted in "a series of reports documenting in detail the information obtained from [the NYPD's] surveillance of New Jersey Muslim communities." *Id.* ¶ 5. These "includ[e] a report focusing on the Muslim community in Newark" (the "Newark report"), *id.;* "more than twenty precinct-level maps of the City of Newark, noting the location of mosques and Muslim businesses and the ethnic composition of the Muslim community," *id.* ¶ 3; "analytical report[s] on every mosque within 100 miles" of New York City, *id.* ¶ 47; and a weekly "MSA Report on schools, including reports on Rutgers New Brunswick and Rutgers Newark," *id.* ¶ 51.

The information and records collected and compiled are extensive and varied. Among these are "pictures, ... video, ... and license plate numbers of [mosque] congregants," *id.* ¶ 46; intelligence about "where religious schools are located," *id.* ¶ 47; indications of religious affiliation and Muslim patronage of shops, restaurants, and grocery stores, *id.;* lists of "businesses owned or frequented by Muslims," *id.;* and "names of professors, scholars, and students" affiliated with MSAs, *id.* ¶ 51. The City also allegedly "compiles databases of new Muslim converts

who take Arabic names, as well as Muslims who take names that are perceived to be 'Western.' " *Id.* ¶ 55.

Besides names and other identifying information of individuals, businesses, and organizations, the NYPD reports include seemingly mundane and innocuous details about Muslim community life in New Jersey, such as: (1) "flyers are posted in shops advertising for Quran tutoring;" (2) "a picture of a mosque hangs in a grocery store;" (3) "a restaurant serves 'religious Muslims;' " (4) "customers visit a Dunkin' ***287** Donuts after Friday prayer;" (5) "a restaurant is located near a particular mosque;" (6) "employees or customers of establishments are observed wearing 'traditional clothing;' " (7) "Muslim prayer mats are hanging on the wall at an Indian restaurant;" and (8) "a store posts a sign that it will be closed on Friday in observance of Friday prayer." *Id.* ¶ 47. Finally, NYPD officers have compiled "the subject[s and details] of conversations overheard at mosques." *Id.* In one 2006 report, for instance, they "document[ed] twenty-three conversations at twenty mosques," though "[n]one of the information collected showed any indication of criminal activity." *Id.*

3. Fall–Out from the Program's Disclosure to the Public

Plaintiffs claim that, despite "initial secrecy," public knowledge of the alleged Program's existence "has become widespread in New Jersey and elsewhere." *Id.* ¶ 45. They also contend that a number of the allegedly generated reports "ha[ve] been widely publicized," *id.* ¶ 20, and that each Plaintiff has been "either specifically named in an NYPD spying report or is a member of at least one mosque or other association named in such a report," Pls.' Br. 21 (citing Compl. ¶¶ 12–15, 17–26, 28–29, 31–32, 34).

Plaintiffs have learned since the news broke, for instance, that the NYPD's so-called "Newark report" designates several of them as a "Location of Concern," defined "as, among other things, a 'location that individuals may find co-conspirators for illegal actions,' and a 'location that has demonstrated a significant pattern of illegal activities.' " Compl. ¶ 58. Similarly, the NYPD's "U.S.—Iran report" describes organizations believed to pose serious threats to New York City, such as Hezbollah and Hamas, along with a list of "Other Shi'a Locations in the vicinity of NYC," which include Plaintiff Muslim Foundation Inc. ("MFI") and Masjid–e–Ali mosque (owned and operated by MFI), "as well as three additional mosques attended by Plaintiff Hassan." *Id.* ¶ 60.

While Plaintiffs allege that the Program is stigmatizing by itself, they also claim these specific defamatory statements targeting them in particular have intensified their harms and that "New York City officials" have exacerbated these injuries by publicly "acknowledg[ing] the [Program's] existence" and "describing it as focused on 'threats' and as an attempt to document the 'likely whereabouts of terrorists.' " *Id.* ¶ 61. "Discussing the surveillance, [former] Mayor Bloomberg has stated publicly" that "[w]e're doing the right thing. We will continue to do the right thing." *Id.* ¶ 64. And "[former Police] Commissioner Kelly has said" that "[w]e're going to continue to do what we have to do to protect the [C]ity." *Id.* Plaintiffs state that these and other "official proclamations," which "falsely suggest that Muslims alone present a unique law enforcement threat," indicate "that [City officials] believe the NYPD's targeting of Muslims for surveillance on the basis of their religion is appropriate and will continue." *Id.* ¶¶ 64–65.

Plaintiffs also contend that, in large part because of the Program's alleged stigmatizing and reputational consequences, the surveillance has affected their worship and religious activities. For example, Plaintiff Hassan, a soldier in the U.S. Army who has worked in military intelligence, asserts that "[h]e has decreased his mosque attendance significantly" because of his belief that "being closely affiliated with mosques under surveillance by law enforcement" will jeopardize his ability to hold a security clearance and will tarnish his reputation among his fellow soldiers and diminish ***288** their trust in him. *Id.* ¶¶ 11–13. Likewise, Plaintiffs Moiz Mohammed, Jane Doe, and Soofia Tahir state that they now avoid (or have avoided) discussing their faith openly or at MSA meetings for fear of being watched and documented, *id.* ¶¶ 24–30, and Plaintiff Mohammad alleges that "[t]he stigma now attached to being a Muslim member of the MSA has caused [him] to avoid discussing his faith or his MSA participation in public and to avoid praying in places where non-Muslims might see him doing so," *id.* ¶ 25.

The individual Plaintiffs are not the only ones affected. The organizational Plaintiffs allege that the Program "has undermined their ability to fulfill their mission[s by] deterring potential members from joining and casting doubt on [their] ability to maintain the confidentiality of their membership." Pls.' Br. 6 (citing Compl. ¶ 17). According to the Complaint, two mosques that are members of Plaintiff Council of Imams in New Jersey, and that are named in the NYPD's Newark report, "have ... seen a decline in attendance ... as a result of the [NYPD's] surveillance" because their congregants can no longer worship freely knowing that law-enforcement agents or informants are likely in their midst. Compl. ¶ 15. Similarly, "[a]s affinity student groups, MSAs subject to surveillance ... are diminished in their ability to

establish viable student organizations that students will feel secure joining and participating in" and are less able "to embark upon integral partnerships with campus administrators and other organizations and [to] fulfill the spiritual needs of their members in a confidential manner." *Id.* ¶ 17. And Plaintiff MFI has changed its religious and educational programming to avoid controversial topics likely to stigmatize its membership further and to attract additional NYPD attention. *Id.* ¶ 23.

Finally, several Plaintiffs also contend that financial harm has accompanied their alleged religious, reputational, and stigmatizing injuries. For example, Plaintiffs All Shop Body Inside & Outside and Unity Beef Sausage Company claim that the surveillance has damaged their "business[es] by scaring away customers," *id.* ¶¶ 19, 21, and Plaintiffs Zaimah Abdur–Rahim and Abdul–Hakim Abdullah allege that the publication of the address and a photograph on the Internet of their home "in connection with the NYPD's surveillance ... has decreased [its] value ... and diminished [its] prospects for sale," *id.* ¶¶ 31–32, 34. Also, two of Plaintiff Council of Imams in New Jersey's member mosques have witnessed "[l]osses in ... financial support," which further "harm[s] both mosques' ability to fulfill their religious missions." *Id.* ¶ 15.

B. District Court

In June 2012, Plaintiffs sued the City pursuant to 42 U.S.C. § 1983 and *Monell v. Department of Social Services of the City of New York,* 436 U.S. 658, 98 S.Ct. 2018, 56 L.Ed.2d 611 (1978), for discriminating against them as Muslims in violation of the Free Exercise and Establishment Clauses of the First Amendment and the Equal Protection Clause of the Fourteenth Amendment. They seek expungement of any unlawfully obtained records pertaining to them, a judgment declaring that the City has violated their First and Fourteenth Amendment rights, an order enjoining their future discriminatory surveillance, and damages.

The District Court granted the City's Motion to Dismiss the Complaint in February 2014 pursuant to Federal Rule of Civil Procedure 12(b)(1) for lack of standing and Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. First, the Court held that Plaintiffs failed to identify ***289** any cognizable "injury-in-fact" (let alone one "fairly traceable" to the City's surveillance). Second, it concluded that Plaintiffs failed to state a claim because "[t]he more likely explanation for the surveillance was a desire to locate budding terrorist conspiracies" than a desire to discriminate. *Hassan v. City of New York,* No. 12–cv–3401, 2014 WL 654604, at *7 (D.N.J. Feb. 20, 2014). It therefore entered judgment in the City's favor. Plaintiffs now appeal these rulings.

III. STANDING

[1] As did the District Court, we begin with Plaintiffs' standing to have a federal court decide their claims. Standing to sue is required for jurisdiction in a federal forum. Derived from Article III of our Constitution, it is the threshold inquiry in every case, one for which "[t]he party invoking federal jurisdiction bears the burden of [proof]." *Lujan v. Defenders of Wildlife,* 504 U.S. 555, 561, 112 S.Ct. 2130, 119 L.Ed.2d 351 (1992). Analyzing this requirement entails a three-part inquiry. Has at least one plaintiff suffered an "injury in fact"? *Id.* If so, is that injury "fairly ... trace [able] to the challenged action of the defendant"? *Id.* at 560, 112 S.Ct. 2130 (alterations in original) (quoting *Simon v. E. Ky. Welfare Rights Org.,* 426 U.S. 26, 41–42, 96 S.Ct. 1917, 48 L.Ed.2d 450 (1976)). And if the answer to both is yes, will that injury be "likely .. redressed by a favorable decision"? *Id.* at 561, 112 S.Ct. 2130 (quoting *Simon,* 426 U.S. at 38, 96 S.Ct. 1917).

[2] When answering these questions, "we must assume that the party asserting federal jurisdiction is correct on the legal merits of his claim, that a decision on the merits would be favorable[,] and that the requested relief would be granted." *Cutler v. U.S. Dep't of Health & Human Servs.,* 797 F.3d 1173, 1179 (D.C.Cir.2015) (internal quotation marks omitted). In other words, to withstand a "facial attack" at the motion-to-dismiss stage, a plaintiff need only plausibly allege facts establishing each constitutional requirement. *Lewis v. Casey,* 518 U.S. 343, 358, 116 S.Ct. 2174, 135 L.Ed.2d 606 (1996).

A. Injury–in–Fact

[3] [4] [5] A plaintiff alleges injury-in-fact when it claims that it has, or is in imminent danger of having, suffered "an invasion of a legally protected interest" that is "concrete and particularized" and " 'actual or imminent, not conjectural and hypothetical.' " *Lujan,* 504 U.S. at 560, 112 S.Ct. 2130 (quoting *Whitmore v. Arkansas,* 495 U.S. 149, 155, 110 S.Ct. 1717, 109 L.Ed.2d 135 (1990)) (internal quotation marks omitted). The burden is low, requiring nothing more than " 'an identifiable trifle' of harm." *Joint Stock Soc'y v. UDV N. Am., Inc.,* 266 F.3d 164, 177 (3d Cir.2001) (Alito, J.) (quoting *United States v. Students Challenging Regulatory Agency Procedures (SCRAP),* 412 U.S. 669, 686, 93 S.Ct. 2405, 37 L.Ed.2d 254 (1973)).

[6] [7] While Plaintiffs point to at least four other injuries

they contend also meet this requirement, "[t]he indignity of being singled out [by a government] for special burdens on the basis of one's religious calling," *Locke v. Davey,* 540 U.S. 712, 731, 124 S.Ct. 1307, 158 L.Ed.2d 1 (2004) (Scalia, J., dissenting), is enough to get in the courthouse door. Unequal treatment is "a type of personal injury [that] ha[s] long [been] recognized as judicially cognizable," *Heckler v. Mathews,* 465 U.S. 728, 738, 104 S.Ct. 1387, 79 L.Ed.2d 646 (1984), and virtually every circuit court has reaffirmed[1]—as has the Supreme Court—that a ***290** "discriminatory classification is itself a penalty," *Saenz v. Roe,* 526 U.S. 489, 505, 119 S.Ct. 1518, 143 L.Ed.2d 689 (1999), and thus qualifies as an actual injury for standing purposes, where a citizen's right to equal treatment is at stake. *See also Ne. Fla. Chapter of Associated Gen. Contractors of Am. v. City of Jacksonville,* 508 U.S. 656, 657, 113 S.Ct. 2297, 124 L.Ed.2d 586 (1993) ("The 'injury in fact' ... is the denial of equal treatment....").[2]

None of the City's arguments to the contrary are persuasive. First, its argument that unequal treatment is only injurious when it involves a tangible benefit like college admission or Social Security takes too cramped a view of Article III's injury requirement. As the Supreme Court has noted,

> discrimination itself, by perpetuating "archaic and stereotypic notions" or by stigmatizing members of the disfavored group as "innately inferior" and therefore as less worthy participants in the political community, can cause serious noneconomic injuries to those persons who are personally denied equal treatment solely because of their membership in a disfavored group.

Heckler, 465 U.S. at 739–40, 104 S.Ct. 1387 (citation omitted) (quoting *Miss. Univ. for Women v. Hogan,* 458 U.S. 718, 725, 102 S.Ct. 3331, 73 L.Ed.2d 1090 (1982)); *see also, e.g., Mardell v. Harleysville Life Ins. Co.,* 65 F.3d 1072, 1074 (3d Cir.1995) (*per curiam*) ("[A] victim of discrimination suffers a dehumanizing injury as real as, and often of far more severe and lasting harm than, a blow to the jaw." (internal quotation ***291** marks omitted)). After all, "[t]he fundamental concern of discrimination law is to redress the dignitary affront that decisions based on group characteristics represent, not to guarantee specific economic expectancies." *Sandberg v. KPMG Peat Marwick, L.L.P.,* 111 F.3d 331, 335 (2d Cir.1997).

The City next argues that Plaintiffs have suffered no injury-in-fact because it has not overtly condemned the Muslim religion. City Br. 35. This argument does not stand the test of time. Our Nation's history teaches the uncomfortable lesson that those not on discrimination's receiving end can all too easily gloss over the "badge of inferiority" inflicted by unequal treatment itself. Closing our eyes to the real and ascertainable harms of discrimination inevitably leads to morning-after regret. *Compare Plessy v. Ferguson,* 163 U.S. 537, 551, 16 S.Ct. 1138, 41 L.Ed. 256 (1896) ("[If] enforced separation of the two races stamps the colored race with a badge of inferiority ... [,] it is not by reason of anything found in the act, but solely because the colored race chooses to put that construction upon it."), *with Brown v. Bd. of Educ.,* 347 U.S. 483, 494, 74 S.Ct. 686, 98 L.Ed. 873 (1954) ("To separate [children] from others of similar age and qualifications solely because of their race generates a feeling of inferiority as to their status in the community that may affect their hearts and minds in a way unlikely ever to be undone.").

[8] [9] Moving on, we are similarly unpersuaded by the City's alternative argument that Plaintiffs' alleged injuries are not "particularized." It is true that "only ... a complainant [who] possesses something more than a general interest in the proper execution of the laws ... is in a position to secure judicial intervention." *Stark v. Wickard,* 321 U.S. 288, 304, 64 S.Ct. 559, 88 L.Ed. 733 (1944). But where a plaintiff is "asserting [his or her] own [equality] right," a claim of discrimination, even where it affects a broad class, "is not an abstract concern or 'generalized grievance.' " *Ad Hoc Comm. of Concerned Teachers v. Greenburgh # 11 Union Free Sch. Dist.,* 873 F.2d 25, 29 (2d Cir.1989) (quoting *Warth v. Seldin,* 422 U.S. 490, 499, 95 S.Ct. 2197, 45 L.Ed.2d 343 (1975)). Because Plaintiffs in this case claim to be the very targets of the allegedly unconstitutional surveillance, they are unquestionably "affect[ed] ... in a personal and individual way." *Lujan,* 504 U.S. at 560 n. 1, 112 S.Ct. 2130.

Further, that hundreds or thousands (or even millions) of other persons may have suffered the same injury does not change the individualized nature of the asserted rights and interests at stake. *See, e.g., Sch. Dist. v. Schempp,* 374 U.S. 203, 223, 83 S.Ct. 1560, 10 L.Ed.2d 844 (1963) (calling religious freedom an "individual" right); *Adarand Constructors, Inc. v. Peña,* 515 U.S. 200, 227, 115 S.Ct. 2097, 132 L.Ed.2d 158 (1995) (referring to a citizen's "*personal* right to equal protection of the laws" (emphasis

in original)). Standing is easily recognized, for instance, in the case of "a widespread mass tort," even though "large numbers of individuals suffer the same common-law injury." *FEC v. Akins,* 524 U.S. 11, 24, 118 S.Ct. 1777, 141 L.Ed.2d 10 (1998). And for good reason: "[t]o deny standing to persons who are in fact injured[,] simply because many others are also injured, would mean that the most injurious and widespread Government actions could be questioned by nobody." *Massachusetts v. EPA,* 549 U.S. 497, 526 n. 24, 127 S.Ct. 1438, 167 L.Ed.2d 248 (2007) (emphasis omitted) (quoting *SCRAP,* 412 U.S. at 688, 93 S.Ct. 2405). Harm to all—even in the nuanced world of standing law—cannot be logically equated with harm to no one.

***292** Against this background, the City's reliance on *Laird v. Tatum,* 408 U.S. 1, 92 S.Ct. 2318, 33 L.Ed.2d 154 (1972), is misplaced. The plaintiffs there alleged only a "chilling effect" on third parties' speech caused by "the mere existence, without more, of [non-discriminatory] governmental investigative and data-gathering activity." *Id.* at 10–11, 92 S.Ct. 2318. Plaintiffs here, by contrast, allege that the discriminatory manner by which the Program is administered itself causes them direct, ongoing, and immediate harm. Because "standing ... is only a problem where no harm independent of the First Amendment is alleged," *Gill v. Pidlypchak,* 389 F.3d 379, 383 (2d Cir.2004) (Calabresi, J.), and *Laird* doesn't stand for the proposition that public surveillance is either *per se* immune from constitutional attack or subject to a heightened requirement of injury, that case's "narrow" holding, *see* 408 U.S. at 15, 92 S.Ct. 2318, doesn't reach the facts of this case.

Indeed, in several post-*Laird* cases we have recognized that, while surveillance in public places may not of itself violate any privacy right,[3] it can still violate other rights that give rise to cognizable harms. *See, e.g., Hall v. Pa. State Police,* 570 F.2d 86, 91 (3d Cir.1978) ("Although it may be assumed that the state may arrange for photographing all suspicious persons entering the bank, it does not follow that its criterion for selection may be racially based, in the absence of a proven compelling state interest." (citation omitted)); *cf. Anderson v. Davila,* 125 F.3d 148, 160–61 (3d. Cir.1997) (Roth, J.) (while public governmental surveillance alone was not cognizable, identical surveillance conducted in retaliation for one's exercise of First Amendment rights gave rise to a separate injury cognizable under Article III).

B. Fair Traceability

[10] The second requirement of injury-in-fact is a causal connection between a defendant's alleged conduct and the plaintiff's harm. *See Lujan,* 504 U.S. at 561, 112 S.Ct. 2130. The City contends that Plaintiffs have failed to satisfy this requirement because the Associated Press ("AP"), not the NYPD, revealed the Program to the public and did so without the City's permission. In short, it argues, "What you don't know can't hurt you. And, if you *do* know, don't shoot us. Shoot the messenger."

Aside from its distortions of the factual record,[4] the City's argument is legally untenable ***293** because (to repeat) the discrimination itself is the legally cognizable injury. Indeed, discrimination often has been likened to a "dignitary tort," *see, e.g., Curtis v. Loether,* 415 U.S. 189, 195 n. 10, 94 S.Ct. 1005, 39 L.Ed.2d 260 (1974) (quoting Charles O. Gregory & Harry Kalven, Jr., *Cases and Materials on Torts* 961 (2d ed.1969)), where "[t]he tort is said to be damage itself," 2 Dan B. Dobbs, *Dobbs Law of Remedies* § 7.4(1), at 334 (2d ed.1993). And, as with other "torts" in this category, "the affront to the other's dignity ... is as keenly felt by one who only knows after the event that an indignity has been perpetrated upon him as by one who is conscious of it while it is being perpetrated." *Restatement (First) of Torts* § 18 cmt. e (1934). Because we view the claimed discrimination itself as the primary injury alleged, it "follows from our definition of 'injury in fact' " that the City "is the 'cause' " of that injury rather than any member of the press. *Ne. Fla. Chapter of Associated Gen. Contractors,* 508 U.S. at 666 n. 5, 113 S.Ct. 2297.

[11] Finally, even if only the collateral consequences of the discrimination—rather than the unequal treatment itself—could count as Article III injury, the City "wrongly equat[es] ... injury 'fairly traceable' to the defendant with injury as to which the defendant's actions are the very last step in the chain of causation." *Constitution Party of Pa. v. Aichele,* 757 F.3d 347, 366 (3d Cir.2014) (second alteration in original) (quoting *Bennett v. Spear,* 520 U.S. 154, 168–69, 117 S.Ct. 1154, 137 L.Ed.2d 281 (1997)). That is incorrect. "[T]here is room for concurrent causation in the analysis of standing, and, indeed, 'an indirect causal relationship will suffice, so long as there is a fairly traceable connection.' " *Id.* (citation omitted) (quoting *Toll Bros. v. Township of Readington,* 555 F.3d 131, 142 (3d Cir.2009) (internal quotation marks omitted)); *see also Block v. Meese,* 793 F.2d 1303, 1309 (D.C.Cir.1986) (Scalia, J.) ("[T]he question of core, constitutional injury-in-fact ... requires no more than *de facto* causality."); *Pitt News v. Fisher,* 215 F.3d 354, 361 (3d Cir.2000) ("but for" causation sufficient to establish traceability to establish standing).

C. Redressability

[12] [13] The last requirement of Article III standing is redressability, which requires the plaintiff to show that "it ... [is] 'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.' " *Lujan,* 504 U.S. at 560, 112 S.Ct. 2130 (quoting *Simon,* 426 U.S. at 38, 96 S.Ct. 1917). Redressability is "easily established in a case where," as here, "the alleged injury arises from an identifiable discriminatory policy." *Smith v. Meese,* 821 F.2d 1484, 1494 (11th Cir.1987). While we cannot predict "the exact nature of the possible relief ... without a full development of the facts, an order enjoining the policy and requiring non-discriminatory investigation and enforcement would redress the injury." *Id.*

[14] As for past harms, the potential avenues for redress depend on how a particular plaintiff's injury shows itself. Those plaintiffs able to prove "actual injur[ies]"—*i.e.*, those other than "the abstract value of [the] constitutional right[s]," such as out-of-pocket losses or emotional distress—may recover compensatory damages. *Memphis Cmty. Sch. Dist. v. Stachura,* 477 U.S. 299, 308, 106 S.Ct. 2537, 91 L.Ed.2d 249 (1986); *see also Carey v. Piphus,* 435 U.S. 247, 264–66, 98 S.Ct. 1042, 55 L.Ed.2d 252 (1978). For other plaintiffs, "the major purpose of the suit may be to obtain a public declaration that the[y are] right and w[ere] improperly treated," *see Restatement (Second) of Torts* § 901 cmt. c (1979), along with nominal ***294** damages that serve as "a symbolic vindication of [their] constitutional right[s]," *Schneider v. County of San Diego,* 285 F.3d 784, 794 (9th Cir.2002) (quoting *Floyd v. Laws,* 929 F.2d 1390, 1403 (9th Cir.1991)). Given the range of available remedies, redressability is easily satisfied.

* * * * * *

Confident in our jurisdiction to hear this case, we now turn to the merits of Plaintiffs' constitutional claims and begin with equal protection.

IV. CONSTITUTIONAL CLAIMSA. Equal–Protection Claim

[15] The Equal Protection Clause of the Fourteenth Amendment to our Constitution provides that "[n]o State shall ... deny to any person within its jurisdiction the equal protection of the laws." U.S. Const. Amend. XIV, § 1. Plaintiffs claim the City is contravening that mandate and violating their rights by surveilling them pursuant to a Program that investigates persons not because of any reasonable suspicion of wrongdoing (or other neutral criterion) but solely because of their Muslim religious affiliation.

[16] A "claim of selective investigation" by the police draws on " 'ordinary equal protection standards.' " *Flowers v. City of Minneapolis,* 558 F.3d 794, 798 (8th Cir.2009) (quoting *Wayte v. United States,* 470 U.S. 598, 608, 105 S.Ct. 1524, 84 L.Ed.2d 547 (1985)). As with other equal-protection claims, we ask whether the City intentionally discriminates against a reasonably identifiable group and whether that intentional discrimination is nonetheless legally justified.

1. Do Plaintiffs Plausibly Allege Intentional Discrimination?

[17] To state an equal-protection claim, Plaintiffs must allege (and ultimately prove) "intentional discrimination." *Washington v. Davis,* 426 U.S. 229, 241, 96 S.Ct. 2040, 48 L.Ed.2d 597 (1976); *Pers. Adm'r of Mass. v. Feeney,* 442 U.S. 256, 276, 99 S.Ct. 2282, 60 L.Ed.2d 870 (1979). It is not enough for them to allege that they are Muslim and that the NYPD surveilled more Muslims than members of any other religion. *See Ashcroft v. Iqbal,* 556 U.S. 662, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009). Rather, Plaintiffs' religious affiliation must have been a substantial factor in that different treatment. *Davis,* 426 U.S. at 235, 96 S.Ct. 2040; *Feeney,* 442 U.S. at 276, 99 S.Ct. 2282.

i. Plaintiffs Plausibly Allege a Surveillance Program with a Facially Religious Classification.

There are a variety of theories to consider in an equal-protection claim of this type. First, Plaintiffs could point to a policy that is facially discriminatory, meaning that the policy "by its own terms" singles out Muslims "for different treatment." 3 Ronald D. Rotunda & John E. Nowak, *Treatise on Constitutional Law* § 18.4 (10th ed.2012); *see, e.g., Adarand,* 515 U.S. at 213, 227–29, 115 S.Ct. 2097. Second, they could identify a policy that "either shows no classification on its face or else indicates a classification which seems to be legitimate," yet one that NYPD officers apply to Muslims with a greater "degree[ ] of severity" than other religious groups. Rotunda & Novak, *supra,* § 18.4; *see, e.g., Yick Wo v. Hopkins,* 118 U.S. 356, 373–74, 6 S.Ct. 1064, 30 L.Ed. 220 (1886). Or, third, Plaintiffs could identify a facially neutral policy that the City purposefully "designed to impose different burdens" on Muslims and that (even if applied evenhandedly) does in fact have the intended adverse effect. Rotunda & Novak, *supra,* § 18.4; *see, e.g., Village of Arlington Heights v. Met. Hous.* ***295** *Dev. Corp.,* 429 U.S. 252, 264–65, 97 S.Ct. 555, 50 L.Ed.2d 450 (1977).

[18] Here, Plaintiffs seek to proceed by way of the first of

these three methods, arguing their "allegations leave no doubt that the ... [Program] relies on an express classification of Muslims for disfavored treatment." *See* Pls.' Br. 10. This is a viable legal theory. Where a plaintiff can point to a facially discriminatory policy, "the protected trait by definition plays a role in the decision-making process, inasmuch as the policy explicitly classifies people on that basis."[5] *Cmty. Servs. v. Wind Gap Mun. Auth.*, 421 F.3d 170, 177 (3d Cir.2005) (quoting *DiBiase v. SmithKline Beecham Corp.*, 48 F.3d 719, 726 (3d Cir.1995)). Put another way, direct evidence of intent is "supplied by the policy itself." *Massarsky v. Gen. Motors Corp.*, 706 F.2d 111, 128 (3d Cir.1983) (Sloviter, J., dissenting).

The City nonetheless attacks the plausibility of the allegations, arguing that Plaintiffs point to only "conclusory allegations ... spread throughout [the] ... [C]omplaint," which "as a matter of law cannot be credited." City Br. 56. It further asserts that, "[o]nce the conclusory allegations are pushed aside, the remaining factual allegations are insufficient to find a facially discriminatory classification." *Id.*

We disagree with this characterization. While the City compares Plaintiffs' claims to the conclusory allegations in *Iqbal*, those were far from what we have here. In our case, Plaintiffs allege specifics about the Program, including *when* it was conceived (January 2002), *where* the City implemented it (in the New York Metropolitan area with a focus on New Jersey), and *why* it has been employed (because of the belief "that Muslim religious identity ... is a permissible proxy for criminality," Compl. ¶ 36). The Complaint also articulates the "variety of methods" by which the surveillance is carried out. *See, e.g., id.* ¶ 39 ("tak[ing] videos and photographs at mosques, Muslim-owned businesses and schools"); *id.* ("monitor[ing Muslim] websites, listservs, and chat rooms"); *id.* ¶ 46 ("snap[ping] pictures, tak[ing] video, and collect[ing] license plate numbers of congregants as they arrive at mosques to pray"); *id.* ¶ 47 ("us[ing] undercover officers ... to monitor daily life in [Muslim] neighborhoods ... and sermons and conversations in mosques"); *id.* ¶ 49 ("plac [ing] informants or undercover officers in all or virtually all MSAs"). These allegations are hardly "bare assertions ... amount[ing] to nothing more than a 'formulaic recitation of the elements' of a constitutional discrimination claim." *Iqbal*, 556 U.S. at 681, 129 S.Ct. 1937 (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. at 544, 545, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)).

Despite the City's demand for more information about when, by whom, and how the policy was enacted and where it was written down, "the *Twombly–Iqbal* duo have *not* inaugurated an era of evidentiary pleading." *Santana v. Cook Cnty. Bd. of Review*, 270 F.R.D. 388, 390 (N.D.Ill.2010) (emphasis in original); *see also* ***296** *Twombly*, 550 U.S. at 570, 127 S.Ct. 1955 (rejecting the proposition that notice pleading "require[s] heightened fact pleading of specifics"). Nor do "factual allegations ... become impermissible labels and conclusions simply because the additional factual allegations explaining and supporting the articulated factual allegations are not also included." *In re Niaspan Antitrust Litig.*, 42 F.Supp.3d 735, 753 (E.D.Pa.2014) (internal quotation marks omitted). While it is possible that Plaintiffs will ultimately falter in meeting their burden of proof, the collection of evidence is the object of discovery.

Moreover, even if the pleading of "evidence" rather than "grounds for relief" were required (which it is not), the Complaint includes numerous examples of persons that the NYPD is surveilling because of their religious affiliation.[6] *See, e.g.*, Compl. ¶ 14 (the Masjid al-Haqq and Masjid Ali K. Muslim mosques); *id.* ¶ 17 (MSAs for Rutgers University campuses at Newark and New Brunswick); *id.* ¶ 18 (All Body Shop Inside & Outside); *id.* ¶ 20 (Unity Beef Sausage Co.); *id.* ¶ 22 (the Masjid–e–Ali mosque); *id.* ¶ 31 (Al–Hidaayah Academy); *id.* (Al Muslimaat Academy). These allegations supplement those that the NYPD "surveil[led] ... at least twenty mosques, fourteen restaurants, eleven retail stores, two grade schools and two [MSAs] in New Jersey," id. ¶ 38; "creat[ed] over twenty precinct-level maps of the City of Newark," *id.;* and attempted to place an "informant inside every mosque within a 250–mile radius of New York City" as well as prepared an "analytical report on every mosque within 100 miles," *id.* ¶ 47.

[19] Finally, because Plaintiffs allege that all of these persons and entities were surveilled without any reasonable suspicion of wrongdoing (as noted above, they assert that, "[i]n all its years of operation, the Program has never generated a single [criminal] lead," *id.* ¶ 2), this case can be easily contrasted with others where the law-enforcement investigation at issue was almost certainly explained by a reasonable suspicion of wrongdoing.[7] *Cf. George v.* ***297** *Rehiel*, 738 F.3d 562, 586 (3d Cir.2013) ("The TSA Officials' suspicion was an obvious alternative explanation for their conduct, which negates any inference of retaliation."). That we might be able to conjure up some non-discriminatory motive to explain the City's alleged conduct is not a valid basis for dismissal. It is "only when [a] defendant's plausible alternative explanation is so convincing" to render the "plaintiff's explanation ... *im* plausible" that a court may dismiss a complaint. *Starr v. Baca*, 652 F.3d 1202, 1216

(9th Cir.2011) (emphasis in original).

In sum, because Plaintiffs have pleaded ample "factual content [that] allows [us] to draw the reasonable inference that the [City] is liable for the misconduct alleged," *Iqbal,* 556 U.S. at 663, 129 S.Ct. 1937, we decline to dismiss their Complaint on the ground that they have not plausibly alleged a surveillance program with a facially discriminatory classification.

ii Intentional Discrimination Does Not Require an Invidious Motive.

[20] The City also argues that, even assuming Plaintiffs have plausibly alleged a facial classification based on religious affiliation, their allegations of discriminatory "purpose" are implausible because "the more likely explanation for the NYPD's actions is public safety rather than discrimination based upon religion." City Br. 49. Its reasoning is essentially two-fold: "the surveillance is alleged to have begun just after the [September 11, 2001] terrorist attacks," *id.,* and "[t]he police could not have monitored New Jersey for Muslim terrorist activities without monitoring the Muslim community itself," *id.* (alteration in original) (quoting *Hassan,* 2014 WL 654604, at *6).

Here's the City's problem: there's a difference between "intent" and "motive." "[A] defendant acts intentionally when he desires a particular result, without reference to the reason for such desire. Motive, on the other hand, is the reason why the defendant desires the result." 2 Harry Sanger Richards et al., *American Law and Procedure* § 8, at 6 (1922). In other words, "intent" asks whether a person acts "intentionally or accidentally," while "motive" asks, "If he did it intentionally, *why* did he do it?" 1 John William Salmond, *Jurisprudence* § 134, at 398 (7th ed.1924) (emphasis in original); *see also Black's Law Dictionary* 881 (Bryan Garner ed., 10th ed. 2014) ("While motive is the inducement to do some act, intent is the mental resolution or determination to do it."). This fundamental "distinction between motive and intent runs all through the law." *Johnson v. Phelan,* 69 F.3d 144, 155 (7th Cir.1995) (Posner, C.J., concurring in part and dissenting in part).

In focusing on what the City contends was its "legitimate purpose[ ]" of "analy[zing] ... potential [security] threats and vulnerabilities," City Br. 50, it wrongly assumes that invidious motive is a necessary element of discriminatory intent. It is not. All you need is that the state actor *meant* to single out a plaintiff because of the *protected characteristic* itself. *See,* ***298** *e.g., Snyder v. Louisiana,* 552 U.S. 472, 485, 128 S.Ct. 1203, 170 L.Ed.2d 175 (2008); *Bray v. Alexandria Women's Health Clinic,* 506 U.S. 263, 269–70, 113 S.Ct. 753, 122 L.Ed.2d 34 (1993). In a school-segregation case, for instance, "the 'intent' which triggers a finding of unconstitutionality is not an intent to harm black students, but simply an intent to bring about or maintain segregated schools." *United States v. Sch. Dist. of Omaha,* 521 F.2d 530, 535 (8th Cir.1975). Likewise, a prosecutor who strikes a juror on the basis of race discriminates intentionally even if motivated by a sincere desire to win his case. *See, e.g., Georgia v. McCollum,* 505 U.S. 42, 59, 112 S.Ct. 2348, 120 L.Ed.2d 33 (1992).

[21] So too here. While the absence of a legitimate motive may bear on whether the challenged surveillance survives the appropriate level of equal-protection scrutiny, "intentional discrimination" need not be motivated by "ill will, enmity, or hostility" to contravene the Equal Protection Clause. *Floyd v. City of New York,* 959 F.Supp.2d 540, 662 (S.D.N.Y.2013) (quoting *Ferrill v. Parker Grp., Inc.,* 168 F.3d 468, 473 n. 7 (11th Cir.1999)); *see also Cmtys. for Equity v. Mich. High Sch. Athletic Ass'n,* 459 F.3d 676, 694 (6th Cir.2006) (distinguishing between "an intent to treat two groups differently" and "an intent to harm"); *Garza v. County of Los Angeles,* 918 F.2d 763, 778 n. 1 (9th Cir.1990) (Kozinski, J., concurring in part and dissenting in part) ("[T]here can be intentional discrimination without an invidious motive."). Thus, even if NYPD officers were subjectively motivated by a legitimate law-enforcement purpose (no matter how sincere), they've intentionally discriminated if they wouldn't have surveilled Plaintiffs had they not been Muslim.

2. Is the Alleged Discrimination Nonetheless Legally Justified?

[22] Once a plaintiff demonstrates treatment different from others with whom he or she is similarly situated and that the unequal treatment is the result of intentional discrimination, "the adequacy of the reasons for that discrimination are ... separately assessed at equal protection's second step" under the appropriate standard of review. *SECSYS, LLC v. Vigil,* 666 F.3d 678, 689 (10th Cir.2012). To apply this traditional legal framework to the facts of this case, we must determine the appropriate standard of review (*i.e.,* rational basis, intermediate scrutiny, or strict scrutiny) and then ask whether it is met.[8]

i. Level of Scrutiny

[23] [24] [25] [26] [27] At a minimum, intentional discrimination against any "identifiable group" is subject to

rational-basis review, which requires the classification to be rationally related to a legitimate governmental purpose. *Johnson v. Cohen,* 836 F.2d 798, 805 n. 9 (3d Cir.1987). Where a "quasi-suspect" or "suspect" classification is at issue, however, the challenged action must survive "intermediate scrutiny" or "strict scrutiny."[9] Intermediate scrutiny (applicable to quasi-suspect classes like gender ***299** and illegitimacy) requires that a classification "be substantially related to an important governmental objective." *Clark v. Jeter,* 486 U.S. 456, 461, 108 S.Ct. 1910, 100 L.Ed.2d 465 (1988). In contrast, strict scrutiny (applicable to suspect classes like race and nationality) is an even more demanding standard, which requires the classification be "narrowly tailored ... [to] further [a] compelling governmental interest[ ]." *Gratz v. Bollinger,* 539 U.S. 244, 270, 123 S.Ct. 2411, 156 L.Ed.2d 257 (2003). Strict and intermediate scrutiny (which we collectively refer to as "heightened scrutiny" to distinguish them from the far less demanding rational-basis review) in effect set up a presumption of invalidity that the defendant must rebut.

Perhaps surprisingly, neither our Court nor the Supreme Court has considered whether classifications based on religious affiliation[10] trigger heightened scrutiny under the Equal Protection Clause. *See* Steven G. Calabresi & Abe Salander, *Religion and the Equal Protection Clause: Why the Constitution Requires School Vouchers,* 65 Fla. L.Rev. 909, 919 (2013); Kenji Yoshino, *Suspect Symbols: The Literary Argument for Heightened Scrutiny for Gays,* 96 Colum. L.Rev. 1753, 1783 (1996). We therefore confront a question of first impression in this Circuit.

Although the answer to this question is not found in binding precedent, we hardly write on a clean slate. To start, it has long been implicit in the Supreme Court's decisions that religious classifications are treated like others traditionally subject to heightened scrutiny, such as those based on race. *United States v. Armstrong,* 517 U.S. 456, 464, 116 S.Ct. 1480, 134 L.Ed.2d 687 (1996) (naming "race" and "religion" as examples of "unjustifiable standard[s]" for a "decision whether to prosecute" (quoting *Oyler v. Boles,* 368 U.S. 448, 456, 82 S.Ct. 501, 7 L.Ed.2d 446 (1962))); *Burlington N. R.R. v. Ford,* 504 U.S. 648, 651, 112 S.Ct. 2184, 119 L.Ed.2d 432 (1992) (referring to "race" and "religion" as "classif[ications] along suspect lines"); *Friedman v. Rogers,* 440 U.S. 1, 17, 99 S.Ct. 887, 59 L.Ed.2d 100 (1979) (calling "race, religion, [and] alienage ... inherently suspect distinctions"); *City of New Orleans v. Dukes,* 427 U.S. 297, 303, 96 S.Ct. 2513, 49 L.Ed.2d 511 (1976) (same); *United States v. Batchelder,* 442 U.S. 114, 125 n. 9, 99 S.Ct. 2198, 60 L.Ed.2d 755 (1979) (listing "race" and "religion" as "unjustifiable standard[s]" under our Constitution (quoting *Oyler,* 368 U.S. at 456, 82 S.Ct. 501)); *Steele v. Louisville & Nashville R.R.,* 323 U.S. 192, 209, 65 S.Ct. 226, 89 L.Ed. 173 (1944) (Murphy, J., concurring) ("The Constitution voices its disapproval whenever economic discrimination is applied under authority of law against any race, creed or color.").

This line of comment can be traced back to the famous footnote four of the Supreme ***300** Court's 1938 decision in *Carolene Products,* where the Court suggested that discriminatory legislation should "be subjected to more exacting judicial scrutiny under the general prohibitions of the Fourteenth Amendment" if "directed at particular *religious,* or national, or racial minorities." *United States v. Carolene Prods. Co.,* 304 U.S. 144, 152 n. 4, 58 S.Ct. 778, 82 L.Ed. 1234 (1938) (citations omitted) (emphasis added). And even before *Carolene Products,* the Court considered religious discrimination to be a classic example of "a denial of the equal protection of the laws to the less favored classes." *Am. Sugar Ref. Co. v. Louisiana,* 179 U.S. 89, 92, 21 S.Ct. 43, 45 L.Ed. 102 (1900); *see also Hall v. De Cuir,* 95 U.S. 485, 505, 24 L.Ed. 547 (1877) ("Directors of schools in Iowa ... [cannot] deny a youth of proper age admission to any particular school on account of nationality, color, or religion.").

[28] It is true that these statements are *dicta.* But even so, Supreme Court *dicta* "requires serious consideration," *United States v. Marzzarella,* 614 F.3d 85, 90 n. 5 (3d Cir.2010), "especially ... when, as here, we encounter a decades-long succession of statements from the Court," *Myers v. Loudoun Cnty. Pub. Sch.,* 418 F.3d 395, 410 (4th Cir.2005) (D. Motz, J., concurring in the judgment). Moreover, this *dicta* is consistent with our own. *Connelly v. Steel Valley Sch. Dist.,* 706 F.3d 209, 213 (3d Cir.2013) (identifying "race, religion, [and] alienage" as "inherently suspect distinctions" (quoting *Schumacher v. Nix,* 965 F.2d 1262, 1266 (3d Cir.1992) (internal quotation marks omitted)); *United States v. DeJesus,* 347 F.3d 500, 510–11 (3d Cir.2003) (Fuentes, J.) (referring in *dictum* to "religious affiliation" as "a protected class")); *Tolchin v. Supreme Court of New Jersey,* 111 F.3d 1099, 1114 (3d Cir.1997) (naming "race, religion or alienage" as "suspect distinctions"); *United States v. Friedland,* 83 F.3d 1531, 1537 (3d Cir.1996) ("[T]he government can[not] refuse to move for a downward [ ] departure under 18 U.S.C. § 3553(e) [if] ... base[d] ... on a constitutionally suspect ground such as race or religion.").

We also are guided by other appellate courts that have subjected religious-based classifications to heightened scrutiny. For instance, both the Eighth and Tenth Circuit Courts have held without fanfare that "[r]eligion is a

suspect classification," *Abdulhaseeb v. Calbone,* 600 F.3d 1301, 1322 n. 10 (10th Cir.2010); *Patel v. U.S. Bureau of Prisons,* 515 F.3d 807, 816 (8th Cir.2008), and the Second and Ninth have done the same in so many words, *see, e.g., United States v. Brown,* 352 F.3d 654, 668 (2d Cir.2003) (Calabresi, J.) (holding that the exercise of a peremptory strike due to a venire member's religious affiliation would violate *Batson v. Kentucky,* 476 U.S. 79, 106 S.Ct. 1712, 90 L.Ed.2d 69 (1986), because "religious classifications ... trigger strict scrutiny"); *Christian Sci. Reading Room Jointly Maintained v. City of San Francisco,* 784 F.2d 1010, 1012 (9th Cir.1986) ("It seems clear that an individual religion meets the requirements for treatment as a suspect class."), *amended,* 792 F.2d 124 (9th Cir.1986).[11]

***301** [29] Today we join these courts and hold that intentional discrimination based on religious affiliation must survive heightened equal-protection review. Before turning more fully to our reasoning, however, we pause to reiterate that the term "heightened scrutiny," as we use it, encompasses both "intermediate scrutiny" and "strict scrutiny." Because the City bears the burden of production and proof with respect to both, *see infra* Part IV(A)(2), we need not—and should not[12]—determine in connection with its motion to dismiss which of the two applies, and we leave that question for the District Court in the first instance when and if it becomes necessary to decide it.

[30] In designating a particular classification as "suspect" or "quasi-suspect" under the Equal Protection Clause, the Supreme Court generally considers a variety of factors "grouped around [the] central idea" of "whether the discrimination embodies a gross unfairness that is [so] sufficiently inconsistent with the ideals of equal protection to term it 'invidious.' " *Watkins v. U.S. Army,* 875 F.2d 699, 724–25 (9th Cir.1989) (*en banc*) (Norris, J., concurring in the judgment). Among these are "whether the ... class is defined by a[n] [immutable] trait that 'frequently bears no relation to ability to perform or contribute to society' " and "whether the class has been saddled with unique disabilities because of prejudice or inaccurate stereotypes." *Id.* at 725 (quoting *Frontiero v. Richardson,* 411 U.S. 677, 686, 93 S.Ct. 1764, 36 L.Ed.2d 583 (1973) (plurality opinion)). But while these factors are those most often considered, "[n]o single talisman can define those groups likely to be the target of classifications offensive to the Fourteenth Amendment ...; experience, not abstract logic, must be the primary guide." *City of Cleburne v. Cleburne Living Ctr., Inc.,* 473 U.S. 432, 472 n. 24, 105 S.Ct. 3249, 87 L.Ed.2d 313 (1985) (Marshall, J., concurring in the judgment in part and dissenting in part).

[31] Courts first have looked with particular suspicion on discrimination based on "immutable human attributes." *Parham v. Hughes,* 441 U.S. 347, 351, 99 S.Ct. 1742, 60 L.Ed.2d 269 (1979) (plurality opinion). Accordingly, a classification is more likely to receive heightened scrutiny if it discriminates against individuals based on a characteristic that they either cannot ***302** realistically change or ought not be compelled to change because it is fundamental to their identities. *See, e.g., Baskin v. Bogan,* 766 F.3d 648, 655 (7th Cir.2014) (Posner, J.) (framing this issue as whether "the unequal treatment [is] based on some immutable or at least tenacious characteristic of the people discriminated against" as opposed to a "characteristic[ ] that [is] easy for a person to change, such as the length of his or her fingernails"); *Watkins,* 875 F.2d at 726 (Norris, J., concurring in the judgment) ("[T]he Supreme Court is willing to treat a trait as effectively immutable if changing it would involve great difficulty, such as requiring a major physical change or a traumatic change of identity.").

Religious affiliation falls within this category. As we have recognized in the immigration context,[13] religious affiliation is typically seen as "capable of being changed," yet "of such fundamental importance that individuals should not be required to modify it."[14] *Ghebrehiwot v. Attorney Gen. of U.S.,* 467 F.3d 344, 357 (3d Cir.2006) (quoting *Escobar v. Gonzales,* 417 F.3d 363, 367 (3d Cir.2005)); *see also Baskin,* 766 F.3d at 655 (Posner, J.) (listing "religion" as an example of "a deep psychological commitment" that would qualify for heightened scrutiny). Moreover, while some immutable characteristics, such as intellectual disability, are so often correlated with "a person's ability to participate in society" that we frequently deem them to be constitutionally permissible bases for discrimination, *see Baskin,* 766 F.3d at 655, a person's religious affiliation is at the other end of that spectrum.

Religious discrimination, "by [its] very nature," has long been thought "odious to a free people whose institutions are founded upon the doctrine of equality." *Bell v. Maryland,* 378 U.S. 226, 288, 84 S.Ct. 1814, 12 L.Ed.2d 822 (1964) (Goldberg, J., concurring) (quoting *Hirabayashi v. United States,* 320 U.S. 81, 100, 63 S.Ct. 1375, 87 L.Ed. 1774 (1943)); *W. Va. State Bd. of Educ. v. Barnette,* 319 U.S. 624, 653, 63 S.Ct. 1178, 87 L.Ed. 1628 (1943) ("[For] Jefferson and those who followed him[,] ... [r]eligious minorities as well as religious majorities were to be equal in the eyes of the political state."); President James Madison, Religious Freedom: A Memorial and Remonstrance Against the General Assessment, in "A Bill Establishing Provision for the

Teachers of the Christian Religion," Presented to the General Assembly of Virginia, at the Session of 1785 (1819) ("A just Government ... will be best supported by protecting every citizen in the enjoyment of his Religion with the same equal hand which protects his ***303** person and his property; by neither invading the equal rights of any Sect, nor suffering any sect to invade those of another.").

Courts also are more likely to subject classifications that are "closely associated with inequality" to a more searching inquiry. *Windsor v. United States,* 699 F.3d 169, 196 (2d Cir.2012), *aff'd on other grounds,* —— U.S. ——, 133 S.Ct. 2675, 186 L.Ed.2d 808 (2013). Thus, if the classification is accompanied by a history of "discrimination based on archaic and overbroad assumptions," *Roberts v. U.S. Jaycees,* 468 U.S. 609, 625, 104 S.Ct. 3244, 82 L.Ed.2d 462 (1984), or if it has been traditionally used as a tool for the oppression and subordination of minority groups, *see, e.g., City of Richmond v. J.A. Croson Co.,* 488 U.S. 469, 495–96, 109 S.Ct. 706, 102 L.Ed.2d 854 (1989) (plurality opinion), heightened scrutiny often is more appropriately applied.

The history of religious discrimination in the United States is intertwined with that based on other protected characteristics, including national origin and race.[15] *Saint Francis Coll. v. Al–Khazraji,* 481 U.S. 604, 611–12, 107 S.Ct. 2022, 95 L.Ed.2d 582 (1987) (noting that "[t]he Ninth edition of the Encyclopedia Britannica .. referred to Arabs, Jews, and other ethnic groups such as Germans, Hungarians, and Greeks, as separate races" (citations omitted)); *Fong Yue Ting v. United States,* 149 U.S. 698, 717, 13 S.Ct. 1016, 37 L.Ed. 905 (1893) (referring to "Chinese laborers" as "of a distinct race and religion"); *In re Halladjian,* 174 F. 834, 838 (C.C.D.Mass.1909) ("A Hindoo ... differs in color no less from a Chinaman than from an Anglo–Saxon...."); Khaled A. Beydoun, *Between Muslim and White: The Legal Construction of Arab American Identity,* 69 N.Y.U. Ann. Surv. Am. L. 29, 33 (2013) (noting that "the conflation of Arab and Muslim identity was deeply entrenched within the courts during the Naturalization Era" and that "Islam was treated as an ethno-racial identity").

It is thus unsurprising that tampering with religious affiliation brings into play the same concerns of inequality. Though "[n]othing but the most telling of personal experiences in religious persecution suffered by our forebears could have planted our belief in liberty of religious opinion any more deeply in our heritage," *Schempp,* 374 U.S. at 214, 83 S.Ct. 1560 (citation omitted), we have struggled to guarantee religious equality since our Nation's founding. *See generally Everson v. Bd. of Educ. of Ewing Twp.,* 330 U.S. 1, 9–10, 67 S.Ct. 504, 91 L.Ed. 711 (1947); *Shaare Tefila Congregation v. Cobb,* 481 U.S. 615, 616, 107 S.Ct. 2019, 95 L.Ed.2d 594 (1987); *Schware v. Bd. of Bar Exam'rs of N.M.,* 353 U.S. 232, 236, 77 S.Ct. 752, 1 L.Ed.2d 796 (1957); *Murdock v. Pennsylvania,* 319 U.S. 105, 109, 63 S.Ct. 870, 87 L.Ed. 1292 (1943). Different religious groups have borne the brunt of majority ***304** oppression during different times, and the battle against religious prejudice continues. *See, e.g.,* U.S. Patriot Act of 2001, Pub.L. 107–56, § 102(a)(3), 115 Stat. 274 ("The acts of violence that have been taken against Arab and Muslim Americans since the September 11, 2001, attacks against the United States should be and are condemned by all Americans who value freedom."); Brief in Support of Appellants by *Amici Curiae* the Asian American Legal Defense & Education Fund & 17 Other Non–Governmental Organizations Supporting Civil Rights for American Muslims 11–22.

In light of this history, distinctions between citizens on religious grounds pose a particularly acute "danger of stigma and stirred animosities." *Bd. of Educ. of Kiryas Joel Vill. Sch. Dist. v. Grumet,* 512 U.S. 687, 728, 114 S.Ct. 2481, 129 L.Ed.2d 546 (1994) (Kennedy, J., concurring in the judgment); *see also Wright v. Rockefeller,* 376 U.S. 52, 67, 84 S.Ct. 603, 11 L.Ed.2d 512 (1964) (Douglas, J., dissenting) ("When racial or religious lines are drawn by the State, the multiracial, multireligious communities that our Constitution seeks to weld together as one become separatist; antagonisms that relate to race or to religion ... are generated...."); *Kunz v. New York,* 340 U.S. 290, 313, 71 S.Ct. 312, 95 L.Ed. 280 (1951) (Jackson, J., dissenting) ("If any two subjects are intrinsically incendiary and divisive, they are race and religion."). That "[c]enturies of experience testify that laws aimed at one ... religious group ... generate hatreds and prejudices which rapidly spread beyond control," *Am. Commc'ns Ass'n, C.I.O. v. Douds,* 339 U.S. 382, 448, 70 S.Ct. 674, 94 L.Ed. 925 (1950) (Black, J., dissenting), also counsels in favor of heightened scrutiny.

A final relevant consideration is whether the Legislative and Executive Branches have concluded that a form of discrimination is inherently invidious. In concluding that gender is a "quasi-suspect" classification deserving of intermediate scrutiny, Justice Brennan noted, for instance, in *Frontiero* that, because Congress is "a coequal branch of Government," its "conclu[sion] that classifications based upon sex are inherently invidious ... [was] not without significance to the question [then] under consideration." 411 U.S. at 687–88, 93 S.Ct. 1764.

Many of the same statutes that foreclose sex-based

discrimination, including Title VII of the Civil Rights Act of 1964 cited by the *Frontiero* plurality, *see id.* at 687, 93 S.Ct. 1764, also forbid religious discrimination. *See, e.g.,* 42 U.S.C. § 2000e–2 (making it an "unlawful employment practice" for an employer to discriminate based on "race, color, religion, sex, or national origin"). And from the passage of the Civil Rights Act of 1875,[16] to those designed to strengthen national security in our post-September 11 world,[17] that commitment to the "sacrosanct ... concept" of equality among "all religious ... groups," *see* U.S. Patriot Act of 2001 § 102(a)(3), is embodied throughout the U.S. Code. *See, e.g.,* 2 U.S.C. § 1311(a) (employment); ***305** 12 U.S.C. § 3106a(1)(B), (2)(B) (banking); 12 U.S.C. § 4545 (fair housing); 22 U.S.C. § 2504(a) (Peace Corps service); 49 U.S.C. § 40127 (air transportation and use of private airports).

The same commitment to religious equality is seen in the pronouncements of the Executive Branch, from those of our first President, George Washington, to our current President, Barack Obama. *See, e.g.,* President George Washington, Address to the Members of the New Church in Baltimore (Jan. 1793), *in* 2 Jared Sparks, *Life of George Washington Commander–in–Chief of the American Armies: to Which Are Added, His Diaries and Speeches; and Various Miscellaneous Papers Relating to His Habits & Opinions* 314, 314–15 (1839) ("In this enlightened age, and in this land of equal liberty, it is our boast that a man's religious tenets will not forfeit the protection of the laws, nor deprive him of the right of attaining and holding the highest offices that are known in the United States."); President Harry Truman, Special Message to the Congress on Civil Rights (Feb. 2, 1948) ("Racial, religious and other invidious forms of discrimination deprive the individual of an equal chance to develop and utilize his talents and to enjoy the rewards of his efforts."); President Theodore Roosevelt, Sixth Annual Message to Congress (Dec. 3, 1906) ("[W]e must treat with justice and good will all immigrants who come here under the law [,] ... [w]hether they are Catholic or Protestant, Jew or Gentile...."); President Barack Obama, State of the Union Address (Jan. 28, 2014) ("[W]e believe in the inherent dignity and equality of every human being, regardless of race or religion, creed or sexual orientation.").

For these reasons, we conclude that classifications on the basis of religious affiliation are subject to heightened scrutiny under the Equal Protection Clause.

ii. Evaluation of Means and Ends

[32] The final step in evaluating an equal-protection claim is to examine the challenged action's "means" and "ends" and the "fit" between the two. The specific analysis differs depending on the level of scrutiny that applies. The higher the scrutiny required, the more persuasive must be the governmental objective and the snugger the means-ends fit. Thus, while it usually matters little for purposes of rational-basis review that a governmental interest is not exceedingly important or that "other means are better suited to the achievement of governmental ends," heightened scrutiny demands a much stronger justification and a much tighter relationship "between the means employed and the ends served." *Tuan Anh Nguyen v. INS,* 533 U.S. 53, 77–78, 121 S.Ct. 2053, 150 L.Ed.2d 115 (2001) (O'Connor, J., dissenting).

[33] Also increasingly demanding is the standard of proof. While the rational-basis standard usually puts the burden of proof on the classification's *opponent* and "permits a court to hypothesize interests that *might* support [the governmental] distinctions," *id.* at 77, 121 S.Ct. 2053 (emphasis added) (citing *Heller v. Doe,* 509 U.S. 312, 320, 113 S.Ct. 2637, 125 L.Ed.2d 257 (1993); *R.R. Ret. Bd. v. Fritz,* 449 U.S. 166, 101 S.Ct. 453, 66 L.Ed.2d 368 (1980)), the burden of justification under both intermediate and strict scrutiny "is demanding and ... rests entirely on the State," *United States v. Virginia,* 518 U.S. 515, 533, 116 S.Ct. 2264, 135 L.Ed.2d 735 (1996). *See also Hogan,* 458 U.S. at 724, 102 S.Ct. 3331 (discussing the standard and burden for intermediate scrutiny); ***306** *Fisher v. Univ. of Tex. at Austin,* —— U.S. ——, 133 S.Ct. 2411, 2419, 186 L.Ed.2d 474 (2013) (strict scrutiny).

[34] Here, the City argues that "[a] comprehensive understanding of the makeup of the community would help the NYPD figure out where to look—and where not to look—in the event it received information that an Islamist radicalized to violence may be secreting himself in New Jersey." City Br. 50. It even goes so far as to assert that "it would be *irresponsible* for the NYPD not to have an understanding of the varied mosaic that is the Muslim community to respond to such threats." *Id.* (emphasis added). But because heightened scrutiny applies in this case, we cannot accept the City's invitation to dismiss Plaintiffs' Complaint based on its assurance that the Program is justified by national-security and public-safety concerns. Rather, the burden of producing evidence to overcome heightened scrutiny's presumption of unconstitutionality is that of the City, *cf. Aiken v. City of Memphis,* 37 F.3d 1155, 1163 (6th Cir.1994) (*en banc*) ("When, as here, a race-based affirmative action plan is subjected to strict scrutiny, the party defending the plan bears the burden of producing evidence that the plan is constitutional."), and must be met *after* its Motion to Dismiss.

[35] To be clear, we acknowledge that a principal reason for a government's existence is to provide security. But while we do not question the legitimacy of the City's interest, "[t]he gravity of the threat alone cannot be dispositive of questions concerning what means law enforcement officers may employ to pursue a given purpose." *City of Indianapolis v. Edmond,* 531 U.S. 32, 42, 121 S.Ct. 447, 148 L.Ed.2d 333 (2000). Rather, heightened scrutiny requires that the relationship between the asserted justification and discriminatory means employed "be substantiated by objective evidence." *Patrolmen's Benevolent Ass'n of New York v. City of New York,* 310 F.3d 43, 53 (2d Cir.2002). "[M]ere speculation or conjecture is insufficient," *id.,* as are appeals to " 'common sense' which might be inflected by stereotypes," *Reynolds v. City of Chicago,* 296 F.3d 524, 526 (7th Cir.2002) (Posner, J.). *See also Lomack v. City of Newark,* 463 F.3d 303, 310 (3d Cir.2006) (citing with approval *Patrolmen's Benevolent Ass'n,* 310 F.3d at 52–53).

[36] And "[e]ven in the limited circumstance" where a suspect or quasi-suspect classification "is permissible to further [an important or] compelling state interest, the government is still 'constrained in how it may pursue that end.' " *Grutter v. Bollinger,* 539 U.S. 306, 333, 123 S.Ct. 2325, 156 L.Ed.2d 304 (2003) (second alteration in original) (quoting *Shaw v. Hunt,* 517 U.S. 899, 908, 116 S.Ct. 1894, 135 L.Ed.2d 207 (1996) (internal quotation marks and citation omitted)). While "[a] classification does not fail rational-basis review because it is not made with mathematical nicety or because in practice it results in some inequality," *Heller,* 509 U.S. at 321, 113 S.Ct. 2637 (internal quotation marks omitted), strict scrutiny requires that "the classification at issue ... 'fit' with greater precision than any alternative means," *Wygant v. Jackson Bd. of Educ.,* 476 U.S. 267, 280 n. 6, 106 S.Ct. 1842, 90 L.Ed.2d 260 (1986) (plurality opinion) (citing John Hart Ely, *The Constitutionality of Reverse Racial Discrimination,* 41 U. Chi. L.Rev. 723, 727 n. 26 (1974)). Intermediate scrutiny falls somewhere in between the two, asking if there is a "direct, substantial relationship between objective and means." *Hogan,* 458 U.S. at 725, 102 S.Ct. 3331.

No matter how tempting it might be to do otherwise, we must apply the same rigorous standards even where national security is at stake. We have learned from experience that it is often where the asserted *307 interest appears most compelling that we must be most vigilant in protecting constitutional rights. "[H]istory teaches that grave threats to liberty often come in times of urgency, when constitutional rights seem too extravagant to endure." *Skinner v. Ry. Labor Execs.' Ass'n,* 489 U.S. 602, 635, 109 S.Ct. 1402, 103 L.Ed.2d 639 (1989) (Marshall, J., dissenting); *see also Grutter,* 539 U.S. at 351, 123 S.Ct. 2325 (Scalia, J., concurring in part and dissenting in part) ("The lesson of *Korematsu [v. United States,* 323 U.S. 214, 223, 65 S.Ct. 193, 89 L.Ed. 194 (1944)] is that national security constitutes a 'pressing public necessity,' though the government's use of [a suspect classification] to advance that objective must be [appropriately] tailored."); *Skinner,* 489 U.S. at 635, 109 S.Ct. 1402 (Marshall, J. dissenting) ("The World War II relocation-camp cases and the Red scare and McCarthy-era internal subversion cases are only the most extreme reminders that when we allow fundamental freedoms to be sacrificed in the name of real or perceived exigency, we invariably come to regret it." (citations omitted)).

Today it is acknowledged, for instance, that the F.D.R. Administration and military authorities infringed the constitutional rights of Japanese–Americans during World War II by placing them under curfew and removing them from their West Coast homes and into internment camps. Yet when these citizens pleaded with the courts to uphold their constitutional rights, we passively accepted the Government's representations that the use of such classifications was necessary to the national interest. *Hirabayashi,* 320 U.S. 81, 63 S.Ct. 1375; *Korematsu,* 323 U.S. 214, 65 S.Ct. 193. In doing so, we failed to recognize that the discriminatory treatment of approximately 120,000 persons of Japanese ancestry was fueled not by military necessity but unfounded fears. *See United States v. Hohri,* 482 U.S. 64, 66, 107 S.Ct. 2246, 96 L.Ed.2d 51 (1987); *see also* Act to Implement Recommendations on the Commission of Wartime Relocation and Internment of Civilians, Pub.L. 100–383, § 2(a), 102 Stat. 903–04 (1988). Given that "unconditional deference to [the] government['s] ... invocation of 'emergency' ... has a lamentable place in our history," *Patrolmen's Benevolent Ass'n,* 310 F.3d at 53–54 (citing *Korematsu,* 323 U.S. at 223, 65 S.Ct. 193), the past should not preface yet again bending our constitutional principles merely because an interest in national security is invoked.

In sum, because Plaintiffs have plausibly alleged that the City engaged in intentional discrimination against a protected class, and because that classification creates a presumption of unconstitutionality that remains the City's obligation to rebut, Plaintiffs have stated a claim under the Equal Protection Clause of the Fourteenth Amendment.

B. First–Amendment Claims

We finally reach Plaintiffs' claims under the Religion

Clauses of the First Amendment. They allege violations of both the Establishment Clause and the Free Exercise Clause, which respectively prohibit the making of any "law respecting an establishment of religion" or "prohibiting the free exercise thereof." U.S. Const. Amend. I.

Plaintiffs bring both claims under the theory that the First Amendment demands strict governmental neutrality among religious sects. While it is intuitive that discriminatory conduct that inhibits a person's full religious expression may run afoul of the Free Exercise Clause of the First Amendment, under the facts here the same is counterintuitive for the Establishment Clause, as the latter ***308** "tend[s] to [involve] challenge[s] to governmental *endorsement.*" *Catholic League for Religious & Civil Rights v. City of San Francisco,* 624 F.3d 1043, 1050 n. 20 (9th Cir.2010) (*en banc*) (emphasis added). *But see Colo. Christian Univ. v. Weaver,* 534 F.3d 1245, 1266 (10th Cir.2008) (McConnell, J.) ("[S]tatutes involving discrimination on the basis of religion, including interdenominational discrimination, are subject to heightened scrutiny whether they arise under the Free Exercise Clause, the Establishment Clause, or the Equal Protection Clause...." (citations omitted)). However, a full discussion of either Religion Clause and its application to our case is unnecessary, as we confine ourselves to the City's arguments raised in its Motion to Dismiss. Those arguments are unpersuasive.

[37] The City first argues that, "according to a three month fact finding investigation by the New Jersey Attorney General, the surveillance Program did not violate New Jersey civil or criminal law." City Br. 44. That this argument could defeat a federal constitutional claim, let alone on a motion to dismiss, borders on the frivolous. Aside from a court's inability to consider such matters extraneous to the pleadings under Federal Rule of Civil Procedure 12(b)(6), it is the United States Constitution—not the "civil or criminal law" of New Jersey—that Plaintiffs seek to enforce. But even more fundamentally, the New Jersey Attorney General's legal conclusion is not helpful in determining whether the City violated Plaintiffs' constitutional rights. "It is emphatically the province and duty of the judicial department"—not the New Jersey executive—"to say what the law is." *Marbury v. Madison,* 5 U.S. (1 Cranch) 137, 177, 2 L.Ed. 60 (1803).

The City's only other argument (aside from a few scattered citations to free-speech and privacy cases that have little application to Plaintiffs' religion claims) is buried in a footnote in its brief amidst a discussion of the Equal Protection Clause:

> [Plaintiffs have also failed to] allege[ ] a classification that violates the Free Exercise and Establishment Clauses of the First Amendment because such claims [similarly] require a showing of *discriminatory purpose. See Church of Lukumi Babalu Aye, Inc. v. City of Hialeah,* 508 U.S. 520, 540, 113 S.Ct. 2217, 124 L.Ed.2d 472 (1993) ("Here, as in equal protection cases, we may determine the city council's object from both direct and circumstantial evidence.") [sic]; *Lemon v. Kurtzman,* 403 U.S. 602, 612–13, 91 S.Ct. 2105, 29 L.Ed.2d 745 (1971) (in order to survive an Establishment Clause challenge, the government practice must (1) have a secular purpose, (2) have a primary effect that neither advances nor inhibits religion, and (3) not foster excessive state entanglement with religion).

City Br. 58 n. 20 (emphasis added). A sentence-long argument buried in a footnote is hardly a satisfactory way to tackle two of the most jurisprudentially challenging and nuanced areas of our law. *Schempp,* 374 U.S. at 246, 83 S.Ct. 1560 (Brennan, J., concurring) (noting "the difficulty ... endemic to issues implicating the religious guarantees of the First Amendment"); *Robinson v. City of Edmond,* 160 F.3d 1275, 1282 (10th Cir.1998) (recognizing that the Establishment Clause is "an area notorious for its difficult case law"); *Harris v. City of Zion,* 927 F.2d 1401, 1410–11 (7th Cir.1991) ("[C]ases arising under the Religion Clauses of the [F]irst [A]mendment have presented some of the most perplexing questions in constitutional law."). We therefore consider this argument waived. *John Wyeth & Brother Ltd.* ***309** *v. CIGNA Int'l Corp.,* 119 F.3d 1070, 1076 n. 6 (3d Cir.1997) (Alito, J.) ("[A]rguments raised in passing (such as in a footnote), but not squarely argued, are considered waived.").

[38] But even if we were to consider the City's halfhearted assertion that allegations of overt hostility and prejudice are required to make out claims under the First Amendment, this argument would easily fail, just as did the identical argument with respect to the Equal Protection Clause. While the contours of neither the Free Exercise nor the Establishment Clause are static and well defined, courts have repeatedly rejected the notion that either Clause "is ... confined to actions based on animus." Laurence H. Tribe, *American Constitutional Law* §§ 5–16, at 956 (3d ed. 2000) ("[A] law that is not neutral or that is not generally applicable can violate the Free Exercise Clause without regard to the motives of those who enacted the measure."); *see also Shrum v. City of Coweta,* 449 F.3d 1132, 1144–45 (10th Cir.2006) (McConnell, J.) ("Proof of hostility or discriminatory motivation may be sufficient to prove that a challenged governmental action is not neutral, but the Free Exercise

Clause is not confined to actions based on animus." (citations omitted)); *Allen v. Morton,* 495 F.2d 65, 72 (D.C.Cir.1973) (Tamm, J., concurring) (noting that, under the Establishment Clause, "good motives cannot save impermissible actions"). At bottom, the City needs something other than this threadbare argument based on the absence of subjective hostility to avoid a non-swinging strikeout.

V. CONCLUSION

The allegations in Plaintiffs' Complaint tell a story in which there is standing to complain and which present constitutional concerns that must be addressed and, if true, redressed. Our job is judicial. We "can apply only law, and must abide by the Constitution, or [we] cease to be civil courts and become instruments of [police] policy." *Korematsu,* 323 U.S. at 247, 65 S.Ct. 193 (Jackson, J., dissenting).

We believe that statement of Justice Jackson to be on the right side of history, and for a majority of us in quiet times it remains so ... until the next time there is the fear of a few who cannot be sorted out easily from the many. Even when we narrow the many to a class or group, that narrowing—here to those affiliated with a major worldwide religion—is not near enough under our Constitution. "[T]o infer that examples of individual disloyalty prove group disloyalty and justify discriminatory action against the entire group is to deny that under our system of law individual guilt is the sole basis for deprivation of rights." *Id.* at 240, 65 S.Ct. 193 (Murphy, J., dissenting).

What occurs here in one guise is not new. We have been down similar roads before. Jewish–Americans during the Red Scare, African–Americans during the Civil Rights Movement, and Japanese–Americans during World War II are examples that readily spring to mind. We are left to wonder why we cannot see with foresight what we see so clearly with hindsight—that "[l]oyalty is a matter of the heart and mind[,] not race, creed, or color." *Ex parte Mitsuye Endo,* 323 U.S. 283, 302, 65 S.Ct. 208, 89 L.Ed. 243 (1944).

We reverse and remand for further proceedings consistent with this opinion.

ROTH, Circuit Judge, concurrence.

I agree that plaintiffs have demonstrated standing and made sufficient allegations of violations of equal-protection rights .. I differ from the majority in its failure to determine whether "intermediate scrutiny" or "strict scrutiny" applies here. In our determinations so far, we have also, I believe, ***310** made the findings necessary to resolve the issue of the appropriate level of scrutiny.

In my opinion, "intermediate scrutiny" is appropriate here. I say this because "intermediate scrutiny" is the level applied in gender discrimination cases. I have the immutable characteristic of being a woman. I am happy with this condition, but during my 80 years on this earth, it has caused me at times to suffer gender discrimination. My remedy now for any future gender discrimination would be reviewed with "intermediate scrutiny." For that reason, I cannot endorse a level of scrutiny in other types of discrimination cases that would be stricter than the level which would apply to discrimination against me as a woman.

All Citations

804 F.3d 277

Footnotes

1 *See, e.g., Davis v. Guam,* 785 F.3d 1311, 1315 (9th Cir.2015) ("[E]qual treatment under law is a judicially cognizable interest ... even if it brings no tangible benefit to the party asserting it."); *Am. Civil Liberties Union of N.M. v. Santillanes,* 546 F.3d 1313, 1319 (10th Cir.2008) ("The injury in fact is the denial of equal treatment."); *Planned Parenthood of S.C. Inc. v. Rose,* 361 F.3d 786, 790 (4th Cir.2004) ("Discriminatory treatment ... qualif[ies] as an actual injury for standing purposes."); *Lutheran Church–Mo. Synod v. FCC,* 154 F.3d 487, 493 (D.C.Cir.1998) ("[T]he claim that the litigant was denied equal treatment is sufficient to constitute Article III 'injury in-fact.' "); *Peyote Way Church of God, Inc. v. Thornburgh,* 922 F.2d 1210, 1214 n. 2 (5th Cir.1991) ("[I]llegitimate unequal treatment is an injury unto itself....").

2 Plaintiffs' personal interest in religious equality falls squarely within the zone of those protected by the constitutional guarantees in question. While their claims certainly strike at the heart of the Equal Protection Clause of the Fourteenth Amendment, the First Amendment's guarantee of freedom of religion includes freedom from religious discrimination. *See, e.g., Permoli v. Municipality No. 1 of New Orleans,* 44 U.S. 589, 597, 3 How. 589, 11 L.Ed. 739 (1845) ("Equality

before the law is of the very essence of liberty, whether civil or religious."); *Colo. Christian Univ. v. Weaver*, 534 F.3d 1245, 1257 (10th Cir.2008) (McConnell, J.) ("From the beginning, this nation's conception of religious liberty included, at a minimum, the equal treatment of all religious faiths without discrimination or preference."); *cf.* Karl Loewenstein, *Some General Observations on the Proposed "International Bill of Rights"* 17 (1942).
"[T]he Religion Clauses ... and the Equal Protection Clause as applied to religion ... all speak with one voice on this point: Absent the most unusual circumstances, one's religion ought not affect one's legal rights or duties or benefits." *Bd. of Educ. of Kiryas Joel Vill. Sch. Dist. v. Grumet*, 512 U.S. 687, 715, 114 S.Ct. 2481, 129 L.Ed.2d 546 (1994) (O'Connor, J., concurring in part and concurring in the judgment in part); *see also, e.g., Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 845, 115 S.Ct. 2510, 132 L.Ed.2d 700 (1995); *Larson v. Valente*, 456 U.S. 228, 244–45, 102 S.Ct. 1673, 72 L.Ed.2d 33 (1982); *Comm. for Pub. Educ. & Religious Liberty v. Nyquist*, 413 U.S. 756, 792–93, 93 S.Ct. 2955, 37 L.Ed.2d 948 (1973); *Gillette v. United States*, 401 U.S. 437, 449, 91 S.Ct. 828, 28 L.Ed.2d 168 (1971); *Epperson v. Arkansas*, 393 U.S. 97, 104, 89 S.Ct. 266, 21 L.Ed.2d 228 (1968); *Everson v. Bd. of Educ. of Ewing Twp.*, 330 U.S. 1, 15, 67 S.Ct. 504, 91 L.Ed. 711 (1947).

3 We do not take a position on whether Plaintiffs could have brought suit to vindicate such an interest. They do not allege a violation of some constitutional right to privacy, but to equal treatment.

4 Far from attesting to the NYPD and AP's respective roles in revealing the once-secret Program, the affidavit of defense counsel on which the City relies merely states that the AP reported on the NYPD's conduct and "released [unredacted] documents to the public at large beginning in ... August 2011." Decl. of Peter G. Farrell ¶ 3. It is impossible to infer reasonably, let alone conclude, from this statement that the AP was the first (or only) public source of the information or that the NYPD played no role for which it may be held legally responsible.
Moreover, even if they were required to do so, Plaintiffs have produced ample evidence in rebuttal showing that: (1) "[a] former NYPD informant ... independently [of the AP] revealed the NYPD's practice of targeting innocent Muslims" by "sp[eaking] publicly in great detail about his part in the NYPD's policy and practice of surveilling Muslims on the basis of religion," Decl. of Glenn Katon ¶ 4; and (2) "[s]ince the AP began publishing reports regarding the NYPD's policy and practice of targeting Muslims for surveillance, senior New York City officials have acknowledged and endorsed the NYPD's tactics," thus "propagat[ing] and amplif[ying] the harm," *id.* ¶ 3.

5 To the extent the City focuses on Plaintiffs' failure to allege the existence of a written policy, there is no requirement that a policy be reduced to written form. *See, e.g., Johnson v. California*, 543 U.S. 499, 502, 509, 125 S.Ct. 1141, 160 L.Ed.2d 949 (2005) (holding that an "unwritten [prison] policy of racially segregating prisoners in double cells" was subject to strict scrutiny). As the Ninth Circuit has explained, "[t]he primary—indeed, perhaps only—difference [between a suit involving a written and unwritten policy] is an evidentiary one." *Hoye v. City of Oakland*, 653 F.3d 835, 855 (9th Cir.2011). While a "[p]laintiff [ ] ha[s] no difficulty establishing what a policy is when the policy is written," "[a]n unwritten policy, by contrast, is usually harder to establish." *Id.*

6 To the extent the City means to argue that Plaintiffs have failed to allege plausibly that even these exemplars have not been singled out by reason of their religious affiliation, we disagree. Plaintiffs' allegations, which draw on the sources of circumstantial evidence commonly used to make out a *prima facie* case of intentional discrimination in a disparate-treatment suit of this type, easily satisfy the plausibility threshold required to survive a motion to dismiss. *See, e.g., Rojas v. Alexander's Dep't Store, Inc.*, 924 F.2d 406, 410 (2d Cir.1990) ("maintenance of records of the race of the arrestees"); *Marshall v. Colum. Lea Reg'l Hosp.*, 345 F.3d 1157, 1170 (10th Cir.2003) (McConnell, J.) (racial designation on a driving-citation form "where none was called for"); *Jean v. Nelson*, 711 F.2d 1455, 1495–96 (11th Cir.1983) (statistical evidence showing "glaring" effect on protected class); *Floyd v. City of New York*, 959 F.Supp.2d 540, 587 (S.D.N.Y.2013) (disparities between minority groups in "hit rates" combined with other evidence); *Rodriguez v. Cal. Highway Patrol*, 89 F.Supp.2d 1131, 1141 (N.D.Cal.2000) (statistical evidence).

7 This of course is not to say that an absence or presence of reasonable suspicion in a particular case determines the viability of a plaintiff's equal-protection claim. *Cf. Whren v. United States*, 517 U.S. 806, 813, 116 S.Ct. 1769, 135 L.Ed.2d 89 (1996) ("[T]he Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment. Subjective intentions play no role in ordinary, probable-cause Fourth Amendment analysis."); *United States v. Scopo*, 19 F.3d 777, 786 (2d Cir.1994) (Newman, C.J., concurring) ("Though the Fourth Amendment permits a pretext arrest, if otherwise supported by probable cause, the Equal Protection Clause still imposes restraint on impermissibly class-based discriminations.").
But although a lack of reasonable suspicion does not afford a presumption that a law-enforcement officer initiated an investigation on the basis of a protected characteristic, it is certainly one factor that may be considered by a finder of fact. *See Bennett v. City of Eastpointe*, 410 F.3d 810, 822 n. 1 (6th Cir.2005) ("While the stop was justified from a Fourth Amendment perspective ... [,] the lack of suspicion ... may properly be considered in the plaintiffs' selective-enforcement claim."); *Anderson v. Cornejo*, 284 F.Supp.2d 1008, 1055 (N.D.Ill.2003) (citing "the lack of

adequate suspicion for a strip search" as probative of the fact that a customs officer "acted, at least in part, because [the plaintiff was] an African–American woman").

8 Although other modes of analysis have also been employed, *see, e.g., Obergefell v. Hodges,* —— U.S. ——, 135 S.Ct. 2584, 2596, 192 L.Ed.2d 609 (2015), we find it appropriate to apply the conventional two-part framework in the context of this case.

9 "Strict scrutiny" is also triggered in the case of a "fundamental right." While "the right to free exercise of religion" is fundamental, *Lewis,* 518 U.S. at 404, 116 S.Ct. 2174, Plaintiffs proceed in this case on the theory that religious affiliation is a protected class.

10 We refer in this opinion only to discrimination based on religious *affiliation* rather than *involvement.* Case law distinguishes between the two. *See, e.g., United States v. DeJesus,* 347 F.3d 500, 510 (3d Cir.2003) (Fuentes, J.) ("Because we affirm the District Court's finding that the government's strikes were based on the jurors' heightened religious involvement rather than their religious affiliation, we need not reach the issue of whether a peremptory strike based solely on religious affiliation would be unconstitutional."); *United States v. Stafford,* 136 F.3d 1109, 1114 (7th Cir.1998) (Posner, C.J.) (explaining that "[i]t is necessary to distinguish among religious affiliation, a religion's general tenets, and a specific religious belief"), *modified,* 136 F.3d 1115 (7th Cir.1998). Nor do we mean to state a position on the separate "question of whether all religions together constitute a suspect or quasi-suspect class." *Christian Sci. Reading Room Jointly Maintained v. City of San Francisco,* 807 F.2d 1466, 1467 n. 1 (9th Cir.1986) (Norris, J., dissenting from the denial of rehearing *en banc*) (stating this as a separate issue that the panel expressly declined to decide).

11 Some appellate courts have recognized the question as an open one, *see, e.g., St. John's United Church of Christ v. City of Chicago,* 502 F.3d 616, 638 (7th Cir.2007); *Wirzburger v. Galvin,* 412 F.3d 271, 283 (1st Cir.2005); *Taylor v. Johnson,* 257 F.3d 470, 473 n. 2 (5th Cir.2001) (*per curiam*), but we are not aware of a single circuit court holding that religious classifications are subject to only rational-basis review.
We also note that numerous state courts either have held that religious affiliation is a suspect classification or have issued opinions with strong *dicta* to that effect. *See, e.g., Bagley v. Raymond Sch. Dep't,* 728 A.2d 127, 137 (Me.1999); *Marrujo v. N.M. State Highway Transp. Dep't,* 118 N.M. 753, 887 P.2d 747, 751 (1994); *Bd. of Cnty. Comm'rs of Saguache v. Flickinger,* 687 P.2d 975, 982 n. 9 (Colo.1984) (*en banc*); *State v. Correll,* 626 S.W.2d 699, 701 (Tenn.1982); *Burmaster v. Gravity Drainage Dist. No. 2 of St. Charles Parish,* 366 So.2d 1381, 1386 n. 3 (La.1978); *Gunn v. Lane County,* 173 Or.App. 97, 20 P.3d 247, 251 (2001); *LaCava v. Lucander,* 58 Mass.App.Ct. 527, 791 N.E.2d 358, 363 (2003). *But see State v. Purcell,* 199 Ariz. 319, 18 P.3d 113, 121 (Ct.App.2001) ("In addition to being a fundamental right, religious affiliation also *may* be a suspect classification under the Equal Protection Clause." (emphasis added)); *State v. Davis,* 504 N.W.2d 767, 771 (Minn.1993), *cert. denied,* 511 U.S. 1115, 114 S.Ct. 2120, 128 L.Ed.2d 679 (1994); *Casarez v. State,* 913 S.W.2d 468 (Tex.Crim.App.1994).

12 *Ashwander v. Tenn. Valley Auth.,* 297 U.S. 288, 347, 56 S.Ct. 466, 80 L.Ed. 688 (1936) (Brandeis, J., concurring) ("It is not the habit of the court to decide questions of a constitutional nature unless absolutely necessary to a decision of the case." (quoting *Burton v. United States,* 196 U.S. 283, 295, 25 S.Ct. 243, 49 L.Ed. 482 (1905))); *Liverpool, N.Y. & Phila. S.S. Co. v. Comm'rs of Emigration,* 113 U.S. 33, 39, 5 S.Ct. 352, 28 L.Ed. 899 (1885) ("In the exercise of [its] jurisdiction, [the Court must] ... never ... formulate a rule of constitutional law broader than is required by the precise facts to which it is to be applied."); *Ala. State Fed'n of Labor v. McAdory,* 325 U.S. 450, 461, 65 S.Ct. 1384, 89 L.Ed. 1725 (1945) ("It has long been [the Court's] considered practice not .. to decide any constitutional question in advance of the necessity for its decision.").

13 Other courts have drawn on the definition of "immutable" in immigration cases when defining the term in the context of an equal-protection suit. *Latta v. Otter,* 771 F.3d 456, 464 n. 4 (9th Cir.2014) (quoting an immigration case for the proposition that "[s]exual orientation and sexual identity are immutable; they are so fundamental to one's identity that a person should not be required to abandon them" (alteration in original)), *cert. denied,* —— U.S. ——, 135 S.Ct. 2931, 192 L.Ed.2d 609 (2015).

14 Aziz Z. Huq, *The Signaling Function of Religious Speech in Domestic Counterterrorism,* 89 Tex. L.Rev. 833, 852 (2011) (recognizing that religion lies "at the core of many individuals' understanding of their identity"); David B. Salmons, Comment, *Toward a Fuller Understanding of Religious Exercise: Recognizing the Identity–Generative and Expressive Nature of Religious Devotion,* 62 U. Chi. L.Rev. 1243, 1258 (1995) (noting the "fundamental role [that religious preference] play[s] in shaping an individual's concept of identity and personhood"); Note, *Reinterpreting the Religion Clauses: Constitutional Construction and Conceptions of the Self,* 97 Harv. L.Rev. 1468, 1474 (1984) ("A society that failed to protect religion would foreclose the individual's choice of the most fundamental part of his identity.").

15 Indeed, the close relationship among race, religion, ethnicity, and national origin is reflected by the allegations in Plaintiffs' Complaint. *See, e.g.,* Compl. ¶ 40 ("In addition to targeting Muslims by focusing on mosques, Muslim-owned businesses, and other Muslim-associated organizations as subjects of surveillance, the Program also intentionally targets Muslims by using ethnicity as a proxy for faith."); *id.* ¶ 41 ("As part of the Program, the Department has designated twenty-eight countries and 'American Black Muslim' as 'ancestries of interest.' "); *id.* ¶ 53 ("To facilitate future surveillance of entire American Muslim communities, the NYPD has created maps indicating the locations of mosques, restaurants, retail establishments, and schools owned by or serving Muslims, as well as ethnic populations from heavily Muslim countries."); *id.* ¶ 55 ("The NYPD also inspects records of name changes and compiles databases of new Muslim converts who take Arabic names, as well as Muslims who take names that are perceived to be 'Western.' ").

16 Act of Mar. 1, 1875, ch. 114, 18 Stat. 335 ("[I]t is essential to just government we recognize the equality of all men before the law, and hold that it is the duty of government in its dealings with the people to mete out equal and exact justice to all, of whatever nativity, race, color, or persuasion, religious or political....").

17 *See, e.g.,* U.S. Patriot Act of 2001, Pub.L. 107–56, § 102(a)(3), b(3), 115 Stat. 274 ("The concept of individual responsibility for wrongdoing is sacrosanct in American society, and applies equally to all religious, racial, and ethnic groups.... [T]he Nation is called upon to recognize the patriotism of fellow citizens from all ethnic, racial, and religious backgrounds.").

End of Document

How DNA on coffee cup led to arrest in 1972 rape, murder of woman: Officials

Jody Loomis, 20, was shot in the head on August 23, 1972.

By Emily Shapiro
April 11, 2019, 2:29 PM • 7 min read

How DNA on coffee cup led to arrest in 1972 rape, murder of woman: Officials

A 77-year-old Washington state man was arrested Wednesday decades after he allegedly killed a 20-year-old woman, and police say he was nabbed through the novel technique of genetic genealogy.

Snohomish County Sheriff's Office

A 77-year-old Washington state man was arrested Wednesday decades after he allegedly killed a 20-year-old woman, and police say he was nabbed through the novel technique of genetic genealogy.

On August 23, 1972, Jody Loomis was on her way to the stables to ride her horse when she was attacked and shot in the head, officials with the Snohomish County Sheriff's Office said at a news conference on Thursday. She was raped and her body was left mostly nude, officials said.

DNA was recovered from semen at the scene and that DNA was later uploaded to the law enforcement database CODIS, but there was never a hit on the sample, investigators said.

Top Stories

How DNA on coffee cup led to arrest in 1972 rape, murder of woman: Officials
Apr 11, 2:29 PM

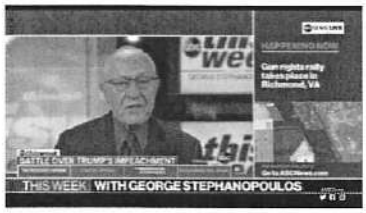
At least 2 dead, 15 injured in Kansas City shooting
Jan 20, 2:49 AM

Top prosecutor receives a racist voicemail, posts it on social media
Jan 18, 2:23 PM

Revered singer-songwriter David Olney dies on stage mid-performance
Jan 20, 4:34 AM

Woman injures 2 after allegedly driving into traffic as a test of faith
Jan 19, 2:08 AM

ABC News Live



24/7 coverage of breaking news and live events

Poster requesting information in the death of Jody Loomis
Snohomish County Sheriff's Office

+ (MORE: Prosecutors to seek death penalty in 'Golden State Killer' case)

The case went cold until the new technique known as genetic genealogy led police to their suspect in 2018.

Genetic genealogy takes the DNA of an unknown killer left behind at a crime scene and identifies a suspect by tracing the family tree through his or her family members, who voluntarily submit their DNA to public genealogy databases. The first public arrest through genetic genealogy was the April 2018 arrest of the suspected "Golden State Killer," and since then, genetic genealogy has helped identify more than 40 suspects in violent crimes.

In 2018, DNA from a semen stain on a boot Loomis was wearing was compared to genetic databases. Genealogists then began to build a family tree, according to the probable cause affidavit.

Jody Loomis and her horse in 1972
Snohomish County Sheriff's Office

+ (MORE: Brother of woman slain on vacation in 1973 calls suspect's arrest 'bittersweet')

Genealogists concluded in August that the unknown DNA profile belonged to one of six brothers. Police zeroed in on one of them, Terrence Miller, who had prior sex offenses, the probable cause affidavit said.

On Aug. 29, 2018, investigators followed Miller to a casino and recovered a coffee cup he threw into the trash; tests later confirmed the DNA on the coffee cup matched the DNA from the sperm on the victim's boot, the probable cause affidavit said.

In November, two undercover detectives went to Millers' home in Edmonds, Washington, where Miller and his wife run a ceramic shop out of their garage, said the probable cause affidavit.

+ (MORE: Young women murdered decades ago may finally find justice through new controversial DNA tool)

After Miller's wife invited the detectives into the garage, they noticed a newspaper from May 2018 on the table, the document said. On the front

page was an article on how genetic genealogy led to an arrest in a local double murder, and that crime also involved rape and gunshot wounds to the head, the document said.

"The presence of the newspaper seemed, at best, an odd coincidence," a prosecutor wrote in the probable cause affidavit. "A fair interference could also be drawn that [the] defendant was keeping track of the techniques law enforcement was using to solve cold cases."

+ (MORE: 'Almost got away with murder': How a job application led to an arrest in woman's 1998 cold case killing)

Miller is a lifelong resident of Snohomish County. Before the crime, he had been divorced twice and had three daughters, according to documents.

At the time of the crime, Miller was 33 years old and living with his third wife, who has since died, according to documents. He also had two daughters with his third wife.

His current wife is his fourth.

+ (MORE: 'Please help my daughter': Maura Murray, 21, has been missing since 2004. New search finds no evidence but her dad's not satisfied)

Miller was arrested at his home on Wednesday and is accused of first-degree murder, according to court documents. He was interviewed on Wednesday but declined to give statements to police, authorities said.

Miller did not know Loomis before the crime, according to authorities.

He is due to make his first court appearance Thursday afternoon, officials said.

What is DNA?

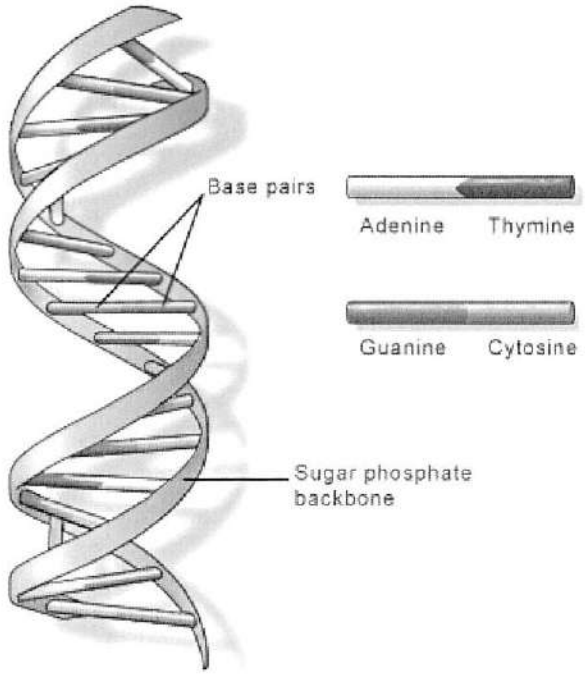
DNA, or deoxyribonucleic acid, is the hereditary material in humans and almost all other organisms. Nearly every cell in a person's body has the same DNA. Most DNA is located in the cell nucleus (where it is called nuclear DNA), but a small amount of DNA can also be found in the mitochondria (where it is called mitochondrial DNA or mtDNA). Mitochondria are structures within cells that convert the energy from food into a form that cells can use.

The information in DNA is stored as a code made up of four chemical bases: adenine (A), guanine (G), cytosine (C), and thymine (T). Human DNA consists of about 3 billion bases, and more than 99 percent of those bases are the same in all people. The order, or sequence, of these bases determines the information available for building and maintaining an organism, similar to the way in which letters of the alphabet appear in a certain order to form words and sentences.

DNA bases pair up with each other, A with T and C with G, to form units called base pairs. Each base is also attached to a sugar molecule and a phosphate molecule. Together, a base, sugar, and phosphate are called a nucleotide. Nucleotides are arranged in two long strands that form a spiral called a double helix. The structure of the double helix is somewhat like a ladder, with the base pairs forming the ladder's rungs and the sugar and phosphate molecules forming the vertical sidepieces of the ladder.

An important property of DNA is that it can replicate, or make copies of itself. Each strand of DNA in the double helix can serve as a pattern for duplicating the sequence of bases. This is critical when cells divide because each new cell needs to have an exact copy of the DNA present in the old cell.

DNA is a double helix formed by base pairs attached to a sugar-phosphate backbone.



Credit: U.S. National Library of Medicine

For more information about DNA:

The National Human Genome Research Institute fact sheet Deoxyribonucleic Acid (DNA) provides an introduction to this molecule.

StatedClearly offers a video introduction to DNA and how it works.

The New Genetics, a publication of the National Institute of General Medical Sciences, discusses the structure of DNA and how it was discovered.

A basic explanation and illustration of DNA can be found on Arizona State University's "Ask a Biologist" website.

The Virtual Genetics Education Centre, created by the University of Leicester, offers additional information on DNA, genes, and chromosomes.

An overview of mitochondrial DNA is available from the Neuromuscular Disease Center at Washington University.

TheScientist
EXPLORING LIFE, INSPIRING INNOVATION

Neanderthal DNA in Modern Human Genomes Is Not Silent

From skin color to immunity, human biology is linked to our archaic ancestry.

Sep 1, 2019
JEF AKST

ABOVE: © SCIENCESOURCE, S. ENTRESSANGLE and E. DAYNES

After the 2010 publication of the Neanderthal draft genome sequence, evolutionary biologist Joshua Akey, then at the University of Washington in Seattle, and his graduate student Benjamin Vernot began looking into its most provocative implication: that the ancient hominins had bred with the ancestors of modern humans. Neanderthals had been living in Eurasia for more than 300 millennia when some human ancestors left Africa some 60,000–70,000 years ago, and according to the 2010 publication, in which researchers compared the Neanderthal draft genome with modern human sequences, about 2 percent of the DNA in the genomes of modern-day people with Eurasian ancestry is Neanderthal in origin.[1]

To investigate the archaic ancestry of the living human population, Akey and Vernot set to work searching for Neanderthal DNA in modern genomes. They developed a statistical approach to identify genetic signatures suggestive of Neanderthal ancestry in the genomes of 379 European and 286 East Asian individuals. The endeavor was further powered by the first high-quality Neanderthal genome sequence, which gave the duo confidence that the sequences they'd identified were indeed of archaic origin. Still, in the back of Akey's mind, he had doubts about the research. "I remember telling Ben [when] we were working on this, 'I wake up every day in a cold sweat that this is all just incomplete lineage sorting'"—a methodological artifact that would undermine their conclusions about Neanderthal ancestry, meaning the sequences were the result of the common ancestry the two groups shared.

Then, as Vernot and Akey were getting ready to submit their work for publication, their department got a visit from Svante Pääbo, a geneticist at the Max Planck Institute for Evolutionary Anthropology who had pioneered techniques for extracting and analyzing DNA from ancient specimens and had led the early Neanderthal genome efforts. They spoke with him about their ongoing project, and Pääbo noted that his collaborator, David Reich at Harvard Medical School, was pursuing a very similar line of research. So Akey gave Reich a call.

"The end result [of the conversation] was we agreed to coordinate publication," Akey recalls. "We also agreed not to even look at each other's papers because we didn't want to influence the results in any way."

See "Simultaneous Release"

Vernot and Akey submitted to *Science*;[2] Reich and his colleagues submitted to *Nature*.[3] The two journals synchronized publication of the papers at the end of January 2014. The day they went live, Akey anxiously began to read the paper from the Reich group. "I remember sitting in my office, reading it, and really sort of just going through the checklist" of the key results, he says. Quickly, the relief set in. "We essentially said the exact same thing," Akey recalls. "Usually when you publish something, it's years before you see validation. . . . This was sort of instant gratification."

> Was it just this curious feature of human history that didn't have an impact, or did it alter the trajectory of human evolution?
>
> —Joshua Akey, Princeton University

The two groups had used different statistical approaches to identify Neanderthal DNA in modern human genomes, putting to bed any skepticism about the history of hominin group interbreeding. "[It was] the final nail on the coffin that it couldn't be anything else," says Janet Kelso, a computational biologist at the Max Planck Institute for Evolutionary Anthropology and a collaborator on Reich's publication.

With the issue of Neanderthal/modern human mating settled, scientists could focus on a new goal, says Akey, now at Princeton University. Namely, what was the consequence of this interbreeding? "Was it just this curious feature of human history that didn't have an impact, or did it alter the trajectory of human evolution?"

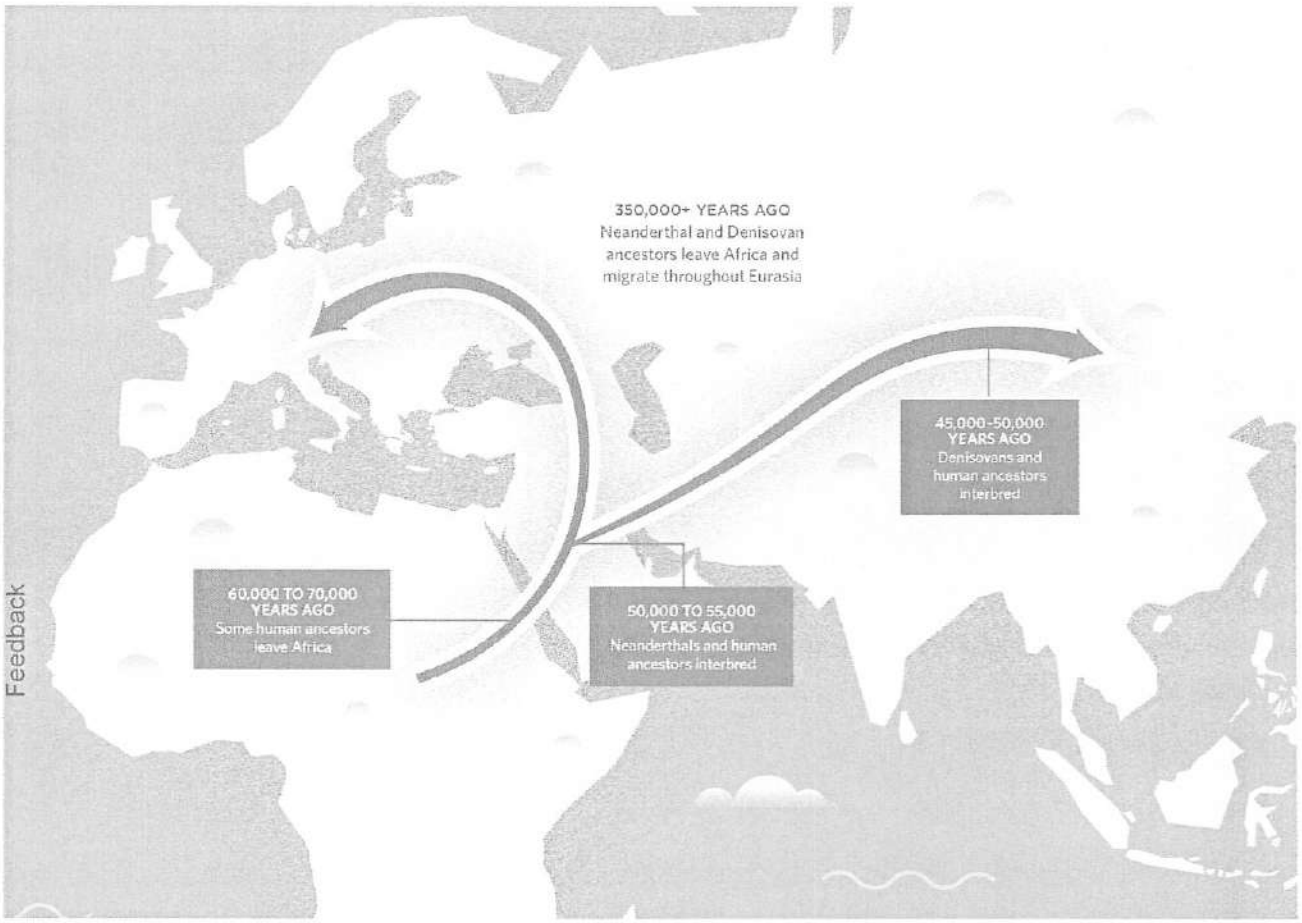
In the past five years, a flurry of research has sought to answer that question. Genomic analyses have associated Neanderthal variants with differences in the expression levels of diverse genes and of phenotypes ranging from skin and hair color to immune function and neuropsychiatric disease. But researchers cannot yet say how these archaic sequences affect people today, much less the humans who acquired them some 50,000–55,000 years ago.

"So far I have not seen any convincing functional studies where you take the Neanderthal variant and the human variant and do controlled experiments" to identify the physiological consequence, says Grayson Camp, a genomicist at the Institute of Molecular and Clinical Ophthalmology Basel (IOB) in Switzerland. "No one has actually shown yet in culture that a human and Neanderthal allele have a different physiological function. That will be exciting when someone does."

A Mixed History

Some 350,000 or more years ago, the group of hominins that would evolve to become Neanderthals and Denisovans left Africa for Eurasia.

A few hundred millennia later, about 60,000 to 70,000 years ago, the ancestors of modern non-Africans followed a similar path out of Africa and began interbreeding with these other hominin groups. Researchers estimate that much of the Neanderthal DNA in modern human genomes came from interbreeding events that took place around 50,000 to 55,000 years ago in the Middle East. Thousands of years later, humans moving into East Asia interbred with Denisovans.



See full infographic: WEB | PDF
THE SCIENTIST STAFF

Neanderthal in our skin

Most Neanderthal variants exist in only around 2 percent of modern people of Eurasian descent. But some archaic DNA is much more common, an indication that it was beneficial to ancient humans as they moved from Africa into Eurasia, which Neanderthals had called home for more

than 300,000 years. In their 2014 study, Vernot and Akey found several sequences of Neanderthal origin that were present in more than half of the genomes from living humans they studied. The regions that contained high frequencies of Neanderthal sequences included genes that could yield clues to their functional effect. Base-pair differences between Neanderthal and human variants rarely fall in protein-coding sequences, but rather in regulatory ones, suggesting the archaic sequences affect gene expression. (See "Denisovans in the Mix" below.)

A number of segments harbor genes that relate to skin biology, such as a transcription factor that regulates the development of epidermal cells called keratinocytes. These variants may underlie traits that were adaptive in the different climatic conditions and lower levels of ultraviolet light exposure at more northern latitudes. Reich's group similarly found genes involved in skin biology enriched in Neanderthal ancestry—that is, more than just a few percent of people carried Neanderthal DNA in these parts of the genome.

It was unclear, however, what specific effect the Neanderthal variants had on phenotype. For that, researchers needed phenotypic data on many different kinds of traits, paired with genetic information, for thousands of people. Vanderbilt University evolutionary geneticist Tony Capra has access to such a resource: the Electronic Medical Records and Genomics (eMERGE) Network. Right around the time the scientific community was beginning to map Neanderthal DNA in the genomes of living people, eMERGE organizers were compiling electronic health records and associated genetic data for tens of thousands of patients from nine health-care centers across the US. "We felt like we had a chance to evaluate some of those hypotheses [about functionality] on a larger scale in a real human population where we had rich phenotype data," says Capra.

> No one has actually shown yet in culture that a human and Neanderthal allele have a different physiological function. That will be exciting when someone does.
>
> —Grayson Camp,
> Institute of Molecular and Clinical Ophthalmology Basel

In collaboration with Akey and Vernot, who helped identify Neanderthal variants in the genetic data included in the database, Capra's group looked for links between the archaic DNA and more than 1,000 phenotypes across some 28,000 people of European ancestry. They reported in 2016 that Neanderthal DNA at various sites in the genome influences a range of immune and autoimmune traits, and there was some association with obesity and malnutrition, pointing to potential metabolic effects. The researchers also saw an association between Neanderthal ancestry and two types of noncancerous skin growths associated with dysfunctional keratinocyte biology—supporting the idea that the Neanderthal DNA was at one point selected for its effects on skin.[4]

"This was crazy to me," says Capra. "What these other groups had predicted based on just the pattern of occurrence—the presence and absence of Neanderthal ancestry around certain types of genes—we were actually seeing in a real human population, that having Neanderthal ancestry influenced traits related to those types of skin cells." What remains unclear, however, is what the benefits of the Neanderthal sequences were for those early humans.

At the same time, Kelso and her postdoc Michael Dannemann were taking a similar approach with a relatively new database called the UK Biobank (UKB), which includes data from around half a million British volunteers who filled out questionnaires about themselves, underwent medical exams, and gave blood samples for genotyping. Formally launched in 2006, the UKB published its 500,000-person-strong resource in 2015, and Kelso and Dannemann decided to see what information they could extract. Conveniently, the genotyping data specifically includes SNPs that can identify variants of Neanderthal origin, thanks to Reich's group, which provided UKB architects with a list of 6,000 Neanderthal variants.

Among the many links Kelso and Dannemann identified as they dug into data from more than 112,000 individuals in the UKB was, once again, an association between certain Neander-thal variants and aspects of skin biology.[5] Specifically, the archaic sequences spanning the *BNC2* gene—a stretch of the genome that Vernot and Akey had identified as having Neanderthal origin in some 70 percent of non-Africans—were very clearly associated with skin color. People who carried Neanderthal DNA there tended to have pale skin that burned instead of tanned, Kelso says. And the stretch that included *BNC2* was just one of many, she adds: around 50 percent of Neanderthal variants linked with phenotype in her study have something to do with skin or hair color.

The effect that Neanderthal DNA might have on skin appearance and function is "fascinating," says Akey. "Something that we're still really interested in and starting to do some experimental work on is: Can we understand what these genes do and then maybe what the selective pressure was that favored the Neanderthal version?"

See "Effects of Neanderthal DNA on Modern Humans"

Denisovans in the mix

Entrance to Denisova Cave archaeological site, Russia
BENCE VOILA, MAX PLANCK INSTITUTE FOR EVOLUTIONARY ANTHROPOLOGY

Neanderthals thrived in Eurasia as a dominant hominin group for hundreds of thousands of years and have long been a focus of scientific inquiry. But less than a decade ago, researchers discovered that there was another group of archaic hominins that coexisted with Neanderthals and the ancestors of modern humans. DNA collected from a single finger bone and two teeth appeared to be neither Neanderthal nor human, and scientists named a new group, the Denisovans, after the Siberian cave in which the remains were found in 2008.

Once researchers reconstructed the entire high-quality Denisovan genome in 2012 (*Science*, 338:222–26, 2012), it became clear that, like Neanderthals, Denisovans had interbred with modern humans during the time that they coinhabited Eurasia, with analyses suggesting that the introgressed DNA likely came from multiple Denisovan populations within the last 50,000 years, sometime after mixing occurred between Neanderthals and human ancestors (*Cell*, 173:P53–61.E9, 2018; *Cell*, 177:P1010–21.E32, 2019). Denisovan DNA makes up 4–6 percent of the genomes of people native to the islands of Melanesia, a subregion of Oceania, and to a lesser extent they left their genetic mark in other Pacific island populations and some modern East Asians, while it is largely absent from the genetic code of most other people. As with Neanderthal introgression, the question that remains to be answered is: What effect did these variants have on our own lineage—and are we still experiencing Denisovans' genetic influence?

As with Neanderthal DNA, experts have identified regions of modern human genomes that are significantly depleted of Denisovan DNA, and they saw that these "deserts" were the same ones that lacked Neanderthal sequences—indications of selection against deleterious variants (*Science*, 352:235–39, 2016). "That's as close as you can get to sort of a replication in this type of work," says Princeton University evolutionary biologist Joshua Akey. In terms of introgressed bits of Denisovan DNA that might have been beneficial to modern humans, researchers have found links to toll-like receptors and other contributors to immune function, similar to links found with Neanderthal variants.

Denisovan DNA may have also offered some unique benefits to ancient humans. One scientific team identified Denisovan variants in the genomes of Greenland Inuits that include genes involved in the development and distribution of adipose tissue, perhaps pointing to advantages in cold tolerance and metabolism (*Mol Biol Evol*, 34:509–24, 2017). And maybe the strongest suggestion of beneficial Denisovan introgression comes from a 2014 study in which researchers linked the archaic sequences with high altitude adaptation among populations that live in the Tibetan highlands (*Nature*, 512:194–97, 2014). The particular variant they focused on was so highly selected, notes Kelso, that "almost everyone living on the plateau carries this piece of Denisovan DNA."

Neanderthal-derived immunity

Another area of human biology tightly linked to Neanderthal variants in the genome is the immune system. Given that human ancestors were exposed to a menagerie of different pathogens —some of which came directly from the Neanderthals—as they migrated through Eurasia, the Neanderthal sequences introgressed into the human genome may have helped defend against these threats, to which Neanderthals had long been exposed.

"Viral challenges, bacterial challenges are among the strongest selective forces out there," says Kelso. Unlike changes in other environmental conditions such as daylight patterns and UV exposure, "pathogens can kill you in one generation."

Hints of archaic DNA's role in immune function surfaced as early as 2011, as soon as the Neanderthal genome was available for cross-referencing with sequences from modern humans. A team led by researchers at Stanford University found that certain human leukocyte antigen (HLA) alleles, key players in pathogen recognition, held signs of archaic ancestry—from Neanderthals, but also from another hominin cousin, the Denisovans.[6] "It's a cool paper and one that contributed to a lot of people thinking about the effects of introgression," says Capra.

Several other studies since then have strengthened the link between archaic DNA and immune function, branching out from the HLA system to include numerous other pathways.[7] For example, multiple labs have tied Neanderthal variants to altered expression levels of genes encoding toll-like receptors (TLRs), key players in innate immune responses. In 2016, Kelso, Dannemann, and a colleague found that pathogen response and susceptibility to develop allergies were associated with Neanderthal sequences that affect TLR production.[8]

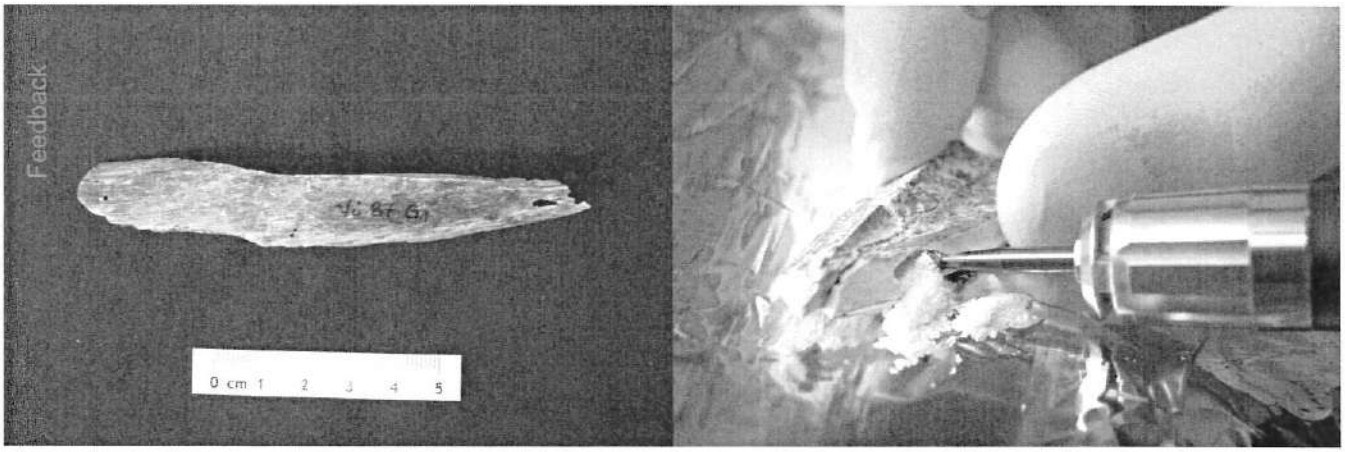
Viruses, in particular, appear to be potent drivers of adaptation. Last year, University of Arizona population geneticist David Enard and colleagues found that one-third of Neanderthal variants under positive selection were linked to genes encoding proteins that interact with viruses.[9]

Researchers have also identified several less-easily explainable phenotypic associations with Neanderthal introgression. In their 2017 analysis, for example, Kelso and Dannemann found that Neanderthal variants were associated with chronotype—whether people identify as early birds or night owls—as well as links with susceptibility to feelings of loneliness or isolation and low enthusiasm or interest. The associations with mood-related phenotypes jibe with what Capra's group had found the year before in its dataset of medical information, which linked Neanderthal variants to risks for depression and addiction. "These were associations that were quite strong," says Capra. "And when we looked at genes where these regions of Neanderthal ancestry fell, in many cases they made sense given what we already know about those genes."

> Viral challenges, bacterial challenges are among the strongest selective forces out there. Pathogens can kill you in one generation.
>
> —Janet Kelso, Max Planck Institute for Evolutionary Anthropology

Why these associations exist is still a mystery. Kelso suspects that light might be a unifying factor, with both changes in day-length patterns and UV exposure reductions as they moved to more-northern latitudes. But that's just a hunch, she emphasizes.

"It's fun speculating about how [Neanderthal introgression] could have been advantageous, or how variants that make us depressed in the modern environment could have been beneficial," says Capra. "I don't really even know what depression meant 40,000 years ago. That's both the challenge and the fun, provocative part about all this."



Left: Bone fragment of a female Neandertal from the Vindija Cave. Right: Drilling of another Neanderthal bone fragment to extract DNA for analysis
M. HAJDINJAK, FRANK VINKEN

A question of functionality

Even with more straightforward associations, such as with skin traits or immune responses, conclusions thus far are drawn from correlations between genotypes and phenotypes. While such

genetic and statistical approaches can conceptually link Neander-thal introgression with phenotypes and hint at why such sequences may have been selected for in humans' early history, researchers have not yet published in vitro validation studies.

"Studying Neanderthal DNA more closely on a molecular level in the lab is pretty tricky," says Dannemann. Neanderthal variants tend to come in packages, and the linkage between the variants makes it difficult to identify the function of each one, he explains.

That challenge hasn't stopped researchers from trying. As a postdoc in Pääbo's lab in Germany, Camp, along with Vernot, Kelso, and Dannemann, established a handful of brain organoids from induced pluripotent stem cell lines of modern Europeans who vary in their Neanderthal-derived genetics, and tracked single-cell transcriptomes as the cultured cells matured. The early data suggest that the Neanderthal variants affect gene expression in the same way as documented by previous work, validating the model.

See "Minibrains May Soon Include Neanderthal DNA"

But such research is still in the proof-of-principle stage, says Camp, who is continuing this work in his own lab in Switzerland. "Now you just need to increase throughput. You need to do this for 100 or 200 individuals." Even then, he adds, the conclusions researchers will be able to draw will be limited. "I am a bit cautious and maybe pessimistic [about whether] you can really identify . . . impacts [of Neanderthal variants] on some physiological outcomes."

There are other fundamental questions that are proving difficult to answer about Neanderthal introgression, says Akey, from the number of hybridization events to the timescale over which those events took place, and whether there was sex bias in patterns of gene flow. "There are all these important things that are really hard to estimate," he says. "I think the field is kind of stuck right now." But he's hopeful that as more genomes from various archaic hominin groups and from modern humans come online, researchers' power to model how all of these groups interbred will strengthen. A second high-quality Neanderthal genome was published in 2017 (*Science*, 358:655–58), and researchers now have the genome of a 40,000-year-old human who had a Neanderthal ancestor just a few generations back. Last year, researchers published the sequence of a first-generation hybrid of Denisovans and Neanderthals.

See "Girl Had a Denisovan Dad and Neanderthal Mom"

Those data will likely yield some surprises. Capra has found evidence, for example, that some of the Neanderthal segments that correlated with modern phenotypes may not affect those phenotypes directly. His work has uncovered cases in which the correlation was driven by sequences close enough in the genome to Neanderthal variants that the two always appear together. These sequences were carried by the common ancestor of Neanderthals and modern humans but were missing from the group of humans who founded the modern Eurasian population. These variants,

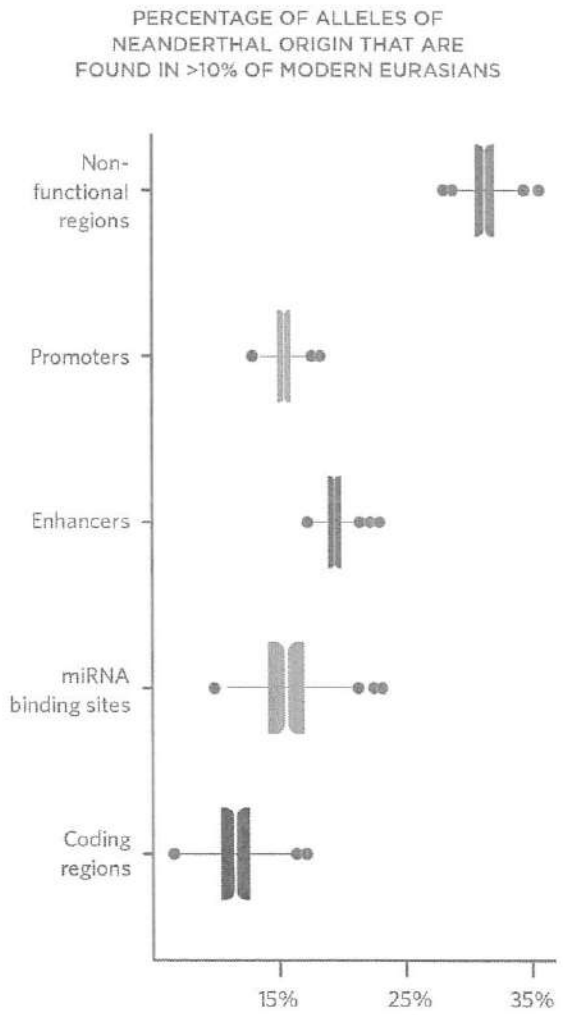
which had been retained by Neanderthals, were then reintroduced to the ancestors of modern non-Africans during periods of interbreeding.[10] "These genetic variants existed in modern [Eurasians only] in the Neanderthal context, but these were not of Neanderthal ancestry," Capra says.

Akey has come upon another interesting twist: Africans do have Neanderthal ancestry. Unpublished work from his group points to the possibility that some of the ancient modern humans that bred with Neanderthals migrated back to Africa, where they mixed with the modern humans there, sharing bits of Neanderthal DNA. If true, that would mean that Africa is not devoid of Neanderthals' genetic influence, Akey notes. "There's Neanderthal basically all over the world."

All About Regulation

In their seminal 2014 studies, the groups of David Reich of Harvard Medical School and Joshua Akey, then at the University of Washington, noted that the Neanderthal variants that correlated with human phenotypes did not appear in coding regions. Two years later, a genome-wide analysis published by investigators in France found that Neanderthal ancestry was enriched in areas tied to gene regulation (*Cell*, 167:643–56.e17, 2016). The implication was that sequences that originated in Neanderthals tend to have "less impact through protein and more impact through gene expression," says coauthor Maxime Rotival, a geneticist at the Pasteur Institute in Paris.

To ask this question more directly, Akey turned to the Genotype-Tissue Expression (GTEx) Project, which has cataloged gene expression data from roughly 50 tissues for each of 10,000 individuals. "It's this really fine-scale record of gene expression," says Akey. His then-postdoc Rajiv McCoy, now an assistant professor at Johns Hopkins University, developed a method to assess messenger RNA levels based on which



ANCESTRAL ANALYSIS: Sequences of Neanderthal origin in people of Eurasian descent are more common in nonfunctional and regulatory regions of the genome than in coding regions.

allele was being expressed—the one from an individual's father or mother—and the researchers applied this approach to people in the GTEx database who were heterozygous for a particular Neanderthal variant. Comparing expression levels based on which allele was being expressed, the researchers found that a quarter of the stretches of Neanderthal DNA in human genomes affect the regulation of the genes in or near those stretches (*Cell*, 168:P916–27.E12, 2017).

"We've known for a long time that gene expression variation is an important source of phenotypic variation within populations and phenotypic divergence between species," says Akey. "We were interested in asking whether Neanderthal sequences make any contribution to gene expression variability." The answer was a resounding yes.

Earlier this year, Rotival and two colleagues calculated ratios of Neanderthal to non-Neanderthal variants across the genome and compared those ratios for protein-coding regions and various regulatory sequences, specifically enhancers, promoters, and microRNA-binding sites. Consistent with previous results, they found a strong depletion of Neanderthal variants in coding portions of genes, and a slight enrichment of the archaic sequences in regulatory regions (*Am J Hum Genet*, doi:10.1016/j.ajhg.2019.04.016, 2019). "What we see is that in coding regions, the ratio of archaic to non-archaic variants is much smaller than the ratio outside of coding regions," says Rotival.

"This is not at all a surprise," says Vanderbilt University's Tony Capra, whose lab has generated similar findings in people of Eurasian descent, "but it's really nice to see it quantified very comprehensively."

References

1. R.E. Green et al., "A draft sequence of the Neandertal genome," *Science*, 328:710–22, 2010.
2. B. Vernot, J. Akey, "Resurrecting surviving Neandertal lineages from modern human genomes," *Science*, 343:1017–21, 2014.
3. S. Sankararaman et al., "The genomic landscape of Neanderthal ancestry in present-day humans," *Nature*, 507:354–57, 2014.
4. C.N. Simonti et al., "The phenotypic legacy of admixture between modern humans and Neandertals," *Science*, 351:737–41, 2016.
5. M. Dannemann, J. Kelso, "The contribution of Neanderthals to phenotypic variation in modern humans," *Am J Hum Genet*, 101:P578–89, 2017.
6. L. Abi-Rached et al., "The shaping of modern human immune systems by multiregional admixture with archaic humans," *Science*, 334:89–94, 2011.

7. H. Quach et al., "Genetic adaptation and Neandertal admixture shaped the immune system of human populations," *Cell*, 167:643–56.e17, 2016.
8. M. Dannemann et al., "Introgression of Neandertal- and Denisovan-like haplotypes contributes to adaptive variation in human toll-like receptors," *Am J Hum Genet*, 98:P22–33, 2016.
9. D. Enard and D.A. Petrov, "Evidence that RNA viruses drove adaptive introgression between Neanderthals and modern humans," *Cell*, 175:P360–71.E13, 2018.
10. D.C. Rinker et al., "Neanderthal introgression reintroduced functional alleles lost in the human out of Africa bottleneck," *bioRxiv*, doi:10.1101/533257, 2019.

Jef Akst is the managing editor of The Scientist. Email her at jakst@the-scientist.com.

Clarification (September 26): This story has been updated to change mentions of "non-African" descent or ancestry to "Eurasian" to avoid confusion. All modern humans have ancestry in Africa. The Scientist *regrets any confusion.*

Keywords:

evolution, evolutionary biology, genetics, genetics & genomics, genomics, hominin, hominin evolution, hominins, human evolution

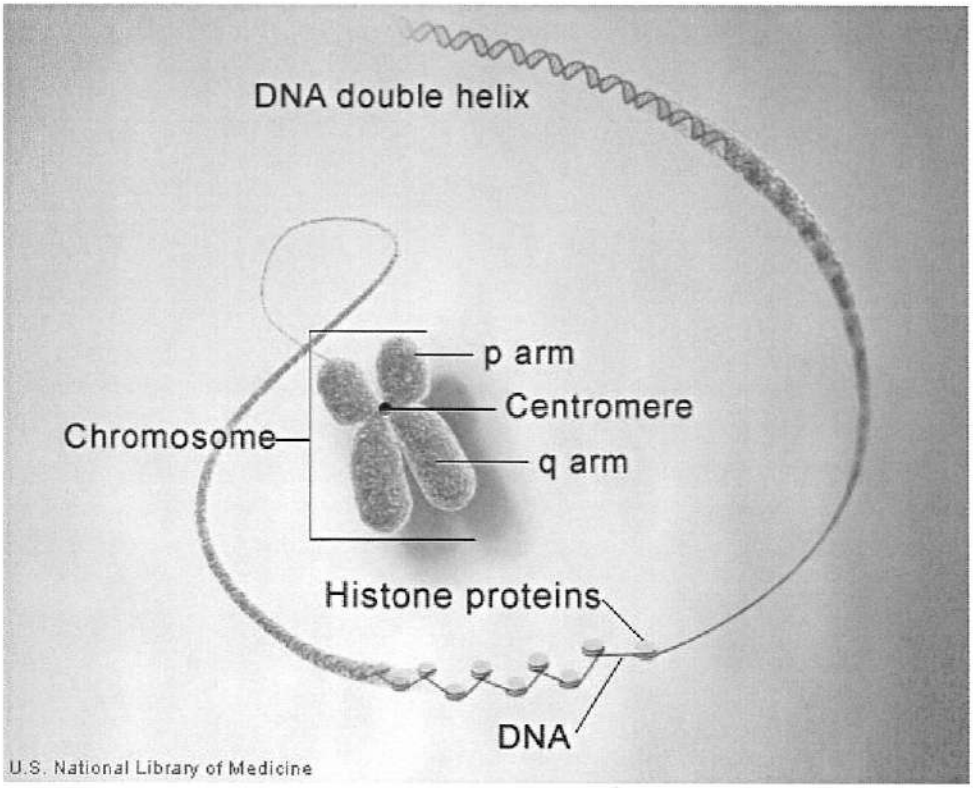
What is a chromosome?

In the nucleus of each cell, the DNA molecule is packaged into thread-like structures called chromosomes. Each chromosome is made up of DNA tightly coiled many times around proteins called histones that support its structure.

Chromosomes are not visible in the cell's nucleus—not even under a microscope—when the cell is not dividing. However, the DNA that makes up chromosomes becomes more tightly packed during cell division and is then visible under a microscope. Most of what researchers know about chromosomes was learned by observing chromosomes during cell division.

Each chromosome has a constriction point called the centromere, which divides the chromosome into two sections, or "arms." The short arm of the chromosome is labeled the "p arm." The long arm of the chromosome is labeled the "q arm." The location of the centromere on each chromosome gives the chromosome its characteristic shape, and can be used to help describe the location of specific genes.

DNA and histone proteins are packaged into structures called chromosomes.



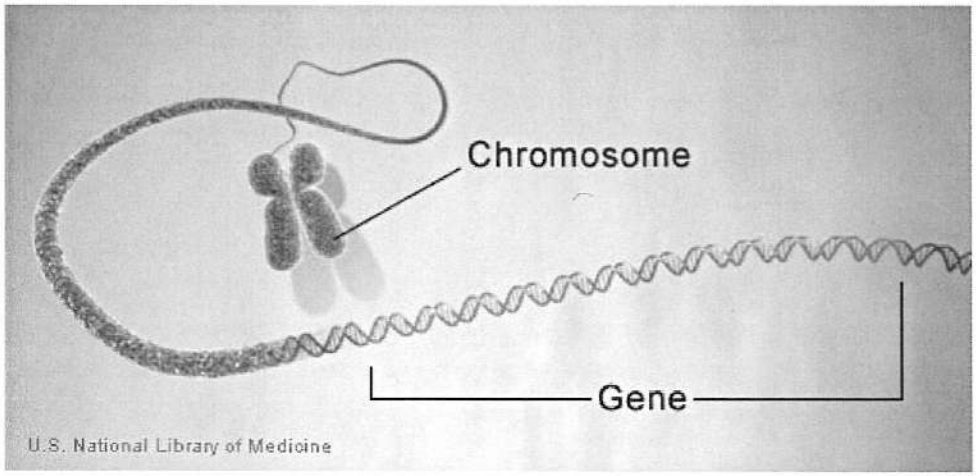
What is a gene?

A gene is the basic physical and functional unit of heredity. Genes are made up of DNA. Some genes act as instructions to make molecules called proteins. However, many genes do not code for proteins. In humans, genes vary in size from a few hundred DNA bases to more than 2 million bases. The Human Genome Project estimated that humans have between 20,000 and 25,000 genes.

Every person has two copies of each gene, one inherited from each parent. Most genes are the same in all people, but a small number of genes (less than 1 percent of the total) are slightly different between people. Alleles are forms of the same gene with small differences in their sequence of DNA bases. These small differences contribute to each person's unique physical features.

Scientists keep track of genes by giving them unique names. Because gene names can be long, genes are also assigned symbols, which are short combinations of letters (and sometimes numbers) that represent an abbreviated version of the gene name. For example, a gene on chromosome 7 that has been associated with cystic fibrosis is called the cystic fibrosis transmembrane conductance regulator; its symbol is *CFTR*.

Genes are made up of DNA. Each chromosome contains many genes.



Credit: U.S. National Library of Medicine

For more information about genes:

U.S. NATIONAL LIBRARY OF MEDICINE

Genetics Home Reference

Your Guide to Understanding Genetic Conditions

What is noncoding DNA?

Only about 1 percent of DNA is made up of protein-coding genes; the other 99 percent is noncoding. Noncoding DNA does not provide instructions for making proteins. Scientists once thought noncoding DNA was "junk," with no known purpose. However, it is becoming clear that at least some of it is integral to the function of cells, particularly the control of gene activity. For example, noncoding DNA contains sequences that act as regulatory elements, determining when and where genes are turned on and off. Such elements provide sites for specialized proteins (called transcription factors) to attach (bind) and either activate or repress the process by which the information from genes is turned into proteins (transcription). Noncoding DNA contains many types of regulatory elements:

- Promoters provide binding sites for the protein machinery that carries out transcription. Promoters are typically found just ahead of the gene on the DNA strand.
- Enhancers provide binding sites for proteins that help activate transcription. Enhancers can be found on the DNA strand before or after the gene they control, sometimes far away.
- Silencers provide binding sites for proteins that repress transcription. Like enhancers, silencers can be found before or after the gene they control and can be some distance away on the DNA strand.
- Insulators provide binding sites for proteins that control transcription in a number of ways. Some prevent enhancers from aiding in transcription (enhancer-blocker insulators). Others prevent structural changes in the DNA that repress gene activity (barrier insulators). Some insulators can function as both an enhancer blocker and a barrier.

Other regions of noncoding DNA provide instructions for the formation of certain kinds of RNA molecules. RNA is a chemical cousin of DNA. Examples of specialized RNA molecules produced from noncoding DNA include transfer RNAs (tRNAs) and ribosomal RNAs (rRNAs), which help assemble protein building blocks (amino acids) into a chain that forms a protein; microRNAs (miRNAs), which are short lengths of RNA that block the process of protein production; and long noncoding RNAs (lncRNAs), which are longer lengths of RNA that have diverse roles in regulating gene activity.

Some structural elements of chromosomes are also part of noncoding DNA. For example, repeated noncoding DNA sequences at the ends of chromosomes form telomeres. Telomeres protect the ends of chromosomes from being degraded during the copying of genetic material. Repetitive noncoding DNA sequences also form satellite DNA, which is a part of other structural elements. Satellite DNA is the basis of the centromere, which is the constriction point of the X-shaped chromosome pair. Satellite DNA also forms heterochromatin, which is densely packed DNA that is important for controlling gene activity and maintaining the structure of chromosomes.

Some noncoding DNA regions, called introns, are located within protein-coding genes but are removed before a protein is made. Regulatory elements, such as enhancers, can be located in introns. Other noncoding regions are found between genes and are known as intergenic regions.

The identity of regulatory elements and other functional regions in noncoding DNA is not completely understood. Researchers are working to understand the location and role of these genetic components.

Scientific journal articles for further reading

Maston GA, Evans SK, Green MR. Transcriptional regulatory elements in the human genome. Annu Rev Genomics Hum Genet. 2006;7:29-59. Review. PubMed: 16719718.

ENCODE Project Consortium. An integrated encyclopedia of DNA elements in the human genome. Nature. 2012 Sep 6;489(7414):57-74. doi: 10.1038/nature11247. PubMed: 22955616; Free full text available from PubMed Central: PMC3439153.

Plank JL, Dean A. Enhancer function: mechanistic and genome-wide insights come together. Mol Cell. 2014 Jul 3;55(1):5-14. doi: 10.1016/j.molcel.2014.06.015. Review. PubMed: 24996062.

For more information about noncoding DNA:

Cold Spring Harbor Laboratory DNA Learning Center: The Human Genome: Genes and Non-coding DNA, 3D Animation with Basic Narration

University of Leicester Virtual Genetics Education Centre: Gene Expression and Regulation

Georgia Tech Biology: Gene Regulation

National Academies Press: Noncoding DNA—Subtlety, Punctuation, or Just Plain Junk?

Khan Academy: Transcription Factors

The Cell: A Molecular Approach (second edition, 2000): Regulation of Transcription in Eukaryotes

Genetic Science Learning Center, University of Utah: RNA's Role in the Central Dogma, Telomeres, and Centromeres

Topics in the Cells and DNA chapter

- What is a cell?
- What is DNA?
- What is a gene?
- What is a chromosome?
- How many chromosomes do people have?
- What is noncoding DNA?

Other chapters in Help Me Understand Genetics

Published: **January 7, 2020**

Rousseau v. Coates, 071719 VTDC, 2:18-cv-205

CHERYL ROUSSEAU and PETER ROUSSEAU, Plaintiffs,

v.

JOHN BOYD COATES, III, M.D., and CENTRAL VERMONT MEDICAL CENTER, INC., Defendants.

No. 2:18-cv-205

United States District Court, D. Vermont

July 17, 2019

RULING ON MOTION TO COMPEL A RULE 35 BUCCAL SWAB

William K. Sessions III District Court Judge

Plaintiffs Cheryl and Peter Rousseau move the Court to compel Defendant John Boyd Coates, III, M.D. to submit to a buccal swab of the inside of his cheek for the purpose of obtaining his DNA. The Rousseaus allege that in 1977, Dr. Coates wrongfully and fraudulently inseminated Cheryl Rousseau with his own genetic material. A buccal swab, they contend, will help to establish that Dr. Coates is the biological father of their adult daughter. Dr. Coates denies paternity. For the reasons set forth below, the Rousseaus' motion is **granted**.

Under Federal Rule of Civil Procedure 35(a), a court "may order a party whose mental or physical condition . . . is in controversy to submit to a physical or mental examination by a suitably licensed examiner" upon a showing of good cause. Fed.R.Civ.P. 35(a). Accordingly, an order requiring an examination under Rule 35 may be issued only when (1) the mental or physical condition of the party is "in controversy, " and (2) good cause supports the order. *Schlagenhauf v. Holder*, 379 U.S. 104, 118-19 (1964). "Controversy" and "good cause" may be established by the pleadings. *Id.* Granting or denying a motion for a physical examination "rests in the sound discretion of the trial court." *Coca-Cola Bottling Co. of Puerto Rico v. Negron Torres*, 255 F.2d 149, 153 (1st Cir. 1958).

A party's mental or physical condition is "in controversy" when that condition is the subject of the litigation. *See Ashby v. Mortimer*, 329 F.R.D. 650, 653 (D. Idaho 2019). Good cause "depends on both relevance and need." *Pearson v. Norfolk-Southern Ry., Co., Inc.*, 178 F.R.D. 580, 582 (M.D. Ala. 1998) (citations omitted). To determine need, "the court must examine the ability of the movant to obtain the desired information by other means." *Ashby*, 329 F.R.D. at 653 (citations omitted).

In this case, initial DNA testing reportedly indicates that Dr. Coates is the biological father of the Rousseaus' daughter. As this suit is predicated upon the claim that Dr. Coates did not impregnate Cheryl Rousseau as promised, his biological relationship to the Rousseaus' daughter is very much at issue. The Rousseaus have therefore satisfied the "in controversy" requirement. *See, e.g., Ashby*, 329 F.R.D. at 654 (concluding that the "in controversy" requirement was

satisfied where "[t]he very core" of the defendant doctor's defense to a claim of fraudulent insemination through use of "his own sperm--requires an analysis of his DNA").

The Court further finds that the Rousseaus have shown good cause for a swab test. At oral argument, the Rousseaus' counsel informed the court that initial DNA-related information was accessed by means of a service or services such as Ancestry.com or 23andMe.com. Such services may be subject to "a variety of attacks" on reliability, including questions about chain of custody, testing methods, and error rates. *Id.* at 655. Legally conclusive evidence is therefore unavailable, and as Dr. Coates denies paternity, there is good cause for further testing. *See D'Angelo v. Potter*, 224 F.R.D. 300, 304 (D. Mass. 2004) (finding good cause to order a DNA examination where plaintiff lacked alternative methods for proving her allegations).

Dr. Coates contends that the law concerning DNA testing in the civil context is undeveloped, and that the Court should not allow such testing under Rule 35. As the Rousseaus' point out, however, Rule 35 has long been used as a vehicle for scientific testing relevant to the question of paternity. *See, e.g., Beach v. Beach*, 114 F.2d 479, 482 (D.C. Cir. 1940). Dr. Coates also submits that such testing should be conducted under the Vermont Parentage Act and overseen by a state court. The Vermont Parentage Act codifies a series of protections for genetic testing, including requirements for accreditation (15C V.S.A. § 602), the manner in which the test results are reported (15C V.S.A. § 605), the means of establishing admissibility (15C V.S.A. § 606), the process by which test results may be contested (15C V.S.A. § 607), and provisions for confidentiality (15C V.S.A. § 614). Such protections may be incorporated into this Court's order for testing. The Court therefore **orders** as follows:

(1) The Rousseaus' motion to compel a buccal swab (ECF No. 25) is **granted**;

(2) counsel for the Rousseaus shall prepare a proposed order that includes safeguards such as those provided in the Vermont Parentage Act, as well as the date, place, manner, conditions, and scope of the examination, including the person or persons who will perform it; provide the proposed order to Dr. Coates's counsel for comments and consent; and submit a stipulated proposed order to the Court within 14 days of this Order;

(3) in the event the parties are unable to agree on a stipulated proposed order, they shall each submit proposed orders to the Court within 21 days of this Order.

Program Agenda

CYBER-PRIVACY AND THE INTERNET

Theodore Roosevelt Inn of Court
February 3, 2020

Introduction of Participants by Elizabeth Schlissel	5:30 - 5:35
Introduction to Data Privacy Issues by Thomas O'Rourke	5:35 - 5:45
Personal Data – What is out there and who wants it by all program participants	5:45 – 6:00
Facial Recognition Technology bye all program participants	6:00 – 6:15
Privacy Policies of Apps that collect your Data by all program participants	6:15 – 6:30
DNA Privacy Issues by all program participants	6:30 – 6:50
Attorney Ethical Obligations Regarding Data Privacy by all program participants	6:50 – 7:20
Summary of Data-Privacy Issues by Andrew Thaler	7:20 - 7:30