THE FOURTH AMENDMENT
&
STATE CONSTITUTION SEARCH AND SEIZURE PROVISIONS

CAN THEY ADAPT TO MODERN TECHNOLOGIES?[1]

[1] Adapted from materials prepared by Richard Guerriero, Esq. Lothstein Guerriero, PLLC

HOW MUCH PROTECTION DOES THE FOURTH AMENDMENT PROVIDE FOR CELL PHONES AND INTERNET USERS?

A Quick Review of the Warrant Requirement.

Part I, Article 19 of the New Hampshire Constitution, and the Fourth Amendment of the United States Constitution, require that search warrants be issued only upon a finding of probable cause. *State v. Letoile*, 166 N.H. 269, 272-73 (2014); *State v. Ball*, 164 N.H. 204, 207 (2012); *State v. Ward*, 163 N.H. 156, 159 (2012).

Probable cause exists if a person of ordinary caution would justifiably believe that what is sought will be found through the search and will aid in a particular apprehension or conviction. *Id.* "The police must demonstrate in an application for a search warrant that there is a substantial likelihood that the items sought will be found in the place to be searched." *State v. Fish*, 142 N.H. 524, 527-28, 703 A.2d 1377 (1994). "The task of the issuing district court is to 'make a practical, common-sense decision whether given all the circumstances set forth in the affidavit before [it], including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, (1983); *see State v. Fish*, 142 N.H. 524, 528 (1997).

GPS Tracking of Vehicles (and the people in them).

In *United States v. Jones*, 132 S. Ct. 945 (2012), the Court ruled that 28 days of GPS tracking of a vehicle required a warrant. This case illustrates the tension between two theories of the Fourth Amendment:

- the "property rights" theory that focuses on formal infringements of property rights such as a physical trespass. This doctrine is associated with more conservative jurists.
- The more modern "reasonable expectation of privacy" doctrine which examines the current values and customs of our society to determine whether the person had a reasonable expectation of privacy in the place searched, even

The Contents of a Cell Phone Are Protected by the Warrant Requirement.

The question of whether a warrant is necessary to search a cellphone was answered clearly and definitively in *Riley v. California*, 134 S. Ct. 2473 (2014). Justice Roberts wrote: "Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple - get a warrant…" *Id.* at 2495. (*Riley* discussed in greater detail below.)

It's Not All or Nothing – The Particularity Requirement Applies.

Part I, Article 19 of the New Hampshire Constitution, and the Fourth Amendment of the United States Constitution, prohibit general warrants. *State v. Fitanides*, 131N.H. 298, 300 (1988); *see also State v. Teletypewriter Mach.*, 97 N.H. 282 (1952). As explained by the United States Supreme Court, the Fourth Amendment provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." (Emphasis supplied.)

These words are precise and clear. They reflect the determination of those who wrote the Bill of Rights that the people should forever "be secure in their persons, houses, papers, and effects" from intrusion and seizure by officers acting under the unbridled authority of a general warrant. *Stanford v. Texas*, 379 U.S. 476, 481 (1965).

By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit. *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).

Pursuant to the constitutional requirement of particularity, a warrant "(1) must supply enough information to guide and control the executing agent's judgment in selecting where to search and what to seize, and (2) cannot be too broad in the sense that it includes items that should not be seized." *United States v. Kuc*, 737 F.3d 129, 133 (1st Cir. 2013).

Even though they pre-date cellphones, two cases from the First Circuit are instructive: *United States v. Roche*, 614 F.2d 6 (1st Cir. 1980) and *In re Application of Lafayette Academy, Inc.*, 610 F.2d 1 (1st Cir. 1979). In both cases, the law enforcement agents referred to the investigation of a specific crime but then obtained search warrants for broad classes of records far beyond those which might be associated with the specific crime under investigation. In both cases, the First Circuit Court of Appeals found that the warrants violated the particularity requirement of the Fourth Amendment. *Roche*, 614 F.2d at 7; *Lafayette Academy*, 610 F.2d at 3.

A search warrant for a cell phone that violates the particularity requirement is analogous to an overly broad search warrant for records. The difference is that a cell phone will likely contain more information, and more personal information, than a file cabinet of paper records. This is because of the unique nature of cell phones, as recognized in *Riley*. Although *Riley* is about the necessity of a warrant in the first instance, the findings in *Riley* also support our particularity arguments.

In *Riley*, the Supreme Court identified the special concerns that arise when cell phones are searched by police:

1. Content: cell phones are not mere phones, but are also "minicomputers" which are also used as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."
2. Storage: Cell phones have an immense storage capacity for many different types of files ranging from documents and data to audio and video. *Id.* There is so much information on a cell phone that the "sum of an individual's private life can be reconstructed" from the files on the phone. Id. Lastly, the court noted that "[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." *Id.* at 2490.

Some courts have recognized that search warrants for cell phones must satisfy the constitutional requirement of particularity and cannot simply authorize wholesale rummaging through the phone. For example, in *United States v. Winn*, 79 F. Supp. 3d 904 (S.D. Ill. 2015), the police were investigating a case in which the suspect allegedly used his phone to take photos of young girls in public while exposing himself. The police applied for a warrant for the suspect's phone, but, rather than seeking authority to search for evidence of the photos of the girls, the police used a template which authorized them to search for "any or all files" on the phone. Just as proposed by the State here, after receiving the phone, the police then did a "complete dump" of the phone's contents using Cellebrite, *id.* at 922. Reviewing the conduct of the police and the warrant, the federal district court found that the warrant violated the particularity requirement of the Fourth Amendment. The warrant should have limited the search to photos taken during a particular timeframe and at a particular location. *Id.* at 921. 6 whatsoever to the criminal activity at issue. Simply put, the warrant told the police to take everything, and they did. As such, the warrant was overbroad in every respect and violated the Fourth Amendment. Id, 79 F. Supp. 3d at 922.

Other federal courts have gone even further and required that search warrants for cell phones be accompanied by specific protocols to satisfy the constitutional requirement of particularity. *See, e.g., United States v. Phua*, 2015 U.S. Dist. LEXIS 37301, 2015 WL 1281603, at 7 (D. Nev. Mar. 20, 2015) ("The court will not approve a search warrant for electronically stored information that does not contain an appropriate protocol delineating what procedures will be followed to address these Fourth Amendment issues."); *In re Premises Known as Three Cellphones and One Micro-SD Card*, 2014 U.S. Dist. LEXIS 108470, 2014 WL 3845157, at 2 (D. Kan. Aug. 4, 2014) (requiring the government to submit a search protocol before issuing a warrant); *In re Search of the Premises Known as a Nextel Cellular Telephone*, 2014 U.S. Dist. LEXIS

88215, 2014 WL 2898262, at 12 (D. Kan. June 26, 2014) (ruling that the government's "search protocol" failed to adequately describe with particularity its search methodology); *In re Search of Apple iPhone*, 31 F. Supp. 3d 159, 166-67 (D.D.C. 2014) (describing the need for search protocols when conducting searches of electronic data); *see also In re Application for Search Warrant*, 71 A.3d 1158, 1170 (Vt. 2012), (*ex ante* instructions were sometimes an acceptable mechanism for ensuring the particularity of a search); *see generally* Gershowitz, "The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches," 69 Vand. L. Rev. 585 (2016).

Everyone carries cell phones. Everyone uses them to communicate and plan things, and to memorialize things (photos, notetaking app, etc). So do the police get to search every suspected criminal's cell phone?

The State will argue that, in this day and age, we all know that everyone uses cell phones so that in any case involving two suspects for the same crime, it will be permissible to search their cell phones to see if they talked about the crime. The law is evolving in this area.

In *Commonwealth v. White*, 59 N.E.2d 369, 375 (Mass. 2016), the Court ruled that the mere fact that the defendant was charged with conspiracy, and he probably used his phone to communicate with his co-conspirators, was not sufficient to seize it without a warrant.

In *White* the police seized the defendant's cell phone "because (a) they had reason to believe that the defendant had participated with others in the commission of a robbery-homicide and (b) their training and experience in cases involving multiple defendants suggested that the device in question was likely to contain evidence relevant to those offenses." *Id.* at 590. The Supreme Judicial Court rejected that information as sufficient to establish probable cause:

> In essence, the Commonwealth is suggesting that there exists a nexus between a suspect's criminal acts and his or her cellular telephone whenever there is probable cause that the suspect was involved in an offense, accompanied by an officer's averment that, given the type of crime under investigation, the device likely would contain evidence. If this were sufficient, however, it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search. *See Riley*, 134 S. Ct. at 2492 (only "inexperienced or unimaginative law enforcement officer … could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone"). We cannot accept such a result, which is inconsistent with our admonition that "individuals have significant privacy interests at stake in their [cellular telephones] and that the probable cause requirement … under both the Fourth

> Amendment … and art. 14 … [must] serve[ ] to protect these interests." [citation omitted].

Id. at 591-92.

A more recent federal case, *United States v. Griffith*, 867 F.3d 1265 (D.C. Cir. 2017), makes the same point. In this case, a warrant authorized police to search for and seize any cell phone or electronic device located inside the defendant's residence. *Id*. at 1268. "The supporting affidavit, however, offered almost no reason to suspect that [the defendant] in fact owned a cell phone, or that any phone or other device containing incriminating information would be found in his apartment." *Id*. The D.C. Circuit Court of Appeals found that "the fact that most people now carry a cell phone was not enough to justify an intrusive search of a place lying at the center of the Fourth Amendment's protections--a home--for any phone [the defendant] might own." *Id*.

Location Data Is Protected.

This summer, the United States Supreme Court held, in *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018), that, whether the Government employs its own surveillance technology or uses the technology and information from a wireless carrier, an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through cell service location information. Thus, a warrant is generally required when the government seeks such information from the carrier.

However, the Court made clear that its decision was 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 [the] *Smith* and *Miller* [cases] 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."

Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

Once the State has that information legally, our Supreme Court's ruling in *State v. DePaula*, 170 N.H. 139, 154-55 (2017) explains how the information can be introduced at trial:

> Given the cell phone records custodians' specialized training and experience interpreting cell phone records, we hold that the custodians could testify as lay witnesses because they possessed sufficient personal knowledge to discuss generally the means by which cell phones connect to the closest cell tower and the general ranges of cell towers. See Kale, 445 F. App'x at 485-86. Moreover, we agree with the trial court's conclusion that the ubiquity of cell phones and cell towers in society allows the average juror to understand the elementary concepts underlying the interactions between cell phones and cell towers. Such understanding is qualitatively different from understanding the scientific and neurological mechanisms of the effects of alcohol on the nervous system referred to in *Cochrane*, which are wholly beyond the ken of the average juror."

The State will have to show compliance with Rule of Evidence 803(6). See generally, *State v. Peters*, 162 N.H. 30 (2011); *State v. Howe*, 159 N.H. 366 (2009); *State v. Wall*, 154 N.H. 237 (2006).

Subscriber Information Is Not Protected, At Least Not Yet.

"Pen Register." Use of a device to record the numbers called from a telephone does not constitute a search does not constitute a search under Part I, Article 19 of the State Constitution. *State v. Valenzuela*, 130 N.H. 175, 189, 536 A.2d 1252 (1987), cert. denied, 485 U.S. 1008, 108 S. Ct. 1474, 99 L. Ed. 2d 703 (1988)

Billing Information for Cell Phone Calls. A defendant does not have a reasonable expectation of privacy in information concerning his cellular telephone calls that was recorded for billing purposes and retained by U.S. Cellular in the ordinary course of its business. *State v. Gubitosi*, 152 N.H. 673, 677-78 (2005)

Internet Service Provider Information. A defendant did not have a reasonable expectation of privacy under U.S. Const. amend. IV and N.H. Const. pt. I, art. 19 in subscriber information voluntarily provided to an Internet service provider. *State v. Mello*, 162 N.H. 115, 120 (2011). The court distinguished subscriber information from the content of communications. *Mello*, 162 N.H. at 122.

Use of Advanced Technology by Law Enforcement

The use of advanced technologies by law enforcement to conduct searches in ways never before possible also pose a challenge to courts trying to apply the Fourth Amendment and state constitutional provisions.

Thermal Imaging Devices

In *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001), the Court held that an agent's use of a thermal imaging device, while seated in a car on a public street to scan the interior of home to detect high-intensity lamps consistent with marijuana grow, was a "search" and was presumptively unreasonable without a warrant.

The case presented a challenge for traditional Fourth Amendment "property rights" analysis because the imaging device did not actually trespass into the person's private home.

The case also presented a challenge for modern "reasonable expectation of privacy" doctrine analysis because the device showed only amorphous heat patterns, not a detailed image of the contents of the home.

"Stingray" Cell Tower Simulators

A "*Stingray*" (manufacturer's trade name) is a $100,000.00 mobile device used by law enforcement that simulates a cellular tower. It emits a radio signal that penetrates the walls of homes and buildings. The signal activates cell phones and tricks them into thinking they are communicating with a cellular tower. The phones then send a signal back to the cell site simulator, revealing to police critical information: the phone number, the phone's serial number, and the precise location of the phone inside the building.

Under the direction of the FBI, some law enforcement agencies and officers refuse to disclose the use of Stingray devices, and have refused to answer questions about the technology, even at the risk of the dismissal of criminal cases.[2]

Prior to the 2018 *Carpenter* decision discussed above, a few courts held that the use of a Stingray constitutes a search of the cellphone within the Fourth Amendment. *United States v. Ellis*, 270 F. Supp. 3d 1134 (N.D. Cal. 2017); *United States v. Lambis*, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016). (Is it also a search of the home or building? A search of the person holding the phone?)

At least insofar as the government seeks to introduce cell phone location information deduced by the device, after the *Carpenter* decision, there can be no doubt that this is a search that must be supported by a warrant or exception to the warrant requirement. *Carpenter v. United States*, 138 S. Ct. 2206, 2220 (2018).

[2] No, this is not from a "conspiracy theory" fringe website. This is from Matt Richtel, A Police Gadget Tracks Phones? Shhh! It's Secret, N.Y. Times (March 15, 2015).

Law Enforcement Hacking and Implantation of Malware (Virus) Software into Civilian Computers

In February and March 2015, the FBI became the world's largest distributor of child pornography on the internet. As part of a global sting operation styled "Operation Pacifier," the FBI seized a website called Playpen that distributed child pornography on the TOR network that is designed to protect user anonymity. The government transferred the Playpen site to a government server in Virginia, and then obtained a warrant to intentionally infect user computers with malware. The malware, called a "NIT" (Network Investigative Technique) allowed the government to determine the identity of user computers accessing the site. The government then became a worldwide purveyor of child pornography, and over the course of two weeks, gathered the IP addresses of over 9000 computers that accessed Playpen, from over 100 countries. *United States v. Tippens*, No. 3:16-cr-05110-RJB, 2016 U.S. Dist. LEXIS 184174 (W.D. Wash. Nov. 30, 2016).

The court in *Tippens* held that the warrant obtained by the government to engage in this conduct was supported by probable cause. The court further held that to the extent that the NIT Warrant authorized the search of computers outside of the Eastern District of Virginia, the NIT Warrant violated" the United States Magistrates Act, 28 U.S.C. § 636(a), and violated Fed. R. Crim. P. 41(b)(1), which both limit the judicial power of federal judges outside of their judicial district. However, based on the good faith exception to the Fourth Amendment, the Court declined to suppress the evidence obtained in violation of the statute and rule of criminal procedure.

Although not a search and seizure issue, another part of the decision is more interesting – the analysis of whether the indictment should be dismissed for outrageous governmental misconduct. The Court began its analysis by stating that "[i]t is easy to conclude that the Government acted outrageously here…" by illegally distributing child pornography in violation of United States criminal statutes, using child victims as "bait" and "revictimizing" them without informing their families, much less seeking their permission, conduct that raised the prosecuting lawyers "in jeopardy of violating ABA Model Rules of Professional Conduct 8.4," and "rais[ing] serious ethical and moral issues for counsel."

However, the Court declined to dismiss the indictment, because the situation did not meet all elements of the rarely applied "dismissal for outrageous governmental conduct" doctrine. "Dismissing an indictment for outrageous conduct . . . is limited to extreme cases in which the defendant can demonstrate that the government's conduct violates fundamental fairness,"

which is "an extremely high standard." *United States v. Black,* 733 F.3d 294, 302 (9th Cir. 2013)