Telephone Technology versus the Fourth Amendment

By Judge Herbert B. Dixon Jr.

The intersection of law and technology is a fascinating study. A notable example of this concerns the seemingly never-ending battle between new and improved telephone capabilities and the extent to which the Fourth Amendment of the U.S. Constitution provides protections to individuals against "unreasonable searches and seizures." Predicting the direction of Fourth Amendment jurisprudence relating to telephones is increasingly difficult because of constant advancements in that technology.

Lest we forget, the Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

As the Fourth Amendment is generally understood, a warrant supported by probable cause is required for government agents to search an individual's person, house, papers, or effects. The validity of a warrantless search of these areas by government agents depends on whether the search was "reasonable" or permitted by a recognized exception to the warrant requirement. A question that frequently arises with each advancement in telephone technology is to what extent have Fourth Amendment protections been lessened. Because the telephone was not invented until nearly 90 years after the Fourth Amendment was proposed and adopted, it does not help to ask how James Madison would have answered the question. Madison died 40 years before the telephone was invented. There should be no dispute of the proposition that Madison never contemplated the effects of telephone technology when he proposed the essence of the Fourth Amendment. When it comes to addressing any Fourth Amendment issue related to the rapid advancements in telephone technology, to ask what the framers intended might be aptly described as a foray into the twilight zone.

Katz v. United States (1967)

A notable case that demonstrates the intersection of telephone technology and the Fourth Amendment is *Katz v. United States*,[1] where law enforcement agents attached an electronic listening and recording device to the outside of the public telephone booth from which Katz placed his calls. The agents did not have a warrant or court order of any sort. The U.S. Supreme Court held that the government's conduct in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and constituted an unlawful "search and seizure" under the Fourth Amendment.

United States v. Miller (1976)

United States v. Miller[2] is a U.S. Supreme Court case that did not involve telephone technology but is often considered when analyzing the impact of telephone technology on Fourth Amendment considerations. *Miller* concerned an investigation into tax fraud where government agents presented subpoenas to the presidents of two banks seeking to obtain Miller's bank account records. Ultimately, the Court held that Miller had no protectable Fourth Amendment interest in the account records because (1) the documents were business records of transactions to which the banks were parties, (2) Miller voluntarily conveyed the information to the banks, and (3) Miller had neither ownership nor possession of the

Judge Herbert B. Dixon Jr. is the technology columnist for *The Judges' Journal*, a member of the ABA Board of Governors, and a former chair of the National Conference of State Trial Judges. He sits on the Superior Court of the District of Columbia. He can be reached at Herbert.Dixon@dcsc.gov. Follow Judge Dixon on Twitter@Jhbdixon.

Published in The Judges' Journal, Volume 55, Number 2, Spring 2016. © 2016 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

papers and the records as they were the business records of the banks that Miller voluntarily conveyed. The Supreme Court noted that the Fourth Amendment does not prohibit government authorities from requesting and obtaining information entrusted to a third party, even if the defendant provided the information to the third party on the assumption it would be used only for a limited purpose.

Smith v. Maryland (1979)

The 1976 *Miller* decision had a notable impact in the telephone technology case of *Smith v. Maryland*.[3] There, the victim of a robbery began receiving threatening and obscene phone calls from a man identifying himself as the robber. Based on information provided by the victim, investigators identified Smith as a suspect. Next, at the request of the law enforcement investigators, the telephone company installed a pen register at its central office to record numbers dialed from Smith's home. Ultimately, the Supreme Court ruled that the installation of a pen register by the telephone company at the request of government agents is not a search under the Fourth Amendment. Relying on the third-party doctrine recognized in *Miller*, the Court noted that when Smith voluntarily conveyed numerical information to the phone company and exposed that information to its equipment in the normal course of business, he assumed the risk that the telephone company would reveal the information to the police.

A pen register, the Court noted, differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications. When Smith used his phone, he voluntarily conveyed numerical information to the telephone company. The switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.

United States v. Jones (2012)

In *United States v. Jones*,[4] government agents obtained a search warrant permitting installation of a global positioning system (GPS) tracking device on a vehicle registered to Jones's wife. The warrant authorized installation of the device in the District of Columbia within 10 days; however, the agents violated the warrant by not installing the GPS unit until the 11th day and installed the device when the vehicle was in Maryland. The government tracked the vehicle's movements for 28 days and used that evidence to secure a conviction on drug trafficking conspiracy charges. The D.C. Circuit reversed, concluding that admission of the evidence obtained by warrantless use of the GPS device violated the Fourth Amendment. The Supreme Court affirmed the Circuit Court's reversal; however, the justices provided different reasons why they deemed GPS tracking unconstitutional and the constitutional distinction, if any, that exists between long-term and short-term GPS surveillance. The concurring opinion of Justice Sonia Sotomayor in *Jones* is frequently cited in cases analyzing the extent to which Fourth Amendment protections are eroded by advancements in telephone technology.

Riley v. California (2014)

Telephone technology again tested the extent of Fourth Amendment protections in *Riley v. California*,[5] where the Supreme Court considered whether the 41-year-old search-incident-to-arrest exception to the warrant requirement[6] applied to the contents of a cell phone in the possession of an arrestee. Although the Supreme Court agreed that a mechanical application of the search-incident-to-arrest principle might well support such a warrantless search, the Court unanimously rejected that argument because cell phones are based on technology nearly inconceivable since the search-incident-to-arrest principle was established. Before cell phones, a search of a person was limited by physical realities and constituted only a narrow intrusion on privacy. However, cell phones can store millions of pages of text, thousands of pictures, or hundreds of videos that can date back for years. To say that a search of cell phone data is "materially indistinguishable" from a search of physical items is akin to saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse found in the possession of an arrestee.

It is no exaggeration to say that many of the over 90 percent 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. Allowing the police to scrutinize such records on a routine basis differs greatly from allowing them to search a personal item or two in the occasional case.

Citing its 2012 decision in *Jones*, the Court noted that data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smartphones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Cell Phones and Cell Site Location Information

Another recurring Fourth Amendment issue is whether government agents must obtain a warrant to request cell site location information (CSLI) related to a particular cell phone. Several states have either established judicial precedent recognizing a reasonable expectation of privacy in CSLI, enacted statutes that require law enforcement to apply for a search warrant to obtain these data, or passed laws requiring police to obtain a search warrant to track a cell phone in real time.[7] The federal circuits are struggling with this issue, as demonstrated by the cases of *United States v. Graham*,[8] *United States v. Davis*,[9] and *In re Application for Telephone Information Needed for a Criminal Investigation*.[10] These cases involve requests by government agents to cell phone service providers for CSLI pursuant to a court order and not pursuant to a warrant supported by probable cause. There is no disagreement that the standard for acquiring a court order to support a request for CSLI is less than the probable cause standard required by a warrant.

Published in The Judges' Journal, Volume 55, Number 2, Spring 2016. © 2016 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

In the case of *In re Application for Telephone Information Needed for a Criminal Investigation*, the government appealed to the U.S. district court a magistrate judge's denial of an application for an order authorizing the government to obtain historical CSLI. The magistrate judge concluded that an order was insufficient and that a warrant supported by probable cause was required for the requested information. After a de novo review of the magistrate judge's decision, the district court affirmed the denial. This decision is now pending appeal in the Ninth Circuit.

In *United State v. Graham*, a Fourth Circuit panel determined that the defendants' Fourth Amendment rights were violated when the government obtained CSLI without a warrant supported by probable cause. The panel found a good faith exception in this instance and directed that, in the future, the government must obtain a warrant supported by probable cause. However, on rehearing en banc, the full court held that the government's acquisition of historical CSLI from the defendants' cell phone provider did not violate the Fourth Amendment. The en banc panel reinstated the affirmance of the defendants' convictions and adopted the panel opinion with respect to all issues not addressed in the en banc opinion.

In *United States v. Davis*, the en banc Eleventh Circuit ruled that the government's procurement of a court order for CSLI on a lesser standard than the probable cause standard for a warrant did not violate the defendant's Fourth Amendment rights. First, like the bank customer in *U.S. v. Miller* and the phone customer in *Smith v. Maryland*, Davis could assert neither ownership nor possession of the third party's business records he sought to suppress. Second, the court ruled that Davis had no subjective or objective reasonable expectation of privacy in the cell service provider's records showing the cell tower locations that wirelessly connected his calls at or near the time of various robberies. Finally, the Eleventh Circuit stated that this claim of privacy was not entitled to the protections the Supreme Court found in *Katz*. The Supreme Court denied the defendant's petition for certiorari.

The essence of the reasoning by some courts to require a warrant based on probable cause to obtain CSLI is first a determination that cell phone users possess a reasonable expectation of privacy in the CSLI associated with their cell phones. Second, those courts have determined that the potential exists for extensive location information concerning the device that approaches that of GPS. The location information includes (1) connections via radio waves to an antenna on a cell tower whenever a cell phone makes or receives a call, sends or receives a text message, or sends or receives data; (2) apps that continually run in the background, sending and receiving data without a user having to interact with the cell phone; (3) periodic identification by cell phones, when turned on and not in airplane mode, to the closest cell tower (normally, the tower with the strongest signal) as the cell phone moves throughout its network coverage every seven to nine minutes regardless of whether there is a call, text, or data to or from the device; (4) the proliferation of small base stations covering specific areas that provide location information tantamount to knowing a phone's location to within an area amounting to individual floors and rooms within buildings; (5) the collection of CSLI by numerous carriers to which there is no subscription when a cell phone travels outside of its own network (e.g., roaming); and (6) compared to GPS tracking, the generation of far more location data because cell phones typically accompany the user everywhere (including, with some folks, to the shower).

Another Telephone Technology Advance—the Cell Site Simulator

While these issues are playing out, there is another emerging telephone technology generically known as cell simulation technology or devices known as a Stingray, triggerfish, swamp box, or some other product name. According to news reports[11] and court decisions,[12] these devices can simulate a cell phone tower and trick nearby cell phones to connect with the simulator. Some reports say that the simulator does not discriminate among nearby cell phones and can collect location information; cell phone identification information; incoming and outgoing call, text, and data information; and even the content of communications. The U.S. Department of Justice has issued policy guidance requiring federal law enforcement officials to get a search warrant before using the technology.[13]

Stay tuned, everyone, for a future challenge to Fourth Amendment protections by the next telephone technology advancement. ■

Endnotes

1. 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).

2. 425 U.S. 435, 96 S. Ct. 1619, 48 L. Ed. 2d 71 (1976).

3. 442 U.S. 735, 99 S. Ct. 2577, 61 L. Ed. 2d 220 (1979).

4. 565 U.S. ___ (2012), 132 S.Ct. 945, 181 L.Ed. 2d 911 (2012).

5. 573 U.S. ——, 134 S. Ct. 2473, 189 L. Ed. 2d 430 (2014).

6. United States v. Robinson, 414 U.S. 218, 94 S. Ct. 467, 38 L. Ed. 2d 427 (1973).

7. *Fourth Amendment*, Cybertelecom: Federal Internet Law & Policy: An Educational Project (2016), http://www.cybertelecom.org/security/ecpamobile.htm.

8. Appeal No. 12-4659 (4th Cir., May 31, 2016) (Available at http://www.ca4.uscourts.gov/Opinions/Published/124659A.P.pdf).

9. 785 F.3d 498 (11th Cir. 2015) (en banc).

10. No. 15-XR-90304, 2015 WL 4594558 (N.D. Cal. July 29, 2015) (appeal filed Sept. 3, 2015).

11. Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, Wired.com (Oct. 28, 2015, 3:00 PM), http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm; *US Justice Department Cracks Down on Mobile Phone Surveillance*, TheGuardian (Sept. 4, 2015, 9:32 PM), http://www.theguardian.com/technology/2015/sep/04/us-justice-department-cracks-down-mobile-phone-surveillance.

12. *In re* Application of the United States of Am. for an Order Relating to Telephones Used by (Suppressed), No. 15 M 0021 (N.D. Ill. Nov. 9, 2015), https://assets.documentcloud.org/documents/2512522/stingray-rules.pdf.

13. Press Release, Dep't of Justice, "Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators" (Sept. 3, 2015), http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

Published in The Judges' Journal, Volume 55, Number 2, Spring 2016. © 2016 by the American Bar Association. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.