FEATURE ARTICLE

PRIVACY VS. PUBLIC SAFETY: PROSECUTING AND DEFENDING CRIMINAL CASES IN THE POST-SNOWDEN ERA

Jason M. Weinstein, William L. Drake, and Nicholas P. Silverman*

I. INTRODUCTION

Over the past several years, there have been signs that federal courts at all levels—from magistrates to the Supreme Court—are increasingly struggling with the privacy implications of evidence-gathering in the digital age. Judicial discomfort with certain law enforcement techniques was already simmering well before anyone ever heard of Edward Snowden, but it only intensified after the former

* Jason M. Weinstein is a partner at Steptoe & Johnson LLP specializing in government investigations and enforcement and cybersecurity matters. He previously served as an Assistant U.S. Attorney in the Southern District of New York and the District of Maryland and as a Deputy Assistant Attorney General in the Department of Justice's Criminal Division, where he oversaw the Division's cybercrime and organized crime enforcement programs. William L. Drake is an associate at Steptoe & Johnson LLP in the firm's White Collar Criminal Defense group. His practice focuses on public corruption, fraud, and internal investigations. Nicholas P. Silverman is also an associate at Steptoe & Johnson LLP in the firm's White Collar Criminal Defense group.

NSA contractor leaked classified documents in June 2013 that revealed that the NSA was collecting bulk records regarding Americans' telephone calls from U.S. telecommunications providers pursuant to Section 215 of the USA Patriot Act as well as the content of and other data regarding Internet communications involving targets believed to be overseas from nine major Internet providers under Section 702 of the FISA Amendments Act.[1]

In the wake of Snowden's leaks, there was an explosion in coverage of digital privacy issues in the mainstream media. "Section 215," "FISA Amendments Act," and PRISM quickly became household words. But the reporting quickly spread beyond articles about the intelligence community's collection practices, with prominent media outlets—and even The Colbert Report and The Daily Show—reporting on evidence-collection techniques used by law enforcement. The New York Times and Washington Post wrote about cell phone location tracking.[2] The Wall Street Journal published articles about the use of airplane-mounted devices to track cellphone signals.[3] These reports spoke to, and helped add fuel to, concerns among interest groups and a significant percentage of the public about perceived government abuses of privacy—often without making distinctions between different parts of "the government."[4]

Much discussion of the Snowden leaks has centered on the legal, political, diplomatic, and economic fallout. There have been legal challenges to and bipartisan calls for the end of the Section 215 bulk collection program. Questions have been raised about the role of the congressional oversight committees and the

---

1. *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (London), Jun. 6, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (London), Jun. 7, 2013, http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

2. *See, e.g.*, Ellen Nakashima, *FBI Clarifies Rules on Secretive Cellphone-Tracking Devices*, WASH. POST, May 14, 2015, https://www.washingtonpost.com/world/national-security/fbi-clarifies-rules-on-secretive-cellphone-tracking-devices/2015/05/14/655b4696-f914-11e4-a13c-193b1241d51a_story.html; Tom Jackman, *Experts Say Law Enforcement's Use of Cellphone Records Can Be Inaccurate*, WASH. POST, Jun. 27, 2014, http://www.washingtonpost.com/local/experts-say-law-enforcements-use-of-cellphone-records-can-be-inaccurate/2014/06/27/028be93c-faf3-11e3-932c-0a55b81f48ce_story.html; Matt Richtel, *A Police Gadget Tracks Phones? Shhh! It's Secret*, N.Y. TIMES, Mar. 15, 2015, http://www.nytimes.com/2015/03/16/business/a-police-gadget-tracks-phones-shhh-its-secret.html.

3. *See, e.g.*, Devlin Barrett, *CIA Aided Program to Spy on U.S. Cellphones*, WALL ST. J., Mar. 10, 2015, http://www.wsj.com/articles/cia-gave-justice-department-secret-phone-scanning-technology-1426009924; Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J., Nov. 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

4. *See, e.g.*, David E. Sanger & and Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES, Sep. 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html ("At Apple and Google, company executives say the United States government brought these changes on itself. The revelations by the former N.S.A. contractor Edward J. Snowden not only killed recent efforts to expand the law, but also made nations around the world suspicious that every piece of American hardware and software—from phones to servers made by Cisco Systems—have 'back doors' for American intelligence and law enforcement.").

FISA Court. Allies in Europe have complained about claimed invasions of their citizens'—or their leaders'—privacy. U.S. cloud providers and other tech companies have faced increasing challenges as foreign competitors seek to exploit the Snowden leaks to gain an advantage in overseas markets.

But far less attention has been paid to the impact of the Snowden leaks on domestic criminal law enforcement. Snowden's revelations have contributed to an increasingly difficult environment for law enforcement agencies in the United States—in the courts, with Internet and telecommunications service providers, and on Capitol Hill.

It is ironic, to say the least, that the backlash over the NSA's bulk collection practices would have such a profound impact on criminal law enforcement, which utilizes court-authorized legal process based on individualized suspicion to collect evidence—precisely the types of checks and balances the NSA's critics say were lacking in the Section 215 and PRISM programs. Indeed, as FBI Director James Comey noted in an October 2014 speech to the Brookings Institution,

> [i]n the wake of the Snowden disclosures, the prevailing view is that the government is sweeping up all of our communications. That is not true. And unfortunately, the idea that the government has access to all communications at all times has extended—unfairly—to the investigations of law enforcement agencies that obtain individual warrants, approved by judges, to intercept the communications of suspected criminals."[5]

Nevertheless, the effects of Snowden's disclosures are felt in investigations of virtually every type of crime imaginable. Because criminals of all types use cell phones, mobile devices, and Internet-based means of communication more than ever, electronic evidence is now critical in prosecuting cases involving terrorism, espionage, violent crime, drug trafficking, kidnapping, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. From emails and text messages to cell tower and GPS location information to social media message platforms to data stored on devices and in the cloud, evidence from the online world is increasingly critical to investigating and prosecuting all types of crimes in the "real world."

The greatest impact for law enforcement has been felt in courtrooms and judges' chambers throughout the country, where prosecutors and agents face increased skepticism from judges and more aggressive challenges from defense lawyers regarding the use of longstanding and previously accepted techniques for collecting digital evidence.

But law enforcement has also faced greater challenges behind the scenes, in dealing with telephone and Internet providers—including those who, after the attacks of September 11, 2001, had been more willing to assist law enforcement

---

5. James B. Comey, Address at the Brookings Institution, Washington, D.C. (Oct. 16, 2014), http://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

and national security in the name of public safety. The sense both domestically and abroad that service providers were either insufficiently protective of consumer data or unwilling to stand up to law enforcement has resulted in actions by those providers to distance themselves from law enforcement as never before.

Law enforcement has felt the impact in Congress as well. The politics of privacy have shifted, turning traditional supporters into skeptics and traditional skeptics into outspoken critics. As a result, the Justice Department has faced increasing resistance to efforts to maintain, let alone address gaps in, its ability to gather electronic evidence.

To be sure, not all of law enforcement agencies' struggles with judges, providers, and legislators are expressly attributable to the Snowden effect. But given the historical context, there can be little doubt that Snowden's leaks made an already difficult environment for law enforcement even more challenging.

This article explores (1) how the changing judicial and political landscape has impacted the ability of law enforcement to use a number of different types of crucial investigative techniques; (2) how these shifting sands have resulted in peril for prosecutors but new opportunities for defense lawyers; and (3) what prosecutors and defense lawyers can expect on the horizon.

II. PRIVACY VS. PUBLIC SAFETY—THE BATTLEGROUNDS

A. Pushback from the Courts

Over the past two years, it has been impossible to escape coverage of the Snowden leaks and the dramatic revelations about the extent to which the NSA was collecting data regarding Americans. Judges read the papers and watch television like the rest of us, so it stands to reason that they followed the coverage too.

But these issues were of more than just general interest to the bench. Judges' phone records were among those collected by the NSA, just like the rest of us. Judges also use laptops, and have tablets, and carry smartphones, just like the rest of us. As the Supreme Court observed in *Riley v. California*, 90% of American adults own a cell phone, and many of them "keep on their person a digital record of nearly every aspect of their lives."[6] This probably includes at least some of the Justices. Indeed, when Chief Justice Roberts described the functionality and capacity of a smart phone in that opinion, he did so with a familiarity that suggests that he has one in his pocket. As judges at all levels become adopters of technology, it is only natural that they, like ordinary citizens, would become more aware of and concerned about the potential privacy invasions that result from surveillance, search, and seizure in the digital era. As a Florida state judge declared during a hearing about the use of cell phone location information, "[w]hat right

6. 134 S.Ct. 2473, 2490 (2014).

does law enforcement have to hide behind the rules and to listen in and take people's information like the NSA? . . . Inhibiting law enforcement's rights are second to protecting mine!"[7] Although certainly colorful, this judge's comments may actually reflect a broader sentiment among members of the bench that digital privacy issues are important not just for their constitutional implications but for their practical impact on all of our lives.

But whatever the cause, it is clear that judges are increasingly concerned about the use of digital evidence-gathering techniques by federal, state, and local law enforcement. That concern has manifested itself in new or more pointed debates over the use of a number of previously well-established investigative techniques.

1. Search Warrants for Seized Devices and Email Accounts

With its opinions in *United States v. Comprehensive Drug Testing, Inc. (CDT)*,[8] the Ninth Circuit kicked off a national debate among judges and commentators about what, if any, special rules should govern searches of computers and other digital devices.

Law enforcement officers have been obtaining and executing search warrants for computers for decades. But as computers and other digital devices have become more pervasive in our lives, and as the volume of personal information stored on them has expanded, courts have become increasingly uncomfortable with the use of that time-honored authority. For some courts, searches of digital devices present unique privacy challenges because of the sheer volume of personal information contained, for example, on a smartphone or laptop. These judges have imposed protocols and rules to constrain law enforcement agents in executing such searches. Other judges view digital searches as essentially the same as physical searches of file cabinets, desk drawers, or other locations where paper documents could be found. For these judges, the privacy issues involved in searches of computers are just part and parcel of criminal investigations in the digital age.

In *CDT*, the majority, in dicta, instructed magistrate judges in the Ninth Circuit to impose search protocols as a condition for approving future applications for search warrants for computers. The court required that these protocols include, among other things:

- government agreement to waive reliance on the "plain view" doctrine;
- the use of an independent third party or specialized personnel to segregate and redact all nonresponsive information;

---

7. Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST, Feb. 22, 2015, https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html.

8. United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915 (9th Cir. 2006), *withdrawn and superseded by* 513 F.3d 1085 (9th Cir. 2008), *reh'g en banc*, 579 F.3d 989 (9th Cir. 2009) (en banc), *denying reh'g en banc*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam).

- a disclosure in applications and subpoenas detailing the actual risks of destruction of information specific to the case at hand, rather than mere allusion to general risks of deletion upon unauthorized entry;
- a search procedure designed to uncover only responsive information; and
- a requirement that the government destroy or return all non-responsive data and file a return as soon as practicable detailing what has been kept.

The Ninth Circuit later made its proposed search protocols advisory, rather than mandatory, as the court issued a per curiam opinion in the underlying case and relegated the search protocols to a concurrence. But the result was prolonged confusion within the Ninth Circuit among law enforcement, government attorneys, and defense counsel over what rules govern digital searches, as well as a split with other circuits over the imposition of search protocols. Indeed, the vast majority of other circuits have rejected the use of either *ex ante* search protocols or requirements that the government forego reliance on plain view as a condition of approving search warrants for computers.[9] Indeed, several of these other circuits have acknowledged that officers executing search warrants for computers are permitted to open and review every computer file where evidence of the crime under investigation might reasonably be found, recognizing that file names and extensions can be manipulated, enabling a criminal to conceal illegal materials by labeling them something mundane and misleading.[10]

Over the past year or so, this debate has migrated to include search warrants for e-mail accounts, with a similar split emerging among courts over whether special rules are needed to limit the scope of such searches.

Typically, when agents serve a search warrant on an e-mail provider as part of a criminal investigation, the provider does not screen the e-mails for relevance. On the contrary, the provider sends a copy of all of the e-mails in the account to the agents, who then review them for responsiveness to the warrant.

Like search warrants for computers, search warrants for email accounts are nothing new; they have been around since the population—including criminals—began using email to communicate. But over the past two years, a growing number of federal magistrate judges have refused to approve searches of e-mail accounts in the absence of protocols requiring that an independent third party or separate group of agents—or even the e-mail provider itself—screen out non-responsive material before turning over evidence to investigators.

---

9. *See, e.g.*, United States v. Richards, 659 F.3d 527, 538, 542 (6th Cir. 2011); United States v. Stabile, 633 F.3d 219, 237–38, 240–41 (3d Cir. 2011); United States v. Mann, 592 F.3d 779, 785 (7th Cir. 2010); United States v. Williams, 592 F.3d 511, 522 (4th Cir. 2010); United States v. Burgess, 576 F.3d 1078, 1094 (10th Cir. 2009); United States v. Cartier, 543 F.3d 442, 447–48 (8th Cir. 2008); United States v. Khanani, 502 F.3d 1281, 1290–91 (11th Cir. 2007); United States v. Upham, 168 F.3d 532, 535 (1st Cir. 1999).

10. *See, e.g.*, *Williams*, 592 F.3d at 522; *Upham*, 168 F.3d at 535. *But see* United States v. Galpin, 720 F.3d 436, 451–52 (2d Cir. 2013) (holding that searches of computers must be targeted at evidence of the crime covered by the warrant and suggesting that to the extent that officers' subjective intent is to seek information outside the scope of the warrant, plain view would be unavailable).

In August 2013, in the midst of the "Summer of Snowden," a federal district judge in Kansas became one of the first, if not the first, federal judge to reject a search warrant application for an e-mail account based on the possible scope of the search. The court rejected five applications for warrants that would have required Google, GoDaddy, Verizon, Yahoo, and Skype to disclose, among other things, the contents of all e-mails, IMs, and chat logs associated with the target accounts as part of an investigation into the theft of computer equipment. The court took issue with the warrants for two reasons: first, the warrants sought all content, regardless of whether that content was relevant to the criminal activity law enforcement was investigating; and, second, the warrants included no sorting or filtering procedures by which law enforcement would cull relevant evidence from either irrelevant or privileged material. The court concluded that the government was essentially requesting a "virtual carte blanche" to review the entire e-mail account of the target, observing that "the breadth of the information sought by the government's search warrant . . . is best analogized to a warrant asking the post office to provide copies of all mail ever sent by or delivered to a certain address so that the government can open and read all the mail to find out whether it [contains evidence]."[11]

Based on these conclusions, the court held that the government had not been sufficiently particular in its description of the scope of the material to be collected, declaring that warrants for Internet communications must contain articulated limits or boundaries. Unlike the Ninth Circuit in *CDT*, the court did not announce any particular search protocols and left the manner of limiting searches up to the government. The court did express approval of the following methods for limiting searches: asking the provider to disclose only content that contained certain key words or that was sent to or from certain parties, appointing a special master with authority to hire an independent vendor to use computerized search techniques, or setting up a "filter group" or "taint team" within the investigating agency.

In what some have referred to as the "Magistrates' Revolt,"[12] a magistrate judge in the District of Columbia went even further, rejecting a number of search warrant applications all on essentially the same grounds: the failure to adopt search protocols to prevent the government from seizing or searching e-mails or other data outside the scope of the warrants, and the failure to provide any timetable for when, if ever, the government intended to return the devices.[13] The judge had

---

11. In re Applications for Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO, 2013 WL 4647554 at *8, *9 (D. Kan. Aug. 27, 2013).

12. Anne E. Marimow & Craig Timberg, *Low-Level Federal Judges Balking at Law Enforcement Requests for Electronic Evidence*, WASH. POST, Apr. 24, 2014, http://www.washingtonpost.com/local/crime/low-level-federal-judges-balking-at-law-enforcement-requests-for-electronic-evidence/2014/04/24/eec81748-c01b-11e3-b195-dd0c1174052c_story.html.

13. *See, e.g.*, In re Search of Apple iPhone, IMEI 013888003738427, 31 F. Supp. 3d 159, 168–69 (D.D.C. 2014); In re Search of Black iPhone 4, S/N Not Available, 27 F. Supp. 3d 74 (D.D.C. 2014); In re Search of

previously instructed the government to include strict protocols in its applications, specifically: the application of keyword searches, the use of an independent special master to conduct initial screening, or implementation of a taint team. When the government failed to follow his instructions, the judge rejected eleven search warrant applications in a two-month period.[14]

Federal district judges in at least three other courts have taken a decidedly different view. Each approved the issuance of, or denied motions to suppress evidence from, warrants that required providers to turn over all e-mails sent to or from target accounts, even in the absence of search protocols or other indications from the government about how the searches would be conducted or what would be done with non-responsive e-mails after the search. As one court noted, searches of electronic communications create "'practical difficulties' that require a flexible approach to the application of the particularity requirement."[15]

The Washington Post and the Wall Street Journal tied the judges' "revolt" against domestic law enforcement directly to Snowden's revelations.[16] And what is perhaps most striking about this battle over the scope of computer and email searches is that the issue is not the evidentiary standard to be applied to law enforcement. On the contrary, the issue only arises in situations where law enforcement has already established probable cause that the devices or email accounts contain evidence of criminal activity. Moreover, the questions are not being raised by defense counsel during adversary proceedings, but rather by judges *sua sponte*, based on a growing concern about the amount of private information available to the government in the digital age.

2. *Searches of Cellphones Incident to Arrest*

Last year, in a landmark decision, the Supreme Court unanimously held that law enforcement generally must obtain a warrant before searching the contents of a cell phone seized from an arrested individual, rejecting the argument that such searches qualify for the "search incident to arrest" exception to the warrant requirement.[17] In doing so, the Court clearly indicated its view that digital devices are different

---

Information Associated with Facebook Account Identified by the Username Aaron.Alexis that is Stored at Premises Controlled by Facebook, Inc., 21 F. Supp. 3d 1, 9–11 (D.D.C. 2013).

14. *See, e.g.*, *Apple iPhone*, 31 F. Supp. 3d at 169; *Black iPhone 4*, 27 F. Supp. 3d at 80; In re Search of ODYS LOOX Plus Tablet, 28 F. Supp. 3d 40 (D.D.C. 2014).

15. *See* United States v. Ayache, 2014 WL 923340, at *2 (M.D. Tenn. Mar. 10, 2014); United States v. Deppish, No. 3:13-cr-153, 2014 WL 349735 (D. Kan. Jan. 31, 2014); United States v. Taylor, 764 F. Supp.2d 230 (D. Me. 2011).

16. Marimow & Timberg, *supra* note 12; Joe Palazzolo, *Judges Rebel Against Prosecutors' Bulk Requests for Emails in Probes*, WALL ST. J., Apr. 4, 2014, http://www.wsj.com/articles/SB10001424052702303847804579479513205095706.

17. *Riley v. California*, 134 S. Ct. 2473 (2014).

from physical items that could be seized incident to arrest because of the greater privacy concerns they present.

Under the "search incident to arrest" doctrine, police are generally permitted to search, without a warrant, an arrestee's person and the area within his immediate control, including some physical containers. The doctrine recognizes that an arrestee has a diminished expectation of privacy once he is in police custody and is based on the need to protect officer safety and prevent the destruction of evidence.

The doctrine has been used to search cell phones seized from arrestees for as long as arrestees have been carrying cell phones. But that all changed with *Riley*. The Supreme Court found that the rationale for the doctrine did not apply to cell phones. First, the digital data on a phone cannot be used as a weapon. While the data could indirectly protect officers by, for example, alerting them that accomplices were en route, the government had not offered evidence to show that this was a real problem and, in any event, other case-specific exceptions, such as that for exigent circumstances, could be used to justify a warrantless search if officer safety were at risk.

The Court also found that a warrantless search of a phone is not generally necessary to prevent the destruction of evidence. While a cell phone could be encrypted, that risk could be addressed by placing the phone in a "Faraday bag"—a bag made of aluminum foil that can block radio waves. While the phone could be remotely wiped, that risk could be addressed by turning the phone off or removing its battery.

But most importantly, the Court determined that even if a suspect has a diminished privacy interest post-arrest, "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search" of physical containers. The Court observed that phones are essentially "minicomputers" that can also be used as, among other things, cameras, video players, rolodexes, maps, calendars, and diaries. In addition, because cell phone have "immense storage capacity," with a capacity to hold "millions of pages of text, thousands of pictures, or hundreds of videos," a search of a phone can far exceed the scope of any search of a physical container. Indeed, the Court recognized that even one type of information typically stored on a phone—such as browsing history, photographs, or location data—can reveal a great deal of private information about a person's life. As the Court noted, a person "might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone." Moreover, a search of a cell phone might allow the police to search data not stored on the device at all, but somewhere in the cloud.

One month before *Riley* was decided, a NSA PowerPoint slide obtained by Snowden was revealed to the public. In it, the NSA described its "collection posture" as "Collect it All," "Process it All," "Exploit it All," "Partner it All,"

"Sniff it All" and, ultimately, "Know it All."[18] In a footnote, the Court in *Riley* ostensibly eschewed any connection between its ruling and the NSA's goals and activities stating that: "[b]ecause the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances."[19] But the environment in which *Riley* was decided cannot be ignored, and it is near certain that the Justices were aware of Snowden's revelations regarding the NSA's activities when confronted by the facts of the case.

The *Riley* case has had and will continue to have a profound and direct impact on law enforcement, making what was a routine practice slower and more cumbersome, and creating an increased risk that important evidence will be lost or encrypted before a warrant can be obtained. The impact of the decision was magnified when, in late 2014, Apple and Google announced that iPhones and Android phones would be encrypted by default and that the providers would not have the technical means to break the encryption. Apple and Google's policy change and its aftermath are discussed later in Section II.B.1.

But the impact of *Riley* on law enforcement goes beyond the need to get warrants where none were previously required. On the contrary, the Court's recognition that existing Fourth Amendment doctrines do not squarely apply to digital devices or evidence—that is, that digital evidence is just different—could signal even more dramatic legal changes and challenges for law enforcement in the years to come.

3. Use of Cell Tower Records

As a general matter, cell phone location information can be divided into two broad categories: cell tower information and precision-location information, often referred to as "GPS." Cell tower information—the records made by a cellular network provider indicating which cell tower serves a user's phone when that user places or receives a call or text message—can also be divided into two categories—"historical" and "prospective."

In order to require a cell phone company to disclose precision-location information for a suspect's cell phone, law enforcement obtains a warrant based on probable cause. That much has been clear. But there has been a great and growing controversy over the standards for obtaining cell tower information.

Since the mid-2000s, there has been a split among magistrates in different districts—and sometimes within the same district—over the standards for obtaining cell tower records prospectively. For some, the question is statutory—whether

18. GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE 97 (2014).

19. 134 S. Ct. at 2489, n.1.

the combination of the Stored Communications Act ("SCA") and the Pen/Trap Statute provide clear authority for the government to obtain these records. For others, the question is constitutional—whether users have a reasonable expectation of privacy in the records, notwithstanding their status as "third party" records. But whatever the cause, the result is that some courts require an order based on a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation," while other courts require a warrant based on probable cause.[20]

Until recently, it has been well-settled that to obtain historical cell tower records, law enforcement officers were not required to show probable cause, but rather were required to obtain a court order based on a showing of "specific and articulable facts."[21] For years, courts largely adopted the view that no warrant was required because, under the "third party doctrine," a user had no reasonable expectation of privacy in information voluntarily disclosed to a third party[22] or because the user had no reasonable expectation of privacy regarding his location while in a public place.[23] But recently defendants have begun challenging, and

---

20. *See* 18 U.S.C. §§ 2703(d), 3122–24 (2012). *Compare* United States v. White, 62 F. Supp. 3d 614, 621 (E.D. Mich. 2014) (requiring probable cause to track real-time location data for four weeks), In re Orders Authorizing the Installation and Use of Pen registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed], 416 F. Supp. 2d 390 (D. Md. 2006) (requiring probable cause in order to obtain prospective cell site information), In re Application of the United States of America for an Order Authorizing the Monitoring of Geolocation and Cell Site Data for a Sprint Spectrum Cell Phone Number ESN Cell Phone Number ESN Cell Phone Number ESN, No. 06-0186, 187, 188, 2006 WL 6217584, at *4 (D.D.C. Aug. 25, 2006) (agreeing with the "majority rule" that Criminal Rule 41 governs the request for prospective cell-site location information and requires probable cause), In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747, 764 (S.D. Tex. 2005), *and* Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) (holding that a person has a reasonable expectation of privacy in his or her cell-site location data in the context of real-time tracking), *with* In re Application of the United States of American for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 205 (E.D.N.Y. 2008) (holding that the Government may obtain prospective cell-site information without a showing of probable cause), In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 459–62 (S.D.N.Y. 2006) (holding that 18 U.S.C. § 2703(c), (d) permits a court to order the disclosure of prospective cell site information without a showing of probable cause), *and* In re Application of the United States for an Order: (1) Authorizing the Installation and Use of Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006) (holding that 18 U.S.C. § 2703(d) permits a court to order the disclosure of prospective cell site information without a showing of probable cause).

21. 18 U.S.C. § 2703(d).

22. In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611–15 (5th Cir. 2013); *accord* United States v. Moreno-Nevarez, No. 13-CR-0841-BEN, 2013 WL 5631017, at *2 (S.D. Cal. Oct. 2, 2013); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at *2–3 (N.D. Ind. Mar. 26, 2010); In re Applications of United States for Orders Pursuant to 18 U.S.C. § 2703(d), 509 F.Supp.2d 76, 81 (D. Mass. 2007).

23. *See, e.g.*, United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); United States v. Navas, 640 F. Supp. 2d 256 (S.D.N.Y. 2009), *rev'd in part on other grounds*, 597 F.3d 492 (2d Cir. 2010); In re Application of the United States for an Order: (1) Authorizing the Installation of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 411 F. Supp. 2d 678 (W.D. La. 2006). *Compare* United States v. Knotts, 460 U.S. 276 (1983) (holding that using a beeper to monitor a person's

courts have begun questioning, whether a warrant should be required for historical records as well.[24]

In *United States v. Graham*, the Fourth Circuit created a circuit split holding that a user has an expectation of privacy in historical cell site location information, and that searching that information therefore requires a warrant.[25] Applying the D.C. Circuit's mosaic theory,[26] the court reasoned that "[m]uch like long-term GPS monitoring, long-term location information disclosed in cell phone records can reveal both a comprehensive view and specific details of the individual's daily life."[27] Notably, the Fourth Circuit rejected the third-party doctrine applied by the Fifth and Eleventh Circuits because "[a] cell phone user cannot be said to "voluntarily convey" to her service provider information that she never held but was instead generated by the service provider itself without the user's involvement."[28] Although a warrant would be required in future situations, the *Graham* court held that the records of the present defendants should not be suppressed because the government relied in good faith on the SCA.[29]

---

location on public roads is not a search), *with* United States v. Karo, 468 U.S. 705 (1984) (holding that using a beeper to monitor a person's location inside a private residence is a search). The problem with this argument is that tracking cell site location data will inevitably lead to tracking a person in both public and private places. *See* United States v. White, 62 F. Supp. 3d. 614, 621 (E.D. Mich. 2014) (requiring probable cause to use cell phone data to track a suspect's movement on public roads because the cell-site location data included private spaces and the four-week time period justified a reasonable expectation of privacy).

24. *Compare* United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015) (en banc) (relying on third-party doctrine to reverse an 11th Circuit panel's probable cause requirement for historical cell site location data), In re Historical Cell Site Data, 724 F.3d 600, 611–15 (5th Cir. 2013) (holding that there is no expectation of privacy in geolocation data and therefore probable cause is not required), *with* United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014) (holding that cell site location information is within a person's reasonable expectation of privacy), *rev'd*, 785 F.3d 498 (11th Cir. May 5, 2015), In re Order Directing a Provider of Elec. Commc'n Serv. To Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (holding that while § 2703(d) does not require probable cause, a magistrate judge may require probable cause to avoid violating a person's reasonable expectation of privacy), *and* United States v. Cooper, No. 13-cr-00693-SI–1, 2015 WL 881578, at *6–8 (N.D. Cal. Mar. 2, 2015) (holding that a person has a reasonable expectation of privacy in historical cell site location data, even for calls made in public, collecting state cases holding the same). For a collection of cases holding that cell phone users have a reasonable expectation of privacy in historical cell site location records, see Tracey v. State, 152 So. 3d 504, 515–16 (Fla. 2014) (holding that a person has a reasonable expectation of privacy in prospective data).

25. United States v. Graham, Nos. 12-4659, 12-4825, slip op. at *31 (4th Cir. Aug. 5, 2015) ("[T]he government invades a reasonable expectation of privacy when it relies upon technology not in general use to discover the movements of an individual over an extended period of time. Cell phone tracking through inspection of CSLI is one such technology.").

26. *See* United States v. Maynard, 615 F.3d 544, 562 n.* (D.C. Cir. 2010) (analyzing a search as a collective mosaic of surveillance), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

27. *Graham*, slip op. at *27.

28. *Id.* at *48.

29. *Id.* at *64.

4. Cell Site Simulators

A cell site simulator[30] is a device that mimics a wireless carrier's base station or cell tower. Nearby wireless devices communicate and attempt to connect to the simulator as they would any nearby station. The simulator records the location and electronic identifying information of each wireless device and stores that information.[31] Law enforcement agencies have used cell site simulators since at least the 1990s.[32] Because the information obtained from the use of these devices constitutes "dialing, routing, addressing, or signaling information" from a mobile device, these devices have historically been understood to qualify as pen registers/trap and trace devices under the Pen/Trap statute[33]; as a result, the Department of Justice has "advised prosecutors to obtain a Pen/Trap order when employing [cell site simulators] in an investigation."[34] Under the Pen/Trap statute, the government need only certify that the information likely to be obtained is relevant to an ongoing criminal investigation.[35]

Despite this two-decade history, over the past three years judges and defense lawyers have begun to question the use of these devices.[36] For instance, in 2012, a federal magistrate judge in the Southern District of Texas rejected the government's argument that a Pen/Trap order was sufficient. Instead, the magistrate judge held that a cell site simulator is equivalent to a mobile tracking device, and

---

30. Other common terms for a cell site simulator are International Mobile Subscriber Identity (IMSI) catcher, digital analyzer, StingRay, and Triggerfish. StingRay and Triggerfish refer to two of the numerous products put out by Harris Corporation. *See* Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 1:00 PM), http://arstechnica.com/tech-policy/2013/09/25/meet-the-machines-that-steal-your-phones-data/.

31. Cell site simulators can also interfere with cell service, perform denial-of-service attacks, and some models can intercept audio or text-based content. *See generally id.*

32. *See, e.g.*, In re Application of the U. S. for an Order Authorizing the Use of a Cellular Tel. Digital Analyzer, 885 F. Supp. 197, 198 (C.D. Cal. 1995); Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, And Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 142 (2014).

33. 18 U.S.C. § 3127(3), (4) (2009).

34. Pell & Soghoian, *supra* note 31, at 143; *see also* Jon Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, LA WEEKLY, Jan. 24, 2013, http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739 (noting that when the LAPD wishes to use a StingRay, it also seeks permission under the Pen Register and Trap and Trace Statute).

35. 18 U.S.C. § 3123(a) (2001).

36. *See* Linda Lye, *In Court: Uncovering Stingrays, A Troubling New Location Tracking Device*, ACLU (Oct. 22, 2012, 12:42 p.m.), https://www.aclu.org/blog/free-future/court-uncovering-stingrays-troubling-new-location-tracking-device?redirect=blog/national-security-technology-and-liberty/court-uncovering-stingrays-troubling-new-location (stating that United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012), represented the "first case in the country to address the constitutional implications of [cell site simulators]"). In *Rigmaiden*, the court denied the defendant's motion for discovery holding that the information was protected by a qualified law enforcement privilege. 844 F. Supp. 2d at 1002. The court then denied the defendant's motion to suppress evidence obtained using the cell site simulator. United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (D. Ariz. May 8, 2013) (noting that defendant had been placed "at no disadvantage by the government's withholding of sensitive law enforcement information").

therefore requires probable cause under the Mobile Tracking Device statute, 18 U.S.C. § 3117.[37] Similarly, responding to a motion to suppress, the government stipulated that cell site simulators constitute a search and therefore require probable cause under the Fourth Amendment.[38]

Questions about the legal standard being used by federal law enforcement have been compounded by media reports suggesting that in numerous local police departments, the devices have been used based on court orders obtained without disclosing information about the operation of the devices to the issuing judge—or worse, without any judicial authorization at all.[39] In several instances that have garnered widespread media attention, defense lawyers have challenged evidence obtained from these devices, only to have local authorities refuse to provide information about the use of the devices—even in response to questioning by the court—citing a nondisclosure agreement between local police and the FBI. Local prosecutors have gone so far as to make favorable plea deals or even to dismiss cases altogether in order to avoid disclosing information about the use of this technique.[40] For instance, in a 2014 robbery prosecution in Baltimore, law enforcement withdrew evidence rather than disclose the device used to collect it (and violate non-disclosure agreements with the FBI and the device's manufacturer).[41] In another robbery case in Florida, the government offered the defendant, who was otherwise subject to at least four years in prison, a plea bargain imposing six months' probation, rather than testify about the use and capabilities of a cell-simulator used to collect evidence against the defendant.[42]

In the wake of press coverage of potential abuses by local law enforcement, Congress has demanded more information from the Justice Department about the use of the technology. The Justice Department reportedly has begun a review into how the devices are used by law enforcement agencies and has said it will begin providing more information publicly about the use of the devices. Meanwhile, the FBI has instructed agents that a warrant should be obtained before using these devices, and has made public statements clarifying that its nondisclosure agree-

---

37. In re Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 752 (S.D. Tex. 2012).

38. *See Rigmaiden*, 2013 WL 1932800, at *15; *see also* State v. Tate, 849 N.W.2d 798, 805 (Wis. 2014).

39. Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, WIRED (Mar. 3, 2014 9:00 AM), http://www.wired.com/2014/03/stingray/ (Florida police have used StingRays over 200 times without judicial permission).

40. *See Rigmaiden*, 844 F. Supp. 2d at 1002 (refusing to order the government to disclose law enforcement sensitive information); Gallagher, *supra* note 29 ("[StingRay] marketing materials come with a warning that anyone distributing them outside law enforcement agencies and telecom firms could be committing a crime punishable by up to five years in jail."); *but see* Nakashima, *supra* note 7.

41. Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, BALT. SUN, Nov. 17, 2014, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html.

42. Nakashima, *supra* note 7.

ments do not actually preclude police from acknowledging that they used the devices.

It is understandable that federal law enforcement officials would be wary about providing sufficient information about the operation of devices such that criminals could figure out how to defeat them. But in many ways, the controversy over stingrays is the product of unforced errors and abuses by local police, which has only fueled perceptions of government overreaching among the public and judiciary.

B. Pushback from Providers

In June 2013, the Washington Post and the Guardian published PowerPoint slides obtained by Snowden that detailed the NSA's PRISM program.[43] The slides described a process by which consumer data from some of the world's largest telecommunications and social media providers flowed into the NSA in order for the agency to surveil e-mail, chat (both video and voice), videos, photos, stored data, VoIP, file transfers, video conferencing, login dates, and social network details.[44]

These providers, who included Apple, Google, Facebook, Skype, AOL, and Microsoft, faced immediate criticism from users and quickly took steps to distance themselves from the NSA and PRISM. Apple released a statement in which it claimed it "first heard of the government's 'Prism' program when news organizations asked us about it on June 6. We do not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order."[45] Facebook's CEO Mark Zuckerberg stated "Facebook is not and has never been part of any program to give the U.S. or any other government direct access to our servers. We have never received a blanket request or court order from any government agency asking for information or metadata in bulk, like the one Verizon reportedly received. And if we did, we would fight it aggressively."[46] But as the controversy over PRISM grew, and as competitors abroad stepped up efforts to use PRISM to competitive advantage, U.S. providers began distancing themselves from the government more generally—including from criminal law enforcement.

The desire of providers to be perceived as privacy advocates and to avoid being perceived as closely aligned with the U.S. government has manifested itself in a number of ways. Among other things, providers aggressively challenged restrictions on what information they could put in their periodic transparency reports

---

43. Barton Gellman & Laura Poitras, *U.S. Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, Jun. 6, 2012, at A1; Greenwald & MacAskill, *supra* note 1.

44. *Id.*

45. *Apple's Commitment to Customer Privacy* (Jun. 16, 2013), https://www.apple.com/apples-commitment-to-customer-privacy.

46. Mark Zuckerberg (Jun. 4, 2013), https://www.facebook.com/zuck/posts/10100828955847631.

about U.S. government surveillance requests, resulting in litigation brought by Twitter and a coalition of tech companies.[47] The coalition settled the dispute after reaching an agreement with the Justice Department.[48] Under the agreement, tech companies may disclose approximately how many customer accounts are targeted. A disclosure's specificity depends on the type of requests disclosed. If a company wishes to disclose the number of national security letters it received, it can use bands of 1,000, such as 0–999. If the same company generalizes the inquiry type, it can be more specific about the number of inquiries received. For example, if a company disclosed the sum of inquiries from either national security letters or the Foreign Intelligence Surveillance Court, it could use bands of 250, such as 0–249. The tech companies can make those disclosures once every six months. While the coalition of tech companies accepted this settlement, Twitter has continued to wage this battle in court.[49]

But providers took other steps to distance themselves from the government that are having, and will continue to have, a particular impact on criminal law enforcement. First, Apple and Google have made encryption the default setting on their cell phones, with the providers unable to assist law enforcement in breaking that encryption even pursuant to a search warrant. Second, led by Microsoft, providers have mounted an aggressive challenge to law enforcement efforts to use search warrants to obtain data stored by those providers overseas. And third, providers generally have been less likely to cooperate voluntarily and more likely to challenge law enforcement than at any time in recent memory.

1. Apple and Google Adopt New Encryption Policies

As of May 2014, Apple, in response to a search warrant, was able to access and turn over data stored on an iPhone phone including "SMS messages, pictures and videos, contacts, audio recordings, and your phone's call history."[50] In October 2014, Apple announced default security upgrades for iPhones and iPads that now prevent the company from accessing any data kept on those devices without a user's passcode.[51] Apple also posted a lengthy message on its website in which it detailed the ways in which it protects customer data in the face of "government

47. Mike Isaac, *Twitter Reports a Surge in Government Data Requests*, N.Y. TIMES BITS (Feb. 9, 2015, 10:00 AM), http://bits.blogs.nytimes.com/2015/02/09/twitter-reports-surge-in-government-data-requests/?_r=0; Ben Lee, *Taking the fight for #transparency to court*, TWITTER (Oct. 7, 2014, 5:19 PM), https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court.

48. Craig Timberg & Adam Goldman, *U.S. to Allow Companies to Disclose More Details on Government Requests for Data*, WASH. POST, Jan. 27, 2014, http://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html.

49. *See* Twitter, Inc. v. Holder, No. 14-cv-4480, 2015 WL 1223466 (N.D. Cal. Jan. 9, 2015).

50. Andrew Cunningham, *New Guidelines Outline*, ARS TECHNICA (May 8, 2014), http://arstechnica.com/apple/2014/05/08/new-guidelines-outline-what-iphone-data-apple-can-give-to-police/.

51. *See* Trevor Timm, *Your iPhone is Now Encrypted*, THE GUARDIAN, Sep. 30, 2014, http://www.theguardian.com/commentisfree/2014/sep/30/iphone-6-encrypted-phone-data-default.

information requests."[52] Apple stated that "[f]or all devices running iOS 8.0 and later versions, Apple will not perform iOS data extractions in response to government search warrants because the files to be extracted are protected by an encryption key that is tied to the user's passcode, which Apple does not possess."[53] Google quickly followed suit, giving users the ability to encrypt data on Android devices so that it remains outside the reach of law enforcement, even in the face of a valid search warrant.[54]

The reaction to these new policies from the Justice Department was swift and, not surprisingly, less than positive. Assistant Attorney General Leslie Caldwell expressed concern about a "zone of lawlessness" created if law enforcement was unable to access information on seized phones despite lawful court orders.[55] Similarly, FBI Director Comey said that he did not comprehend why companies would "market something expressly to allow people to place themselves beyond the law."[56] He later observed that "[t[here's no doubt that all of us should care passionately about privacy, but we should also care passionately about protecting innocent people."[57]

Other Justice Department officials expressed similar concerns that the new systems would "make it harder, if not impossible, to solve some cases," with one observing that the companies had promised their customers "the equivalent of a house that can't be searched, or a car trunk that could never be opened."[58] In an October 2014 meeting between Justice Department officials and Apple executives, a DOJ official reportedly told the company that "a child would die" because police would not be able to scour a suspect's phone.[59] Even the President got into the mix, describing the providers' new encryption policies as dangerous: "If we get into a situation in which the technologies don't allow us at all to track somebody that we're confident is a terrorist . . . despite having a phone number or a social media

---

52. *Privacy—Government Information Requests*, APPLE, http://www.apple.com/privacy/government-information-requests/ (last visited June 24, 2015).

53. *Id.*

54. *See New Security Features in Android 5.0*, ANDROID OFFICIAL BLOG (Oct. 28, 2014), http://officialandroid.blogspot.co.uk/2014/10/a-sweet-lollipop-with-kevlar-wrapping.html.

55. Julian Hattem, *DOJ Fears Tech "Zone of Lawlessness,"* THE HILL (Jan. 27, 2015, 10:09 AM), http://thehill.com/policy/technology/230840-doj-fears-tech-zone-of-lawlessles (quoting Leslie Caldwell).

56. Brian Naylor, *Apple Says iOS Encryption Protects Privacy*, NPR (Oct. 8, 2014, 5:17 PM), http://www.npr.org/sections/alltechconsidered/2014/10/08/354598527/apple-says-ios-encryption-protects-privacy-fbi-raises-crime-fears (quoting FBI Director Comey).

57. Ellen Nakashima, *Tech Giants Don't Want Obama to Give Police Access*, WASH. POST, May 19, 2015, http://www.washingtonpost.com/world/national-security/tech-giants-urge-obama-to-resist-backdoors-into-encrypted-communications/2015/05/18/11781b4a-fd69-11e4-833c-a2de05b6b2a4_story.html.

58. Devlin Barrett & Danny Yadron, *New Level of Smartphone Encryption Alarms Law Enforcement*, WALL ST. J., Sept. 22, 2014, http://online.wsj.com/articles/new-level-of-smartphone-encryption-alarms-law-enforcement-1411420341.

59. Devlin Barrett et al., *Apple and Others Encrypt Phones, Fueling Government Standoff*, WALL ST. J., Nov. 18, 2014, http://www.wsj.com/articles/apple-and-others-encrypt-phones-fueling-government-standoff-1416367801.

address or email address, [if] we can't penetrate that, that's a problem."[60]

Local officials echoed those concerns as well. In an op-ed in the Washington Post, Cyrus Vance Jr., the district attorney for Manhattan, argued that Apple and Google's encryption of smartphones posed a threat to public safety and national security.[61] He wrote that "[w]hen threats to the common public safety arise, we ask Congress to do everything within its constitutional authority to address them. The provision of cloaking tools to murderers, sex offenders, identity thieves and terrorists constitutes such a threat. Absent remedial action by the companies, Congress should act appropriately."[62]

Apple and Google have pushed back. Apple executives described the DOJ's dire warnings about the kidnappings and murders that could result if law enforcement cannot gain access to an encrypted phone as "inflammatory."[63] Google's CEO Eric Schmidt brushed aside law enforcement's concerns, stating that "there are many ways law enforcement can get to data."[64] Apple's CEO Tim Cook echoed that sentiment: "Look, if law enforcement wants something, they should go to the user and get it. It's not for me to do that."[65] U.S. officials have observed that this dispute marks "a new low in relations between Silicon Valley and Washington since former National Security Agency contractor Edward Snowden began leaking state secrets last spring."[66]

Regardless of one's position on these issues, this much is clear—the adoption of these encryption protocols is a direct response to negative perceptions of providers' privacy protections in the wake of the NSA leaks, and—for better or worse—they will have a significant impact on law enforcement as much as any intelligence agency.

2. Jurisdictional Challenges to Search Warrants

Microsoft is currently litigating a search warrant issued by a magistrate judge in the Southern District of New York that orders the company to produce to the government emails kept by Microsoft on servers at a data center in Ireland.[67]

---

60. Remarks by President Obama and Prime Minister Cameron of the United Kingdom in Joint Press Conference (Jan. 16, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/01/16/remarks-president-obama-and-prime-minister-cameron-united-kingdom-joint-.

61. Cyrus R. Vance Jr., Op-Ed, *Apple and Google Threaten Public Safety with Default Smartphone Encryption*, WASH. POST, Sept. 26, 2014, http://www.washingtonpost.com/opinions/apple-and-google-threaten-public-safety-with-default-smartphone-encryption/2014/09/25/43af9bf0-44ab-11e4-b437-1a7368204804_story.html.

62. *Id.*

63. Barrett et al., *supra* note 59.

64. Danny Yadron, *Google's Schmidt Fires Back Over Encryption*, WALL ST. J., Oct. 8, 2014, http://www.wsj.com/articles/googles-schmidt-says-encrypted-phones-wont-thwart-police-1412812180.

65. Barrett et al., *supra* note 59.

66. *Id.*

67. Ellen Nakashima, *Microsoft Fights U.S. Search Warrant for Customer E-Mails Held in Overseas Server*, WASH. POST, Jun. 10, 2014, http://www.washingtonpost.com/world/national-security/microsoft-fights-us-search-

Microsoft moved to quash the warrant under the theory that the SCA only authorizes warrants to be issued pursuant to the Federal Rules of Criminal Procedure, which do not allow for extraterritorial enforcement.[68] Apple, Cisco, and Verizon have filed amicus briefs in support of Microsoft's position.[69]

In the Government's response to Microsoft's motion to vacate the warrant, it argued that electronic records controlled by a party are reachable by compulsory process no matter where the records are stored and that warrants issued pursuant to the SCA were fundamentally different from those authorizing law enforcement to enter physical premises and seize evidence.[70] Microsoft responded that such an argument re-writes the SCA and ignores the Fourth Amendment. Microsoft also argued that enforcing the warrant would "authorize the Government (including state and local governments) to violate the territorial integrity of sovereign nations and circumvent the commitments made by the United States in mutual legal assistance treaties expressly designed to facilitate cross-border criminal investigations."[71] Microsoft complained that if the Government's position were adopted it would have a "significant negative impact on Microsoft's business, and the competitiveness of U.S. cloud providers in general."[72] The Government maintained that not adopting its position would "serve[] as a dangerous impediment to the ability of law enforcement to gather evidence of criminal activity."[73] The magistrate judge ruled in the Government's favor and when Microsoft refused to produce the documents at issue, the company agreed to be held in contempt of court pending its appeal to the Second Circuit, which is ongoing.[74]

---

warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html.

68. Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States at 14–15, 17; In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 13-mj-2814 (S.D.N.Y. Jun. 6, 2014).

69. Memorandum in Support by Cisco Systems, Inc., Apple Inc., In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 13-mj-2814 (S.D.N.Y. Jun. 13, 2014); Memorandum in Support by Verizon Communications, Inc., In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 13-mj-2814 (S.D.N.Y. Jun. 10, 2014). NB: Verizon is a Steptoe client and its brief was filed by Michael Vatis.

70. Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant at 1, In re Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, No. 13-mj-2814 (S.D.N.Y. Apr. 25, 2014).

71. Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States at 1, In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 13-mj-2814 (S.D.N.Y. Jun. 6, 2014).

72. *Id.* at 5.

73. Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant at 2, In re Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, No. 13-mj-2814 (S.D.N.Y. Apr. 25, 2014).

74. Joe Mullin, *Microsoft agrees to contempt order so e-mail privacy case can be appealed*, ARS TECHNICA (Sep. 9, 2014), http://arstechnica.com/tech-policy/2014/09/microsoft-agrees-to-contempt-order-so-e-mail-privacy-case-can-be-appealed/.

As one Microsoft official put it, Snowden's revelations had "certainly put a premium on demonstrating to people that we are fighting."[75] Significantly, this is the kind of issue about which there would have been no fight prior to Snowden. Previously, the only litigated issue was whether the U.S. had jurisdiction over the served company, not where the data was stored. The outcome of this litigation will have a tremendous effect either way—either it will dramatically change the way law enforcement collects evidence even from U.S. providers, or it will profoundly affect the ability of providers to compete in overseas markets.

3. Less Cooperation, More Confrontation

Providers' public efforts to distance themselves from the government have impacted their private dealings with law enforcement as well. Anecdotally, law enforcement officials have observed that their relationships with providers are fundamentally different post-Snowden. Relationships that were friendly are now more arm's-length, and relationships that were already arm's-length are more distant. For instance, providers are more likely to require warrants or court orders where subpoenas previously would have sufficed, and they are less likely to agree not to disclose government requests to users without a court order directing them not to do so.[76]

C. The Politics of Privacy on the Hill

In the two years since Snowden's disclosures, many members of Congress who were once reliably pro-law enforcement and pro-national security have expressed increasing concern about government abuse of authority and surveillance overreach. Dissent has been heard from liberals and conservatives alike and has endangered reauthorization of portions of the PATRIOT Act as well as the passage of new legislation proposed by the Department of Justice. Members of Congress have also begun speaking out about perceived overreaching by local law enforcement, asking new questions about Stingrays, tracking devices, and cell site simulators.

Since 2009, one of the FBI's highest priorities on Capitol Hill was legislation to address what is often called the "Going Dark" problem. In a nutshell, while the Communications Assistance for Law Enforcement Act (CALEA) requires telecommunication carriers and broadband providers to build interception capabilities into their networks for court-ordered surveillance, that law does not reach providers of newer forms of communication.[77] As a result, in many cases, law enforcement is

---

75. Nakashima, *supra* note 66.

76. Craig Timberg, *Apple, Facebook, others defy authorities, increasingly notify users of secret data demands after Snowden revelations*, WASH. POST, May 1, 2014, http://www.washingtonpost.com/business/technology/apple-facebook-others-defy-authorities-increasingly-notify-users-of-secret-data-demands-after-snowden-revelations/2014/05/01/b41539c6-cfd1-11e3-b812-0c92213941f4_story.html.

77. Comey, *supra* note 5.

unable to execute a court-authorized wiretap order for a suspect's communications because the provider lacks the technical capability to implement it.[78] The FBI and DOJ worked for years on a legislative proposal to address this issue by incentivizing communications providers not covered by CALEA to build lawful intercept capabilities so that court-authorized wiretaps can be carried out. As Director Comey has explained, "We aren't seeking to expand our authority to intercept communications. We are struggling to keep up with changing technology and to maintain our ability to actually collect the communications we are authorized to intercept."[79] That legislation was a tough sell before Snowden, but now it's politically plutonium, as members of Congress are more wary of supporting any legislation that is meant to improve the government's ability to carry out surveillance.[80]

In addition, there is broad support from both privacy groups and the technology industry for Congress to pass bi-partisan legislation to modernize and reform the Electronic Communications Privacy Act (ECPA).[81] Although there are multiple iterations of the proposal, all would require the government to seek a warrant based on probable cause in order to obtain stored emails, eliminating ECPA's current distinctions based on how old the emails are and whether they were opened.[82] Many of those proposals also require a warrant to obtain any cell phone location information—including both prospective and historical cell tower information.[83] DOJ has said that it does not oppose a "warrant for all content" rule with limited exceptions,[84] but its ability to push back against other aspects of these bills with which it disagrees is almost certainly more limited post-Snowden.

If, in the words of FBI Director Comey, law enforcement was "going dark"[85] before Snowden, then now it is arguably going even darker.

---

78. *Id.*

79. *Id.*

80. Ellen Nakashima, *Proliferation of New Online Communications Services Poses Hurdles for Law Enforcement*, WASH. POST, July 26, 2014, http://www.washingtonpost.com/world/national-security/proliferation-of-new-online-communications-services-poses-hurdles-for-law-enforcement/2014/07/25/645b13aa-0d21-11e4-b8e5-d0de80767fc2_story.html.

81. *See, e.g.*, Allison Grande, *Google, Others Breathe New Life Into ECPA Reform*, Law360 (Jan. 29, 2013, 10:10 PM), http://www.law360.com/articles/410977/google-others-breathe-new-life-into-ecpa-reform; Mark Stanley, *Five Reasons to Reform ECPA Now*, CENTER FOR DEMOCRACY & TECHNOLOGY (Sept. 4, 2013), https://cdt.org/blog/five-reasons-to-reform-ecpa-now/.

82. Grande, *supra* note 80.

83. *E.g.*, Rainey Reitman, *New Bill Would Ensure Law Enforcement Gets a Warrant Before Reading Email*, ELEC. FRONTIER FOUND. (Mar. 8, 2013), https://www.eff.org/deeplinks/2013/03/new-bill-would-ensure-law-enforcement-get-warrant-reading-email.

84. *See ECPA Part 1: Lawful Access to Stored Content: Hearing Before the S. Comm. on Crime, Terrorism, Homeland Security, and Investigations*, 113 Cong. (2013) (statement of Acting Assistant Attorney General Elana Tyrangiel).

85. Comey, *supra* note 5.

II. CHALLENGES FOR PROSECUTORS, OPPORTUNITIES FOR DEFENSE LAWYERS

Because electronic evidence is so important to cases involving all types of crimes, every prosecutor and every defense lawyer should be aware of the challenges and opportunities presented by this post-Snowden environment.

For prosecutors, this is a time of great challenges. Prosecutors cannot take anything for granted, as investigative techniques that were once unquestioned are now at risk, and legal questions that were once considered routine are now controversial. More than ever, prosecutors need to be prepared for the fact that digital evidence-gathering techniques will be questioned by judges and that challenges from defense lawyers are much more likely to gain traction.[86]

For defense lawyers, this is a time of great opportunity. Defense lawyers, too, should take nothing for granted, and should capitalize on a renewed ability to challenge evidence collected using digital means. The days when a defense lawyer would move to suppress a wiretap (and would be unlikely to succeed) are over. Now, the evidence underlying the wiretap—the pen register data, the cell phone location information, the digital tracking devices—is in play as well. The same is true for search warrants, both physical and digital. Search warrants for computers and email accounts should be challenged, at least based on their scope. Motions attacking search warrants for physical locations should also be considered, especially to the extent the probable cause is derived from electronic evidence-gathering. It is more important than ever that defense counsel not leave points on the board.

III. WHAT'S NEXT?

We will continue to see post-Snowden privacy concerns at work both in the courts and on the Hill in the months and years ahead. In the courts, only time will tell how *Riley* will impact the caselaw on the scope of digital searches. We have already seen at least one case in which a magistrate judge rejected a search warrant for a seized cell phone based in part on a failure to satisfy the particularity requirement of the Fourth Amendment, relying extensively on the *Riley* Court's discussion of the vast amount of private data contained on cell phones and the differences between searches of cell phones and searches of physical items.[87]

---

86. *See, e.g.*, United States v. Daoud, No. 12-cr-723, 2014 WL 321384, at *3 (N.D. Ill. Jan. 29, 2014) (ordering disclosure to defense counsel of FISA application materials), *rev'd*, 755 F.3d 479 (7th Cir. 2014) (requiring that the trial judge review FISA materials ex parte in camera to determine whether disclosure was necessary and whether it would harm national security), *opinion supplemented by* 761 F.3d 678 (7th Cir. 2014), *cert. denied*, 135 S. Ct. 1456 (2015); United States v. Brown, No. 11-cr-60285-RSR, Doc. 786 (S.D. Fla. June 10, 2013) (ordering the prosecution to respond regarding whether the NSA had cell site location data that would exculpate the defendant).

87. *See, e.g.*, In re Search of Cellular Telephones Within Evidence Facility Drug Enforcement Admin., Kansas City Dist. Office, Case No. 14-MJ-8017-DJW (D. Kan. Dec. 30, 2014); *see also* State v. Henderson, 289 Neb. 271

But just three weeks later, a judge in the Southern District of New York reached the opposite conclusion, granting a warrant to search an entire Gmail account and noting that as with searches of paper files, "ample case authority sanctions some perusal, generally fairly brief, of . . . documents (seized during an otherwise valid search) . . . in order for the police to perceive the relevance of the documents to crime." The court declined to impose a search protocol in advance, observing that the Supreme Court has specifically said that "'[n]othing in the language of the Constitution or in th[e] Court's decisions suggests that . . . search warrants . . . must include a specification of the precise manner in which they are to be executed.'"[88] Moreover, the court found that imposing such restrictions ex ante would be a bad practice because there is no way to know in advance how a criminal may label or code his files or emails and because the government might need to examine seemingly innocuous emails as new information was obtained during the investigation. Future cases will tell us whether *Riley*'s observations about the difference between digital devices and physical containers will lead to new restrictions on the scope or methodology of electronic searches.

The growing unease among judges with digital privacy issues also has implications for the future of the third-party doctrine. Will the government continue to be able to rely on the doctrine to obtain digital data disclosed to a third party with a subpoena or court order, much like it does with bank, credit card, and other third party records? Or will digital data be treated differently?

Law enforcement should not look for relief on the Hill, where ECPA reform bills detrimental to law enforcement's stated goals continue to garner bipartisan sponsors and support from privacy groups and industry. Whether anything gets passed is another story—it is Congress, after all—but what does get passed is likely to be more restrictive on law enforcement, not less. We should expect similar results in state legislatures. Indeed, since May 2013, at least 10 states have passed laws curtailing the ability of law enforcement to access, use, or retain digital evidence, including state laws requiring warrants for cell phone metadata, location data, or the use of cell site simulators.[89]

(Neb. 2014) (relying on Riley and holding that scope of warrant to search cell phone was overly broad because of vast amounts of personal information stored on the phone).

88. In re Warrant for All Content and Other Info. Associated with the Email Account xxxxxxxx@gmail.com Maintained at Premises Controlled by Google, Inc, Case No. 1:14-MJ-00309-UA (S.D.N.Y.Jul. 18, 2014) (citing United States v. Grubbs, 547 U.S. 90, 97–98 (2006)).

89. S.B. 14–193, 69th Gen. Assemb., 2d Reg. Sess. (Co. 2014); H.B. 1384, 2014 Gen. Assemb., Reg. Sess. (Ind. 2014); H.B. 1009, 2014 Gen. Assemb., Reg. Sess. (Ind. 2014); S.B. 484, 126th Leg., Reg. Sess. (Me. 2013); S.B. 157, 126th Leg., Reg. Sess. (Me. 2013); S.B. 698, 2014 Gen. Assemb., Reg. Sess (Md. 2014); S.B. 2466, Minn. State Leg., Reg. Sess (Minn. 2014); S.B. 2087, 108th Gen. Assemb., Reg. Sess. (Tenn. 2014); H.B. 128, 2014 Utah State Leg., Gen. Sess. (Utah 2014); H.B. 17, 2014 Gen. Assemb., Reg. Sess. (Va. 2014); H.B. 536, 2013–2014 Leg. (Wi. 2014); H.B. 1440, 2015–2016 Leg., Reg. Sess. (Wash. 2015).

IV. CONCLUSION

In the wake of the Snowden disclosures, criminal lawyers on both sides of the "v" should continue to watch developments in the courts and on the Hill with great interest. For prosecutors, evidence-gathering techniques they once took for granted are increasingly under attack, while defense lawyers must be alert to new or greater avenues to pursue the suppression of digital evidence and the fruits thereof. Now more than ever, the "offense" has to play defense, and the defense has to go on the offensive.