



2014

# A Lot More than a Pen Register, and Less than a Wiretap

Stephanie Pell  
*Stanford Law School*

Christopher Soghoian  
*Yale Law School*

Follow this and additional works at: <http://digitalcommons.law.yale.edu/yjolt>

 Part of the [Computer Law Commons](#), [Intellectual Property Law Commons](#), and the [Science and Technology Law Commons](#)

### Recommended Citation

Pell, Stephanie and Soghoian, Christopher (2014) "A Lot More than a Pen Register, and Less than a Wiretap," *Yale Journal of Law and Technology*: Vol. 16: Iss. 1, Article 4.

Available at: <http://digitalcommons.law.yale.edu/yjolt/vol16/iss1/4>

This Article is brought to you for free and open access by Yale Law School Legal Scholarship Repository. It has been accepted for inclusion in Yale Journal of Law and Technology by an authorized administrator of Yale Law School Legal Scholarship Repository. For more information, please contact [julian.aiken@yale.edu](mailto:julian.aiken@yale.edu).

**A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP:<sup>1</sup>  
WHAT THE STINGRAY TEACHES US ABOUT HOW CONGRESS SHOULD  
APPROACH THE REFORM OF LAW ENFORCEMENT SURVEILLANCE  
AUTHORITIES<sup>2</sup>**

Stephanie K. Pell\* & Christopher Soghoian\*\*

16 YALE J.L. & TECH. 134 (2013)

**ABSTRACT**

*In June 2013, through an unauthorized disclosure to the media by ex-NSA contractor Edward Snowden, the public learned that the NSA, since 2006, had been collecting nearly all domestic phone call detail records and other telephony metadata pursuant to a controversial, classified interpretation of Section 215 of the USA PATRIOT Act. Prior to the Snowden disclosure, the existence of this intelligence program had been kept secret from the general public, though some members of Congress knew both of its existence and of the statutory interpretation the government was using to justify the bulk collection. Unfortunately, the classified nature of the Section 215 metadata program prevented them from alerting the public directly, so they were left to convey their criticisms of the program directly to certain federal agencies as part of a non-public oversight process. The efficacy of an oversight regime burdened by such strict secrecy is now the subject of justifiably intense debate. In the context of that debate, this Article examines a very different surveillance technology—one that has been used by federal, state and local law enforcement agencies for more than two decades without invoking even the muted scrutiny Congress applied to the Section 215 metadata program. During that time, this technology has steadily and significantly expanded the government’s surveillance capabilities in a manner and to a degree to date largely unnoticed and unregulated. Indeed, it has never been explicitly authorized*

---

<sup>1</sup> “A little more than kin, and less than kind.” WILLIAM SHAKESPEARE, HAMLET act 1, sc.

2.

<sup>2</sup> The authors would like to thank Susan Freiwald and Jim Green for their feedback and assistance.

\* Principal, SKP Strategies, LLC; Non-resident Fellow at Stanford Law School’s Center for Internet and Society; former Counsel to the House Judiciary Committee; former Senior Counsel to the Deputy Attorney General, U.S. Department of Justice; former Counsel to the Assistant Attorney General, National Security Division, U.S. Department of Justice; and former Assistant U.S. Attorney, Southern District of Florida.

\*\* Principal Technologist, Speech, Privacy & Technology Project, American Civil Liberties Union; Visiting Fellow, Information Society Project, Yale Law School. The opinions expressed in this article are this author’s alone, and do not reflect the official position of his employer.

16 YALE J.L. & TECH. 134 (2013)

2013-2014

*by Congress for law enforcement use. This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices, enables the government, directly and in real-time, to intercept communications data and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the assistance of a wireless carrier. Drawing from the lessons of the StingRay, this Article argues that if statutory authorities regulating law enforcement surveillance technologies and methods are to have any hope of keeping pace with technology, some formalized mechanism must be established through which complete, reliable and timely information about new government surveillance methods and technologies can be brought to the attention of Congress.*

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

I. INTRODUCTION .....	136
II. A BRIEF DESCRIPTION OF A STINGRAY AND ITS CAPABILITIES .....	144
III. IN BETWEEN OR BEYOND THE REACH OF STATUTORY LANGUAGE.....	148
A. <i>Real-time Cell Phone Tracking and Secrecy</i> .....	149
B. <i>The StingRay and Secrecy</i> .....	154
1. <i>The 1995 Digital Analyzer Magistrate Opinion</i> .....	157
2. <i>2012 StingRay Magistrate Opinion</i> .....	160
IV. WARNINGS FOR LEGISLATORS .....	163
V. SUGGESTIONS FOR REFORM .....	165
VI. CONCLUSION .....	169

## I. INTRODUCTION

Beginning in June 2013, the details of several National Security Agency (NSA) classified surveillance programs were revealed in a series of articles by journalists who had received documents from ex-NSA contractor Edward Snowden.<sup>3</sup> Among the many disclosures and subsequent releases of information by the Administration and Members of Congress was the revelation that, since 2006, the NSA has been collecting domestic call detail records and other domestic telephony metadata<sup>4</sup> in bulk, pursuant to a controversial interpretation of Section 215 of the USA PATRIOT Act

<sup>3</sup> See Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order> (“The National Security Agency is currently collecting the telephone records of millions of US customers of Verizon, one of America’s largest telecoms providers, under a top secret court order issued in April.”); see also Danny Yadron and Evan Perez, *T-Mobile, Verizon Wireless Shielded from NSA Sweep*, WALL ST. J., June 14, 2013, <http://online.wsj.com/article/SB10001424127887324049504578543800240266368.html> (explaining that the NSA “doesn’t collect information directly from T-Mobile USA and Verizon Wireless . . . [but the NSA] still capture[s] information, or metadata, on 99% of U.S. phone traffic because nearly all calls eventually travel over networks owned by U.S. companies that work with the NSA”).

<sup>4</sup> The Administration defines this telephony metadata as including “information about what telephone numbers were used to make and receive the calls, when the calls took place, and how long the calls lasted. . . . [T]his information does *not* include any information about the content of those calls—the Government cannot, through this program, listen to or record any telephone conversations.” Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act on Section 215, at 2 (Aug. 9, 2013) [hereinafter Administration White Paper on Section 215], <http://info.publicintelligence.net/DoJ-NSABulkCollection.pdf>.

(PATRIOT Act).<sup>5</sup> Section 215 is an intelligence collection authority permitting the government to compel “tangible things” from third parties that are “relevant” to an “authorized investigation” in order: (1) “to obtain foreign intelligence information not concerning a United States person”; or (2) to “protect against international terrorism or clandestine intelligence activities.”<sup>6</sup> The public has also learned that this massive quantity of data is collected and stored in a centralized database in order to enable future searches by the NSA—that is, if and when there is a reasonable articulable suspicion that an identifier (e.g. a phone number) is associated with a particular foreign terrorist organization<sup>7</sup> or with terrorism.<sup>8</sup> The goal of the program is “to enable the government to identify communications among known and unknown terrorism suspects, particularly those located inside the United States.”<sup>9</sup>

---

<sup>5</sup> For the most complete factual and legal explanation of the 215 metadata program from the Administration to date, see Administration White Paper on Section 215, *supra* note 4. Since the time the Administration chose to declassify and disclose the Section 215 White Paper to the public, two different federal district courts have issued dueling opinions on the legality of this intelligence program. See *ACLU v. Clapper*, No. 13-3994 (WHP) (S.D.N.Y. Dec. 27, 2013) (holding that the 215 bulk collection metadata program is lawful as both a statutory and constitutional matter); *Klayman v. Obama*, No. 13-0851 (RJL) (D.D.C. Dec. 16, 2013) (finding that the plaintiffs have demonstrated a substantial likelihood of success on a claim that the Section 215 metadata program violates the Fourth Amendment).

<sup>6</sup> 50 U.S.C. § 1861(a)(1).

<sup>7</sup> See Transcript: Newseum Special Program—NSA Surveillance Leaks: Facts and Fiction 8 (June 26, 2013) (statement of Robert Litt, General Counsel of the Office of Director of National Intelligence), <http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction> (“The metadata that is acquired and kept under this program can only be queried when there is reasonable suspicion, based on specific, articulable facts, that a particular telephone number is associated with specified foreign terrorist organizations. And the only purpose for which we can make that query is to identify contacts.”); see also Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL’Y (forthcoming 2013), <http://justsecurity.org/wp-content/uploads/2013/10/Just-Security-Donohue-PDF.pdf> (explaining that the Foreign Intelligence Court (FISC) “requires that the NSA establish a ‘reasonable, articulable suspicion’ that a seed identifier used to query the data be linked to a foreign terrorist organization before running it against the bulk data. Once obtained, information responsive to the query can be further mined for information. The NSA can analyze the data to ascertain second- and third-tier contacts, in steps known as ‘hops.’”).

<sup>8</sup> Privacy and Civil Liberties Oversight Board (PCLOB) Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 8-9, <http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf> [hereinafter PCLOB Report].

<sup>9</sup> *Id.* at 8.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

One major criticism of this domestic surveillance program is that the “common sense” reading of the statutory text of Section 215 does not, on its face, appear to permit collection on this scale. More specifically, critics argue that the contents of an entire massive database of records—in this case the records of nearly every domestic telephone call<sup>10</sup>—cannot simply

---

<sup>10</sup> See Yadron and Perez, *supra* note 3. *But see* Ellen Nakashima, *NSA is Collecting Less Than 30 Percent of U.S. Call Data, Officials Say*, WASH. POST, Feb. 7, 2014, [http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da\\_story.html](http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html) (“The National Security Agency is collecting less than 30 percent of all Americans’ call records because of an inability to keep pace with the explosion in cellphone use, according to current and former U.S. officials. . . . In 2006, a senior U.S. official said, the NSA was collecting ‘closer to 100’ percent of Americans’ phone records from a number of U.S. companies.”). For the sake of argument, suppose we assume those sources are correct and the NSA is collecting call records pertaining to no more than 30 percent of all domestic calls (presumably not much less, since the officials who were the sources of that figure in the article certainly did not choose that number arbitrarily but according to some rationale regarding an upper limit the government feels it can defend in attempting to mitigate larger figures claimed by other authors to date). Such a figure would still describe a sample justifiably characterized as “massive” in size, leaving the necessity, much less the legality, of collecting a cache of information so large, still quite open to question, whether or not *some* of the records in question are found to be actually relevant to an investigation.

The Administration has attempted to defend its interpretation of relevance:

It is well-settled in the context of other forms of legal process for the production of documents that a document is “relevant” to a particular subject matter not only where it directly bears on that subject matter, but also where it is reasonable to believe that it could lead to other information that directly bears on that subject matter. . . .

In light of that basic understanding of relevance, courts have held that the relevance standard permits requests for the production of entire repositories of records, even when any particular record is unlikely to directly bear on the matter being investigated, because searching the entire repository is the only feasible means to locate the critical documents. More generally, courts have concluded that the relevance standard permits discovery of large volumes of information in circumstances where the requester seeks to identify much smaller amounts of information within the data that directly bears on the matter. Federal agencies exercise broad subpoena powers or other authorities to collect and analyze large data sets in order to identify information that directly pertains to the particular subject of an investigation. Finally, in the analogous field of search warrants for data stored on computers, courts permit Government agents to copy entire computer hard drives and then later review the entire drive for the specific evidence described in the warrant.

be deemed relevant because *some* of the records in that database are actually relevant to an investigation.<sup>11</sup>

---

Administration White Paper on Section 215, at 9-10, *supra* note 4 (internal citations omitted).

<sup>11</sup> See Orin Kerr, *The Problem With the Administration “White Paper” on the Telephony Metadata Program*, VOLOKH CONSPIRACY (Aug. 12, 2013, 2:34 PM), <http://www.volokh.com/2013/08/12/problem-with-the-administration-white-paper-on-the-telephony-metadata-program> (arguing that the Administration position as expressed in its Section 215 White Paper does not adequately address “whether a massive database of billions of records can be deemed ‘relevant’ because some records inside the database are relevant”); see also Brief of Amicus Curiae, Professors of Information Privacy and Surveillance Law at 10-17, *In Re Electronic Privacy Information Center*, No. 13-58 (Aug. 12, 2013), <http://www.law.indiana.edu/front/etc/section-215-amicus-8.pdf> (arguing that call detail records and telephone metadata on all domestic Verizon calls could not be relevant to an authorized investigation); Donohue, *supra* note 7, at 48-49 (arguing that the telephony metadata program “violates the express statutory language . . . with regard to the language ‘relevant to an authorized investigation’; [and, among other ways,] in relation to [Section 215’s] requirement that the information sought can be obtained under subpoena duces tecum”).

In a recently declassified March 2009 Order from the Foreign Intelligence Surveillance Court (FISC), authorizing domestic bulk collection of metadata under Section 215, Chief Judge Reggie Walton acknowledges that the bulk collection of metadata “pertaining to communications of United States (‘U.S.’) persons located within the U.S. who are not the subject of an FBI investigation” could “not otherwise be legally captured in bulk.” *In re Production of Tangible Things From [REDACTED]*, No. BR 08-13, at 2-3 (FISA Ct. Mar. 2, 2009), [http://www.dni.gov/files/documents/section/pub\\_March%20202009%20Order%20from%20FISC.pdf](http://www.dni.gov/files/documents/section/pub_March%20202009%20Order%20from%20FISC.pdf).

Nevertheless, the FISC appears to authorize the program because of:

- (1) the government’s explanation, under oath of how the collection of and access to such data are necessary to analytical methods that are vital to the national security of the United States; and (2) minimization procedures that carefully restrict access to the BR metadata and includes specific oversight requirements.

*Id.* at 11-12.

Three Members of the PCLOB (Chairman David Medine and Board Members Jim Dempsey and Judge Patricia Wald) have concluded that the 215 metadata program fails to comply with Section 215’s statutory language. The major arguments for the program’s non-compliance with Section 215 of the PATRIOT Act can be summarized as follows:

- First, the telephone records acquired under the program have no connection to any specific FBI investigation at the time of their

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

While the existence of this intelligence program had been kept from the general public prior to the summer 2013 Snowden disclosures and subsequent declassification of information by the Executive branch, some members of Congress knew of its existence and were privy to the statutory interpretation the government was employing to justify the bulk collection of domestic telephone records. Indeed, during a floor debate in 2011, Senator Ron Wyden warned his colleagues that “when the American people find out how their government has secretly interpreted the PATRIOT Act, they will be stunned and they will be angry.”<sup>12</sup>

As this Article goes to print, the Executive and Legislative branches of government are finally engaging the public in a much more robust, transparent discussion about the Section 215 metadata program. Moreover,

---

collection. Second, because the records are collected in bulk potentially encompassing all telephone calling records across the nation they cannot be regarded as “relevant” to any FBI investigation as required by the statute without redefining the word relevant in a manner that is circular, unlimited in scope, and out of step with the case law from analogous legal contexts involving the production of records. Third, the program operates by putting telephone companies under an obligation to furnish new calling records on a daily basis as they are generated (instead of turning over records already in their possession) an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole. Fourth, the statute permits only the FBI to obtain items for use in its investigations; it does not authorize the NSA to collect anything.

PCLOB Report, *supra* note 8, at 10.

Two other PCLOB Members (Elisebeth Collins Cook and Rachel Brand) did not agree, however, that the 215 metadata program lacked statutory authorization. *See* Separate Statement by Board Member Elisebeth Collins Cook at 1, <http://www.pcllob.gov/SiteAssets/Pages/default/PCLOB-Cook-Statement.pdf>; Separate Statement by Board Member Rachael Brand at 3, <http://www.pcllob.gov/SiteAssets/Pages/default/PCLOB-Brand-Statement.pdf>.

For a defense or more detailed analysis of the Administration’s interpretation of relevance under Section 215, *see* Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, 1 LAWFARE RESEARCH PAPER SERIES (Sept. 1, 2013), <http://www.lawfareblog.com/wp-content/uploads/2013/08/Bradbury-Vol-1-No-3.pdf>; David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RESEARCH PAPER SERIES (Sept. 29, 2013), <http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf>.

<sup>12</sup> Press Release, Senator Ron Wyden, In Speech, Wyden Says Official Interpretations of Patriot Act Must be Made Public (May 26, 2011), <http://wyden.senate.gov/newsroom/press/release/?id=34eddcdb-2541-42f5-8f1d-19234030d91e>.

as the Administration continues declassification of Section 215-related documents, several Members of Congress are calling for reforms to the statute, some arguing for termination of the entire Section 215 bulk collection program.<sup>13</sup> Even President Obama has suggested that the government should no longer hold the data, although the Administration has not yet taken a position on who or what entity should warehouse the voluminous call records and other telephony business records.<sup>14</sup>

Meanwhile, a clearer picture of earlier cryptically worded criticisms of the program voiced by members of Congress has emerged. We now know that some members of Congress who were aware of the government's legal interpretation of Section 215 actively urged the Executive branch to engage in a more public discussion of the issue in a manner that would not harm national security. In other words, as controversial as the Section 215 program has come to be in light of the Snowden revelations, prior to those unauthorized disclosures an established process had already enabled at least some measure of congressional oversight and review.<sup>15</sup> That process, in turn, enabled Senators Russ Feingold, Richard Durbin, Wyden, and Mark Udall to warn the public and other members of Congress that the

---

<sup>13</sup> See, e.g., The USA Freedom Act of 2013, S. 1599, 113th Cong. (2013); The USA Freedom Act of 2013, H.R. 3361, 113th Cong. (2013) (prohibiting bulk collection of American's records by, among other things, limiting the use of Section 215 to records or tangible things pertaining to: "(A) a foreign power or agent of a foreign power, (B) the activities of a suspected agent of a foreign power who is the subject of . . . [an] authorized investigation, or (C) an individual in contact with, or known to, a suspected agent of a foreign power").

<sup>14</sup> See President Obama's Prepared Remarks on Signals Intelligence Programs 7 (Jan. 17, 2014), <http://justsecurity.org/wp-content/uploads/2014/01/President-Speech-on-Intelligence-Reforms.pdf> ("I am therefore ordering a transition that will end the Section 215 bulk metadata program as it currently exists, and establish a mechanism that preserves the capabilities we need without the government holding this bulk meta-data."); see also PCLOB Report, *supra* note 8, at 102 ("[S]anctioning the NSA's program under Section 215 requires an impermissible transformation of the statute . . . . Because Section 215 does not provide a sound legal basis for the NSA's bulk telephone records program, we believe the program must be ended."). *But see* Separate Statements of Board Members Elisebeth Collins Cook and Rachael Brand, *supra* note 11 (dissenting from the PCLOB's recommendation to shut down the 215 metadata program).

<sup>15</sup> See *The USA PATRIOT Act: Hearing before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 8 (2009) (oral testimony of Todd M. Hinnen, Deputy Assistant Attorney General), [http://judiciary.house.gov/\\_files/hearings/printers/111th/111-35\\_52409.PDF](http://judiciary.house.gov/_files/hearings/printers/111th/111-35_52409.PDF) ("The business records provision [Section 215] allows the government to obtain any tangible thing it demonstrates to the FISA court is relevant to a counterterrorism or counterintelligence investigation. . . . It also supports an important, sensitive collection program about which many members of the Subcommittee or their staffs have been briefed.")

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

government was misusing its Section 215 authority, albeit in opaque and suggestive language necessitated by the classified status of the surveillance program.<sup>16</sup> While it is fair to argue that congressional oversight of government intelligence programs is far from ideal, we must at least acknowledge that the government's expansive interpretation and use of Section 215 was known and debated by some Members of Congress—some approving of the program,<sup>17</sup> some not—even if it could not be directly named or described in public until after Edward Snowden's disclosures. The efficacy of an oversight regime burdened by such strict secrecy is now the subject of justifiably intense debate.

In the context of that debate, this Article examines a very different surveillance technology—one that has been used by federal, state and local law enforcement agencies for more than two decades without invoking even the muted scrutiny Congress applied to the 215 metadata program.<sup>18</sup> In that time, this technology has steadily and significantly expanded the government's surveillance capabilities in a manner and to a degree to date largely unnoticed and unregulated—indeed, it has never been explicitly authorized by Congress for law enforcement use.<sup>19</sup> This technology, commonly called the StingRay, the most well-known brand name of a family of surveillance devices known more generically as “IMSI catchers,” is used by law enforcement agencies to obtain, directly and in real time, unique device identifiers and detailed location information of cellular phones—data that it would otherwise be unable to obtain without the

---

<sup>16</sup> See Christopher Soghoian, *Senators Hint at DOJ's Secret Reinterpretation and Use of Section 215 of the Patriot Act*, SLIGHT PARANOIA, May 24, 2011, <http://paranoia.dubfire.net/2011/05/senators-hint-at-doj-s-secret.html> (describing statements by Senators hinting at the existence of an alternate use of Section 215).

<sup>17</sup> See Ed O'Keefe, *Transcript: Dianne Feinstein, Saxby Chambliss Explain, Defend NSA Phone Records Program*, WASH. POST, June 6, 2013, <http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program> (defending the 215 metadata program, Senator Dianne Feinstein stated, “As far as I know, this is the exact three month renewal of what has been the case for the past seven years. This renewal is carried out by the FISA Court under the business records section of the Patriot Act. Therefore, it is lawful.”).

<sup>18</sup> See Glen L. Roberts, *Who's On The Line? Cellular Phone Interception at its Best*, FULL DISCLOSURE, (1991), archived at <http://blockyourid.com/~gbpprorg/2600/harris.txt> (describing the marketing by the Harris Corporation of TriggerFish passive surveillance devices to law enforcement agencies at the National Technical Investigators Association conference in 1991).

<sup>19</sup> See *infra* Part III.B.

assistance of a wireless carrier.<sup>20</sup> Whether installed in a vehicle, mounted on a drone, or carried by hand, this unregulated and technologically unmediated surveillance technology can, for example, send signals through the walls of homes to locate and identify nearby cell phones without the assistance of a wireless carrier and without providing any notice to the targets of the surveillance operation.<sup>21</sup>

This Article describes how the StingRay's unmediated collection capabilities do not fit well into the post-9/11 (or, for that matter, pre-9/11) Pen Register and Trap and Trace statute ("Pen/Trap"),<sup>22</sup> the criminal surveillance authority normally used by federal law enforcement agencies to acquire certain types of non-content communications data in real-time. The lack of specific statutory authorization has not, however, served as a practical barrier to use of this technology by law enforcement agencies. Indeed, for several years prior to the passage of the PATRIOT Act, the official Department of Justice (DOJ) policy was that, since no specific statutory or Fourth Amendment prohibition forbade the practice, law enforcement could use StingRays without any form of judicial oversight.<sup>23</sup> After the PATRIOT Act broadened the definitional section of the Pen/Trap statute, DOJ interpreted the statute to authorize the collection of nearly all non-content information exchanged between a mobile device and a cell tower and, accordingly, advised prosecutors to obtain a Pen/Trap order when employing IMSI-catchers in an investigation.<sup>24</sup>

The StingRay, therefore, illustrates how the legislature's authority can be effectively short-circuited when: (1) the government stretches existing statutory definitions to accommodate a new type of collection capability or surveillance technology not contemplated by Congress; and (2) there is no established mechanism to ensure legislative notice and review that would enable Congress affirmatively to choose whether or not to regulate the government's use of new or existing surveillance methods and technologies.

Drawing from the lessons of the StingRay, this Article argues that, if statutory authorities regulating law enforcement surveillance technologies

---

<sup>20</sup> See *infra* Part II. Some IMSI catchers also have the capacity to intercept content communications, though we are unaware of any public evidence regarding the extent to which law enforcement uses this capacity, if at all. See *infra* note 46.

<sup>21</sup> *Id.*

<sup>22</sup> 18 U.S.C. §§ 3121–3127 (2012).

<sup>23</sup> See *infra* Part III.B.

<sup>24</sup> See *id.* It is currently unclear from publically available information, however, when and under what circumstances DOJ—due to potential Fourth Amendment issues or other policy considerations—may advise prosecutors to seek additional types of judicial authorization under existing statutes.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

and methods are to have any hope of keeping pace with technology, some formalized mechanism must be established through which complete, reliable and timely information about new and existing government surveillance methods and technologies shall be brought to the attention of Congress. That information, among other things, must include: (1) how the government interprets existing law to permit or, conversely, not to prohibit its use of a particular collection method; and (2) how it uses such technologies in criminal investigations.

Moreover, through a discussion of how the StingRay has evaded formal congressional oversight, this Article identifies several specific characteristics of any new or existing surveillance technologies or methods that should guide Congress in assessing the need for new regulation, as well as periodic assessment of any potential need to update existing statutory authorities to accommodate technological change and innovation. Finally, under the theory that Congress cannot begin to address the policy challenges posed by new surveillance technologies in the absence of adequate notice about their existence and actual or reasonably likely use by law enforcement, this Article proposes a way for Congress to create a mechanism to ensure that it receives such notice.

## II. A BRIEF DESCRIPTION OF A STINGRAY AND ITS CAPABILITIES<sup>25</sup>

Mobile phones communicate by radio signal with a wireless carrier's network of cellular base stations or "cell sites." These cell sites are generally located on cell towers that serve geographic areas of varying sizes.<sup>26</sup> The regular communication between phone and cell sites enables the carrier to route calls, text messages and Internet data to and from a subscriber's mobile phone. To facilitate this process, cellular phones periodically register themselves with the nearest cell site so that the network can connect incoming calls and text messages to the subscriber's phone.<sup>27</sup> This registration process, as well as the act of making a call or transmitting data, automatically generates location data of varying degrees of precision.<sup>28</sup> Government agencies can compel a provider to disclose

---

<sup>25</sup> For a more detailed technical description and analysis of the StingRay, see Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and its Impact on National Security and Consumer Privacy* (2014) (on file with the Journal).

<sup>26</sup> See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 *BERKELEY TECH. L.J.* 117, 126 (2012).

<sup>27</sup> *Id.* at 126-27.

<sup>28</sup> *Id.* at 126-33.

location data, whether the data was automatically generated by the wireless carrier in the normal course of business or specifically created in response to a surveillance request to “ping” a phone.<sup>29</sup> Such “carrier-assisted surveillance” can reveal a phone’s historical, current, or prospective location (e.g., real-time tracking),<sup>30</sup> as well as other types of data, such as numbers called<sup>31</sup> and the addresses of web pages viewed from a mobile device.<sup>32</sup>

Carrier-assisted surveillance is not, however, the only means through which law enforcement can acquire such information. By impersonating a cellular network base station, a StingRay—a surveillance device that can be carried by hand, installed in a vehicle, or even mounted on a drone<sup>33</sup>—tricks all nearby phones and other mobile devices into identifying themselves (by revealing their unique serial numbers) just as

---

<sup>29</sup> *Id.* at 131-32. See also Comments of CTIA—The Wireless Association on U.S. Department of Justice Petition for Expedited Rulemaking at 17, *In re* Petition for Expedited Rulemaking To Establish Technical Requirements and Standards Pursuant to Section 107(b) of the Communications Assistance for Law Enforcement Act, Docket No. RM-11376 (FCC July 25, 2007), <http://fjallfoss.fcc.gov/ecfs/comment/view?id=5514711157> (“Law enforcement routinely now requests carriers to continuously ‘ping’ wireless devices of suspects to locate them when a call is not being made . . . so law enforcement can triangulate the precise location of a device and [seek] the location of all associates communicating with a target.”); see also *Devega v. State*, 689 S.E.2d 293, 299 (Ga. 2010) (“[T]he investigators requested that Devega’s cell phone provider ‘ping’ his phone, which the officers described as sending a signal to the phone to locate it by its global positioning system (GPS). The company complied and informed the police that the phone was moving north on Cobb Parkway.”).

<sup>30</sup> See generally Pell & Soghoian, *supra* note 26, at 126-132.

<sup>31</sup> See generally collections of files posted at [http://www.markey.senate.gov/documents/2013-10-03\\_ATT\\_re\\_Carrier.pdf](http://www.markey.senate.gov/documents/2013-10-03_ATT_re_Carrier.pdf) and [http://www.markey.senate.gov/documents/2013-12-09\\_VZ\\_CarrierResponse.pdf](http://www.markey.senate.gov/documents/2013-12-09_VZ_CarrierResponse.pdf) (describing their disclosure of real-time ‘pen register’ and ‘trap and trace’ data to law enforcement agencies).

<sup>32</sup> *Id.* See Christopher Soghoian, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA, Dec. 1, 2009, <http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html> (quoting Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, stating: “On the Sprint 3G network, we have IP data back 24 months, and we have, depending on the device, we can actually tell you what URL they went to.”) See also Verizon Wireless, Law Enforcement Resource Team (LERT), Apr. 20, 2009, <http://info.publicintelligence.net/VerizonLawEnforcementResourceTeam.pdf> (a presentation to law enforcement agencies by Verizon Wireless revealing that the company retains “IP destination information” for “30 days”).

<sup>33</sup> See Jennifer Valentino-DeVries, *Judge Questions Tools That Grab Cellphone Data on Innocent People*, WALL ST. J., Oct. 22, 2012, <http://blogs.wsj.com/digits/2012/10/22/judge-questions-tools-that-grab-cellphone-data-on-innocent-people> (“StingRay equipment can be carried by hand or mounted on vehicles or even drones.”).

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

they would register with genuine base stations in the immediate vicinity.<sup>34</sup> As each phone in the area identifies itself, the StingRay can determine the location from which the signal came.<sup>35</sup> The StingRay and other similar devices also have the capacity, if so configured, to intercept data transmitted and received by the phone, including the content of calls, text messages, numbers dialed, and web pages visited.<sup>36</sup> This process is accomplished without any visual indication to the target that she is under surveillance or any mediating involvement on the part of the carrier whose network the StingRay is impersonating.<sup>37</sup> In circumstances where the government either cannot acquire, or chooses not to compel, assistance from a provider, the StingRay may be the surveillance technique of choice.<sup>38</sup> Moreover, unlike carrier-assisted surveillance, in which the third-party provider necessarily has knowledge of surveillance performed and copies of records disclosed at the request of law enforcement, the unmediated nature of the StingRay dictates that only the operator of the device has: (1) knowledge that an

<sup>34</sup> See Daehyun Strobel, *IMSI Catcher*, Seminar Work 17 (Ruhr-Universität Bochum, 2007), [http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi\\_catcher.pdf](http://www.emsec.rub.de/media/crypto/attachments/files/2011/04/imsi_catcher.pdf) (“An IMSI Catcher masquerades as a Base Station and causes every mobile phone of the simulated network operator within a defined radius to log in. With the help of a special identity request, it is able to force the transmission of the IMSI.”).

<sup>35</sup> In fact, a different device made by the same company that manufactures the StingRay is used to locate devices. However, for clarity’s sake, we use the term StingRay in this article to refer to all of the devices in that family of products. See Harris Corp., *Sole Source Vendor Letter 6* (2008), <http://egov.ci.miami.fl.us/Legistarweb/Attachments/48003.pdf> (describing the Harris AmberJack Direction Finding System).

<sup>36</sup> See Harris Corp, *Price List 4* (2008), <https://info.publicintelligence.net/Harris-SurveillancePriceList.pdf> (listing an optional “GSM Intercept Software package” for the StingRay).

<sup>37</sup> See Executive Office for United States Attorneys, *Cell Site Simulators, Triggerfish, Cell Phones*, USA BOOK 18 (2008), [https://www.aclu.org/pdfs/freespeech/cellfoia\\_release\\_074130\\_20080812.pdf](https://www.aclu.org/pdfs/freespeech/cellfoia_release_074130_20080812.pdf) (obtained through FOIA by the American Civil Liberties Union) (“A cell site simulator . . . is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN) and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider.”). USA Bulletins such as these are published by the Executive Office of United States Attorneys (EOUSA) and distributed to United States Attorney’s Offices across the country. They cover a range of topics and issues (like law enforcement surveillance methods) of interest to federal prosecutors, including new case law, law enforcement tools and practices, statutory authorities, and internal DOJ guidance. See also Strobel, *supra* note 34, at 21 (“In most cases, the [use of an IMSI catcher] cannot be recognized immediately by the subscriber.”).

<sup>38</sup> Intelligence agencies operating on foreign soil and thus presumably unable to compel the assistance of telephone companies could, for example, use a StingRay for communications interception.

interception ever took place,<sup>39</sup> and (2) or access to the information intercepted. Thus, to the extent that telephone companies are able to act as a proxy for their customers' privacy interests and may "push back" against overbroad or otherwise improper government surveillance,<sup>40</sup> no such advocate exists for the target when a Stingray is used. In short, the unmediated nature of StingRay technology makes it essentially "invisible" in operation and leaves behind no retrievable trace that is subject to future detection.<sup>41</sup>

Consider, for example, a situation where law enforcement agents can physically identify a target during the course of an investigation, but do not know the telephone she is currently using, perhaps because the target frequently cycles through disposable "burner" cell phones.<sup>42</sup> Investigators can position a StingRay in the vicinity of the target to capture the unique serial number of the target's phone.<sup>43</sup> In this case, law enforcement collects the identifying data in real-time because the StingRay, masquerading as the

---

<sup>39</sup> In those circumstances where a court knowingly grants a Pen/Trap order authorizing law enforcement use of a StingRay in a criminal investigation, the judge would have knowledge that law enforcement intended to collect communications data but would not likely know when the surveillance occurred or the scope and amount of data collected. See *infra* Part III.B. for a discussion of federal magistrate opinions considering government applications to use cellular interception devices pursuant to the Pen/Trap statute.

<sup>40</sup> At a House Judiciary Committee hearing in 2011, Congressman Robert C. Scott asked Todd Hinnen, then the Acting Assistant Attorney General for National Security at the Department of Justice, "why would [a service provider] . . . have an incentive to hire lawyers to protect [their subscribers' privacy] rights?" Mr. Hinnen responded by stating his belief that "telecommunication providers and Internet service providers take the privacy of their customers and subscribers very seriously and I think are often an effective proxy for defending those rights." *Permanent Provisions of the PATRIOT Act: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 69 (2011) (statement of Acting Assistant Att'y Gen. for National Security, Todd M. Hinnen), [http://judiciary.house.gov/hearings/printers/112th/112-15\\_65486.PDF](http://judiciary.house.gov/hearings/printers/112th/112-15_65486.PDF).

<sup>41</sup> *Cell Site Simulators, Triggerfish, Cell Phones*, *supra* note 37, at 18 ("This can be done without the user knowing about it").

<sup>42</sup> See *The Wire: Amsterdam*, at 00:42:23 (HBO television broadcast Oct. 10, 2004) ("They make a couple of calls with a burner, throw it away. Go on to the next phone, do the same." "There's more of those things laying around the streets of West Baltimore than empty vials." "Well, how the fuck you supposed to get a wire up on that?" "Yeah, well, first it was payphone and pagers. Then it was cell phones and face-to-face meets. Now this. The motherfuckers do learn. Every time we come at them, they learn and adjust.")

<sup>43</sup> See Complaint at 8 n.1, *United States v. Arguijo et al.* (N.D. Ill. Feb. 13, 2012) (under seal), [http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222\\_01d.pdf](http://www.justice.gov/usao/iln/pr/chicago/2013/pr0222_01d.pdf) ("Law enforcement officers . . . used a digital analyzer device on three occasions in three different locations where Chaparro was observed to determine the IMSI associated with any cellular telephone being carried by Chaparro.").

### A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

cell site with the strongest signal,<sup>44</sup> receives the information immediately and directly as it is communicated by the mobile phones, leaving no trace of the interception with the third party provider.<sup>45</sup> Moreover, while law enforcement may only seek to identify or locate the target's mobile device, a StingRay will also, as a matter of course, collect data from many other mobile devices in the surrounding area.<sup>46</sup>

### III. IN BETWEEN OR BEYOND THE REACH OF STATUTORY LANGUAGE

Perhaps the most disconcerting aspect of the Section 215 metadata program to some surveillance scholars, beyond the sheer volume of information that was collected about hundreds of millions of Americans' domestic communications, is that a common sense reading of Section 215 does not support the government's interpretation that such broad, indiscriminate collection is permissible.<sup>47</sup> Indeed, one lawmaker who was an author of the PATRIOT Act has stated, "the government must request specific records relevant to its investigation . . . . To argue otherwise renders the provision meaningless . . . . It's like scooping up the entire ocean to guarantee you catch a fish."<sup>48</sup> The government's interpretation of intelligence authorities, where we have come to expect (if not accept) a lack of transparency with respect to the type and scope of collection allowed

---

<sup>44</sup> See *MMI Research Ltd v. Cellxion Ltd. & Ors.*, [2009] EWHC (Pat) 418, [140] (Wales), <http://www.bailii.org/ew/cases/EWHC/Patents/2009/418.html> ("The [signal] strength of the simulated cell is maintained at a stronger value than the [signal] strength of the authentic network cells detected by the mobile to be tapped. When the mobile to be tapped begins to set up a call, the false cell, as the most powerful station, receives a request for a channel.").

<sup>45</sup> See Strobel, *supra* note 34, at 5 ("The IMSI Catcher is an expensive device to identify, track and tap a mobile phone user in such a way, that even the network operator cannot notice anything.").

<sup>46</sup> Although the focus of this essay is on certain legal and policy implications surrounding law enforcement collection of *metadata* via a StingRay, it is also worth noting that StingRay technology is capable of intercepting communications *content*. It remains unclear, however, which law enforcement agencies, if any, use such intercept capabilities during surveillance operations. See Harris GCSO Price List, *supra* note 36, at 4 (listing an optional "Sting[R]ay GSM intercept software package" for sale).

<sup>47</sup> See Brief of Amicus Curie, Professors of Information Privacy and Surveillance Law, *supra* note 11, at 9 ("The government acknowledges that the vast majority of data collected under the Verizon Order has not been relevant to any investigation, and its argument that the NSA can assess relevance on its own after the data are collected violates the plain language of § 215.").

<sup>48</sup> Jennifer Valentino-Devries and Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, WALL ST. J., July 8, 2013, [http://online.wsj.com/article\\_email/SB10001424127887323873904578571893758853344-1MyQjAxMTAzMDAwNzEwNDcyWj.html](http://online.wsj.com/article_email/SB10001424127887323873904578571893758853344-1MyQjAxMTAzMDAwNzEwNDcyWj.html) (quoting Rep. Sensenbrenner).

under various statutes, is not, however, the only area where such opacity exists. The StingRay, a surveillance technology that is used not only by the intelligence community, but also by the military and law enforcement agencies,<sup>49</sup> raises some of the same transparency issues. Indeed, the StingRay's capacity for invasive surveillance (i.e. sending signals through walls and into homes<sup>50</sup> and overbroad collection of innocent third party information<sup>51</sup>) could well provoke the same kind of surprise and dismay with respect to the government's interpretation of the Pen/Trap statute as sufficiently authorizing its use. This Part will describe those issues after first discussing real-time cell phone tracking as an example of how surveillance methods can fall into interpretive gaps within and between statutes.

### A. Real-time Cell Phone Tracking and Secrecy

In the context of criminal investigations, there are only two statutory authorities that explicitly authorize the interception of communications information in real-time: the Wiretap Act<sup>52</sup> and the Pen/Trap statute.<sup>53</sup> Consequently, when the government wants to use a new surveillance

---

<sup>49</sup> See John Kelly, *Cellphone data spying: It's not just the NSA*, USA TODAY, Dec. 8, 2013, <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> (“Initially developed for military and spy agencies, the Sting[R]ays remain a guarded secret by law enforcement and the manufacturer, Harris Corp. of Melbourne, Fla.”)

<sup>50</sup> These devices send signals like those emitted by a carrier's own base stations. See, e.g., Harris Corp. Product Sheet 1, [http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris\\_StingRay.pdf](http://servv89pn0aj.sn.sourcedns.com/~gbpprorg/2600/Harris_StingRay.pdf) (“Active interrogation capability emulates base station.”). Those signals, of course, “penetrate walls” (necessarily, to provide connectivity indoors). See *What You Need to Know About Your Network*, AT&T, <http://www.att.com/gen/press-room?pid=14003>; see also E.H. Walker, *Penetration of Radio Signals Into Buildings in the Cellular Radio Environment*, 62 THE BELL SYS. TECH. J. 2719 (1983), <http://www.alcatel-lucent.com/bstj/vol62-1983/articles/bstj62-9-2719.pdf>.

<sup>51</sup> See *infra* Part II.

<sup>52</sup> 18 U.S.C. §§ 2511–2520 (2012) (authorizing the interception of wire, oral or electronic communications—including communications content—by law enforcement to investigate crimes enumerated in the statute upon satisfying various elements set out in the statute).

<sup>53</sup> 18 U.S.C. §§ 3121–3127 (2012) (authorizing law enforcement to install and use a pen register device to “recor[d] or decod[e] . . . [non-content] dialing, routing, addressing, or signaling information . . . transmitted by an instrument or facility for which a wire or electronic communication is transmitted [or] provided” and to install and use a trap and trace device to “captur[e] the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication”).

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

method to collect data in real-time, it must first determine whether the technology or acquisition method fits under these existing statutory collection authorities. It must also conduct a Fourth Amendment analysis in order to determine if a search warrant must first be obtained. Cell phone location tracking represents one example of how the government analyzes and implements a real-time law enforcement collection method that has not been explicitly authorized by Congress.

It has already been described in the literature<sup>54</sup> and documented to a recent Congress<sup>55</sup> that nothing in the Electronic Communications Privacy Act (ECPA), which includes both the Wiretap Act and Pen/Trap statute,<sup>56</sup> articulates a legal standard Congress intended the government to meet before acquiring real-time cellular location data (i.e. tracking a mobile

---

<sup>54</sup> See Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L. J. 117, 134-35 (2012) (explaining how “[l]ocating the proper law enforcement access standard for prospective location data in the current law is, in some respects, like the quest for the Holy Grail, the search for the fountain of youth, or the hunt for a truly comfortable pair of high heels—one is unlikely to find them”); see also Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. REV. 589, 606–09 (2007) (analyzing how the Wiretap Act and Pen/Trap statute do not provide the requisite authority for such “tracking” and the Stored Communications Act (SCA) only authorizes retrospective access to previously stored communications content and non-content information).

<sup>55</sup> See *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 82-83 (2010) [hereinafter *Location Hearing*], [http://judiciary.house.gov/hearings/printers/111th/111-109\\_57082.pdf](http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf) (written statement of Judge Stephen Wm. Smith, U.S. Magistrate Judge, describing the difficulty he and other magistrate judges experienced in determining the proper law enforcement access standard for real-time location information: “Moreover, none of the other categories of electronic surveillance seemed to fit. The pen register standard was ruled out by a proviso in a 1994 statute known as CALEA. The wiretap standard did not apply because CSI does not reveal the contents of a communication. The Stored Communications Act (SCA) standard did not seem to apply for two reasons: the definition of ‘electronic communication’ specifically excludes information from a tracking device; and the structure of the SCA was inherently retrospective, allowing access to documents and records already created, as opposed to prospective real time monitoring.”).

<sup>56</sup> Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.). This Article uses the term ECPA to describe the first three titles of the Electronic Communications Privacy Act: Title I (“Interception of Communications and Related Matters”), 100 Stat. at 1848, which amended the Wiretap Act (codified as amended at 18 U.S.C. §§ 2511–2520 (2012)); Title II (“Stored Wire and Electronic Communications and Transactional Records Access”), commonly referred to as the Stored Communications Act (SCA) (codified as amended at 18 U.S.C. §§ 2701–2712 (2012)); and Title III (“Pen Registers and Trap and Trace Devices”), commonly referred to as the Pen/Trap Devices statute, (codified as amended at 18 U.S.C. §§ 3121–3127 (2012)).

device in real-time) from a carrier. Indeed, the only hint from Congress suggesting a standard for law enforcement access to real-time location data is found in the Communications Assistance for Law Enforcement Act (CALEA), whose limited prescription instructs that “any information that may disclose the physical location of [a telephone service] subscriber” may not be acquired “solely pursuant to the authority for pen registers and trap and trace devices.”<sup>57</sup> So CALEA points only to the insufficiency of a Pen/Trap order to support a government request for real-time or “prospective” (as opposed to “historical”) location data. It provides, however, no specific affirmative guidance as to what level of process would provide sufficient support.

Left without explicit direction from Congress, DOJ created the controversial “hybrid-order” theory by stitching together the elements of a Pen/Trap order and an 18 U.S.C. § 2703(d) order for the disclosure of stored electronic communications found in ECPA’s Stored Communication’s Act (SCA).<sup>58</sup> Since at least 2005, criminal investigators have applied for both types of orders from judges when seeking to compel carriers to track a cellular phone in real-time.<sup>59</sup> Over time, however, some magistrate judges have accepted this hybrid theory and some have not. Those who have rejected the hybrid theory have required law enforcement agents to apply for a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure.<sup>60</sup>

The appropriate standard for law enforcement access to real-time location data is, however, still an open question for both Congress and the courts. In the interim, a patchwork of non-binding magistrate and district court decisions has emerged,<sup>61</sup> with only one federal circuit court addressing the issue.<sup>62</sup> For now, the state of the law can be described fairly as a chaotic, “inconsistent legal landscape” that provides no clarity for law enforcement, courts, criminal defense attorneys or those citizens and advocacy organizations interested the protection of privacy.<sup>63</sup>

---

<sup>57</sup> 47 U.S.C. § 1002(a)(2) (2012).

<sup>58</sup> See Pell & Soghoian, *supra* note 26, at 135-36.

<sup>59</sup> *Id.*

<sup>60</sup> See *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005); *In re E.D.N.Y. Application*, 396 F. Supp. 2d 294, 322 (E.D.N.Y. 2005).

<sup>61</sup> See Pell & Soghoian, *supra* note 26, at 137-41.

<sup>62</sup> See *United States v. Skinner*, 690 F.3d 772 (2012) (explaining that the defendant did not have a reasonable expectation of privacy in the location that his cell phone was broadcasting, i.e., “the data given off by . . . his phone.”). *Id.* at 777.

<sup>63</sup> Pell & Soghoian, *supra* note 26, at 140.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

Scholars and some courts have criticized the hybrid theory on a number of grounds, ranging from its constitutionality<sup>64</sup> to whether, notwithstanding the constitutional question, Congress would have intended to permit the government's joining of historical and real-time surveillance statutes to authorize law enforcement access of real-time location data.<sup>65</sup> Absent better direction from Congress with respect to the appropriate standard for law enforcement access to real-time location data, the government would need, however, to arrive at some view of the appropriate process to follow when engaging in this form of surveillance. Considering that DOJ has used the hybrid theory to acquire real-time location data since at least 2005, that wireless carriers receive tens of thousands of court orders requiring the disclosure of location data per year,<sup>66</sup> and that, to date, there is still no real clarity in the law, it is fair to argue that judicial review has not adequately tested whether the government's hybrid theory: (1) fully complies with the Fourth Amendment;<sup>67</sup> (2) is consistent with congressional intent; or even (3) is consistent with the plain meaning of the relevant statutes.

Magistrate Judge Stephen Wm. Smith, an early critic of warrantless real-time tracking,<sup>68</sup> offers an important perspective on why appellate

---

<sup>64</sup> See Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 677, 717 (2011) (arguing that courts should require a warrant for access to location data in all cases because such acquisition is a search under the Fourth Amendment).

<sup>65</sup> *In re* E.D.N.Y. Application, 396 F. Supp. 2d 294, 322 (E.D.N.Y. 2005); see also *In re* W.D.N.Y. Application, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2005) (“[T]he challenge here is to the *statutory* justification for . . . [the government’s] application. . . . The Court does not agree with the government that it should impute to Congress the intent to ‘converge’ the provisions of the Pen Statute, the SCA, and CALEA to create a vehicle for disclosure of prospective cell information on a real time basis on less than probable cause.”).

<sup>66</sup> Letter from Sprint to Rep. Edward J. Markey, Co-Chairman, Congressional Bipartisan Privacy Caucus 10 (May 23, 2012), <http://web.archive.org/web/20121110192245/http://markey.house.gov/sites/markey.house.gov/files/documents/Sprint%20Response%20to%20Rep.%20Markey.pdf> (“Over the past five years, Sprint has received . . . 196,434 court orders for location information.”).

<sup>67</sup> One Circuit has held, however, that a defendant does not have a reasonable expectation of privacy in the real-time location broadcasted by his cell phone, at least with respect to his movements along public thoroughfares. In this case, the government obtained court orders (but apparently not a warrant) to “ping” the defendant’s phone. *Skinner*, 690 F.3d at 776-781.

<sup>68</sup> See *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Authority (*In re* 2005 S.D. Tex. Application), 396 F. Supp. 2d 747, 753–64 (S.D. Tex. 2005) (rejecting the government’s “hybrid theory” and finding that compelled disclosure of prospective cell site data is more akin to the tracking device placed under a vehicle, as defined in 18 U.S.C. § 3117 (defining a tracking device as “an electronic or mechanical

review of real-time location tracking and other types of government surveillance subject to ECPA is a rare occurrence: for the most part, the government is the *only* party with the ability and potential incentive to appeal unfavorable judgments.<sup>69</sup> ECPA surveillance orders are issued *ex parte* and often remain sealed long past an investigation's end.<sup>70</sup> A target of a sealed ECPA order is thus unlikely to become aware of the government's acquisition of her information unless an investigation proceeds to charges. It is at that point, as a criminal defendant, that a target can challenge the ECPA order. If an investigation never proceeds to an indictment, the innocent target will never learn that a third party disclosed her information to the government.<sup>71</sup> Moreover, while the third party provider receives the order compelling disclosure of information, such disclosure order is often accompanied by a gag order.<sup>72</sup> The third party provider could challenge the gag order, as well as the primary disclosure order, but instances where companies have "pushed back" against law enforcement ECPA orders in criminal investigations have not, to date, resulted in a steady stream of appellate court review.<sup>73</sup> In sum, as Judge Smith observes, "[t]hrough a potent mix of indefinite sealing, nondisclosure (i.e. gagging), and delayed-notice provisions, ECPA surveillance orders all but vanish into a legal void."<sup>74</sup>

The issues identified by Judge Smith lend discomfiting credence to Justice Alito's recent observation that, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."<sup>75</sup> But for the legislature to act, it must, at a minimum, have accurate information about how government agencies interpret their existing surveillance authorities, as well as the nature of new, unregulated surveillance technologies now in use. Judge Smith notes that, although the location tracking of cell phones first came to Congress' attention in 1994, nearly two decades have passed without any amendment to ECPA

---

device which permits the tracking of the movement of a person or object.")); *see also* 18 U.S.C. § 3117(b) (2012).

<sup>69</sup> Stephen Wm. Smith, *Gagged, Sealed and Delivered: Reforming ECPA's Secret Docket*, 6 HARV. L. & POL'Y REV. 313, 323-29 (2012).

<sup>70</sup> *Id.* at 315.

<sup>71</sup> *See* Memorandum and Order, No. 10-291-M-01 (D.D.C. Nov. 1, 2010), <https://www.dcd.uscourts.gov/dcd/sites/dcd/files/mag10-291.pdf> (holding that the notice requirements in Rule 41 are satisfied by notifying the email provider, rather than the target of the surveillance order).

<sup>72</sup> Smith, *supra* note 69, at 323.

<sup>73</sup> *Id.* at 328.

<sup>74</sup> *Id.* at 314.

<sup>75</sup> *United States v. Jones*, 132 S. Ct. 945, 964 (2012).

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

clarifying the appropriate law enforcement access standard.<sup>76</sup> While there is rarely one reason for why Congress is or is not able to pass legislation on a particular issue, one important factor affecting Congress' ability to legislate in the area of law enforcement access to location data is that Congress has not had current, accurate data on the nature and extent of cell phone surveillance for many years.<sup>77</sup> As we will discuss below, the StingRay presents even greater challenges to transparency and congressional awareness of government surveillance.

### *B. The StingRay and Secrecy*

Much less is known about law enforcement use of StingRays in criminal investigations than is known about more traditional cell phone location tracking. What little is known comes mostly from a limited number of magistrate judge opinions, a tenacious criminal defendant seeking discovery in his own prosecution,<sup>78</sup> and a few obscure DOJ guidance documents.<sup>79</sup> This section discusses DOJ's interpretation of the Pen/Trap statute as authorizing law enforcement use of StingRays. It argues that, given the StingRay's powerful, unmediated and largely indiscriminate surveillance capabilities, a common sense reading of the text does not

---

<sup>76</sup> Smith, *supra* note 69, at 316.

<sup>77</sup> *Id.* Indeed, public information about the scale of location requests by law enforcement was not available to Congress until 2012 when then Representative (now Senator) Ed Markey received data from wireless carriers. *See, e.g.,* Pell & Soghoian, *supra* note 26, at 158-59 (noting that during the time Congress was considering reforms to ECPA in 2010—in contrast to information about Wiretap and Pen/Trap surveillance—Congress did not “even have a sense of the number and scope of law enforcement requests for location information”). Of the carriers that provided data to then Rep. Markey, only Sprint provided specific numbers about law enforcement requests for location data. *See* Letter from Sprint to Rep. Edward J. Markey, *supra* note 66 (“[O]ver the past five years, Sprint has received . . . 196,434 court orders for location information.”). Additional carrier responses are available at *Markey Letters to Wireless Carriers on Law Enforcement Requests*, WEBPAGE OF SEN. EDWARD MARKEY, [http://www.markey.senate.gov/Markey\\_Letters\\_to\\_Wireless\\_Carriers.cfm](http://www.markey.senate.gov/Markey_Letters_to_Wireless_Carriers.cfm) (last visited Dec. 16, 2013).

<sup>78</sup> *See* United States v. Rigmaiden, 2013 WL 1932800 (D. Ariz. May 8, 2013). The government prosecuted Rigmaiden for his role in a scheme in which he allegedly obtained fraudulent tax refunds for hundreds of deceased persons and third parties. Law enforcement agents used a StingRay device to identify Rigmaiden as the alleged perpetrator of these crimes. In the course of pre-trial discovery and motion practice, Rigmaiden, a pro-se defendant, filed substantial discovery requests and motions to suppress evidence, some of which related to the government's use of a StingRay. *See* Order, *United States v. Rigmaiden*, Case 2:08-cr-00814-DGC, (No. 1009) (Mar. 08, 2013) (on file with the Journal).

<sup>79</sup> *See supra* Part II.

provide adequate notice to legislators that the Pen/Trap statute purportedly authorizes law enforcement use of a StingRay in criminal investigations. Such lack of notice, when compounded with the propensity for ECPA orders to vanish into a legal void<sup>80</sup> without revealing how DOJ and magistrate judges are interpreting surveillance authorities, severely restricts (even undermines) the ability of Congress to conduct meaningful oversight of government surveillance and to regulate new surveillance technologies and methods.

The crux of our argument is not that it is impossible to read the plain text of the Pen/Trap statute as being applicable to the StingRay but that, as collection capabilities expand in power and scope (as we have seen occur with the NSA's domestic telephony data collection program), government lawyers may interpret the text of statutes to authorize greater surveillance powers than a plain reading of the text would disclose or suggest. Moreover, through examining two magistrate court opinions discussing StingRay technology, we will illustrate the limited ability magistrate judges have to restrain government power when there is no statute directly authorizing or limiting a surveillance method or technology. First, however, we will discuss the parameters of the Pen/Trap statute itself.

The Pen/Trap statute authorizes law enforcement agencies, upon obtaining a Pen/Trap order from a court, to compel providers to disclose, in real-time, various types of transactional information pertaining to wire or electronic communications.<sup>81</sup> The statute references a "telephone line or other facility to which the pen register or trap and trace is to be attached or applied,"<sup>82</sup> and the standard for such issuance is extraordinarily low.<sup>83</sup> Indeed, the government need only certify that the information "likely to be obtained is relevant to an ongoing criminal investigation."<sup>84</sup>

Assuming that the magistrate judge finds that the Pen/Trap statute authorizes the kind of collection that the government seeks, then, upon such

---

<sup>80</sup> See Smith, *supra* note 69, at 314.

<sup>81</sup> See 18 U.S.C. §§ 3121-3124 (2012) (defining the relevant transactional information as "dialing, routing, addressing, and signaling information used in the processing and transmitting of wire or electronic communications" (Section 3121); describing the Pen/Trap application process (Section 3122); explaining the circumstances and standards governing a court's issuance of a Pen/Trap order (Section 3123); and mandating requirements for third party assistance for installation of a Pen/Trap order (Section 3124)).

<sup>82</sup> 18 U.S.C. § 3123(b)(1)(A) (2012).

<sup>83</sup> Location Hearing, Written Statement of Judge Smith, *supra* note 55, at 92 Exhibit A (illustrating the Pen/Trap standard as the lowest of standards found in the surveillance statutes requiring court approval).

<sup>84</sup> 18 U.S.C. §§ 3122(b)(2), 3123(a)(1) (2012).

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

certification, the court must grant the application.<sup>85</sup> It is for this reason that at least one circuit court has characterized the role of magistrate judges in such instances as being “ministerial in nature.”<sup>86</sup> In other words, when granting the Pen/Trap order, the magistrate does not examine or analyze whether there are sufficient facts to support the government’s certification that the information sought is relevant to an ongoing criminal investigation.

The Pen/Trap statute arguably authorizes the government to compel production of a broad array of both telephony and Internet data.<sup>87</sup> While DOJ’s public manual on “Searching and Seizing Computers” does not give a detailed list of all of the specific types of transactional information that can be obtained with a Pen/Trap Order, it notes that the statute’s reference to “dialing, routing, addressing [and/or] signaling information” encompasses almost *all* non-content information in a communication.<sup>88</sup>

Given the broad array of real-time data that the Pen/Trap statute appears to authorize the government to compel from a third party provider, does a plain reading of the statute suggest that it also authorizes law enforcement to use a sophisticated technological device to impersonate a cell site operated by the target’s cellular provider and collect such

---

<sup>85</sup> See 18 U.S.C. § 3123(a) (“Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.” (emphasis added)).

<sup>86</sup> *United States v. Fregoso*, 60 F.3d 1314, 1320 (8th Cir. 1995) (“The judicial role in approving use of trap and trace devices is ministerial in nature.”).

<sup>87</sup> The statute defines the non-content data that the government can acquire with a Pen/Trap order as “dialing, routing, addressing, and signaling information used in the processing and transmitting of wire or electronic communications.” 18 U.S.C. § 3121(c).

<sup>88</sup> Computer Crime and Intellectual Prop. Section, Criminal Div., *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, U.S. DEP’T OF JUSTICE, at 154 (3rd ed. 2009) [hereinafter DOJ Manual] (emphasis added). <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>. With respect to telephony metadata, the Electronic Frontier Foundation (EFF) has interpreted the scope of the DOJ’s statement to include: the numbers a phone calls and receives; the starting and ending of each call; the duration of each call; whether each call was connected or went to voicemail; and (although a disputed, controversial use of Pen/Trap) “post-cut-through dialed digits” (digits after a call is connected, like a banking PIN number or a prescription refill number). With respect to Internet metadata, EFF speculates that the Pen/Trap statute may authorize real-time collection of addresses of sent and received email; the time each email is sent or received; the size of each email that is sent or received; IP (Internet Protocol) addresses to include IP addresses of other computers a target computer exchanges information with, as well as the communications ports and protocols used (which, in turn, can be used to determine the types of communications sent and the types of applications used). See “*Pen Registers*” and “*Trap and Trace Devices*,” EFF SURVEILLANCE SELF-DEFENSE BLOG, <https://ssd.eff.org/wire/govt/pen-registers>.

information, without the assistance of a third party? Moreover, does a plain reading of the statute suggest that law enforcement is authorized to use a device that may, in the process of collecting data about a target's device, also collect data about a significant number of innocent third parties, depending on how the device is used?<sup>89</sup> In posing these questions, we are moving beyond a mere inquiry as to whether the statute conceivably authorizes this type of surveillance to ask whether legislators are on notice that the statute can be, and is being, interpreted to authorize surveillance that potentially impacts so many innocent people.

### 1. *The 1995 Digital Analyzer Magistrate Opinion*

The first published opinion (and one of only a few that are public) that helps to address some of these questions came in 1995, when Magistrate Judge Edwards took the position that no authority, including the Fourth Amendment, either authorizes or limits the government's use of a far more rudimentary predecessor of the StingRay<sup>90</sup>—a device commonly referred to as a “digital analyzer” or “TriggerFish.”<sup>91</sup>

In this case, the government applied for a Pen/Trap order to employ a digital analyzer to intercept the signals from cellular phones used by five named subjects in a criminal investigation.<sup>92</sup> Magistrate Judge Edwards found, however, that because the digital analyzer was not intended to be, nor could it be, physically attached to the cellular phone, the Pen/Trap statute was not applicable to its use.<sup>93</sup> Judge Edwards also found, pursuant

---

<sup>89</sup> See John Kelly, *Cellphone data spying: It's not just the NSA*, USA TODAY, Dec. 8, 2013, <http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/> (“Typically used to hunt a single phone's location, the system intercepts data from all phones within a mile, or farther, depending on terrain and antennas.”)

<sup>90</sup> Whereas the StingRay actively interacts with cellular phones and sends signals into the homes of the target and anyone else in the vicinity, the Triggerfish passively intercepts and decodes the signals sent between cellular base stations and phones. See generally Pell & Soghoian, *supra* note 25.

<sup>91</sup> *In re* Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. 197 (C.D. Cal. 1995). The government submitted an *ex parte* application for an order permitting agents of the Orange County Regional Narcotics Suppression Program (“RNSP”) to use a digital analyzer. *Id.* at 198-99.

<sup>92</sup> The agents likely needed to use this technology because they did not know the particular phone numbers of the devices that the targets were using, *id.* at 199, and thus could not seek more specific surveillance assistance from their wireless carriers.

<sup>93</sup> The court further explained its reasoning:

The statutory definition of a ‘trap and trace device’ does not include the limitation in the definition of a pen register described above, limiting the devices to those that are attached to a telephone line. See 18 U.S.C.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

to *Smith v. Maryland*,<sup>94</sup> that the government’s use of a digital analyzer raised no Fourth Amendment concerns.<sup>95</sup> This ruling was consistent with DOJ’s position, first publically documented in 1997, that neither the Fourth Amendment nor any statutory authority prohibited its use of the digital analyzer, as long as the acquisition of non-content data did not involve the assistance of carriers.<sup>96</sup> While not a legal requirement, DOJ still advised prosecutors to seek a Pen/Trap order when using a digital analyzer as a Pen/Trap device. Thus, in 1995, it appears DOJ sought court authorization via the Pen/Trap statute merely “out of an abundance of caution.”<sup>97</sup>

---

§ 3127(4). Nonetheless, it appears from the construction of related sections of the statutes governing trap and trace devices that they include only devices that are attached to a telephone line. Specifically, 18 U.S.C. § 3123(b) requires that an order for use of both pen registers and trap and trace devices include ‘the number and, if known, physical location of the telephone line to which the pen register or trap and trace device is to be attached. . . .’ This limitation on the proscription against pen registers and trap and trace devices to prohibit only devices that are ‘attached’ to a telephone line cannot be assumed to be inadvertent. In other statutes relating to interceptions of telephone communications, Congress encompassed, generally, any types of interceptions of wire, oral, or electronic communications—regardless of whether the intercepting device was ‘attached’ to a telephone line. *See, e.g.*, 18 U.S.C. § 2511. That Congress did not impose equally comprehensive restrictions on lesser interceptions that do not raise 4th Amendment issues, such as those made with pen registers and trap and trace devices, is neither surprising nor inconsistent. In any event, it must be remembered that the prohibition against the use of pen registers and trap and trace devices without court order is found in a criminal statute. *See* 18 U.S.C. § 3121(d). Under well-settled principles, the statute should be strictly construed, and any ambiguity in its scope must be construed narrowly.

*Id.* at 200.

<sup>94</sup> 442 U.S. 735 (1979).

<sup>95</sup> *In re* Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. at 199. The court noted that “[n]umbers dialed by a telephone are not the subject of a reasonable expectation of privacy . . . [and] no logical distinction is seen between telephone numbers called and a party’s own telephone number (or [device serial] number), all of which are regularly voluntarily exposed and known to others.” *Id.*

<sup>96</sup> *See* Executive Office for United States Attorneys, *Electronic Investigative Techniques*, USA BULLETIN, Sept. 1997, at 13-15, [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usab4505.pdf](http://www.justice.gov/usao/eousa/foia_reading_room/usab4505.pdf) (“it does not appear that there are constitutional or statutory constraints on the warrantless use of such a [digital analyzer] device.”).

<sup>97</sup> *In re* Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer, 885 F. Supp. at 200.

Although ultimately ruling that the Pen/Trap statute did not regulate—and thus did not prohibit—government use of a digital analyzer, the judge expressed serious reservations about its capabilities and use. Specifically, the judge expressed concern about the potential intrusion upon the privacy of innocent third parties. That is, if the court authorized the government to use a digital analyzer to identify the particular phones used by known targets, such an order would essentially permit agents to sweep the relevant surrounding areas and intercept signals emitted from *all* phones in those areas. Indeed, Judge Edwards recognized that “depending upon the effective range of the digital analyzer, telephone numbers and calls made by others than the subjects of the investigation could be inadvertently intercepted.”<sup>98</sup> Moreover, although the agents were not seeking to intercept communications content, the digital analyzer was capable of being used for that purpose.<sup>99</sup>

The court also noted that its authorization could permit the government to collect data about large numbers of phones without any recordkeeping or reporting requirements, thus preventing effective congressional oversight of the surveillance tool.<sup>100</sup> The court contrasted this lack of record production with the statutory reporting requirements to Congress in the Pen/Trap statute, such as “the use of court orders that identified particular telephones and the investigative agency” and “periodic reports to Congress stating the numbers of such orders.”<sup>101</sup> Noting these differences and others,<sup>102</sup> the court stated that the government’s application “would not insure sufficient accountability.”<sup>103</sup>

The court’s reasoning appears to illustrate broader concerns about a circumvention of congressional authority that would occur if the court

---

<sup>98</sup> *Id.* at 201.

<sup>99</sup> See *Electronic Investigative Techniques*, *supra* note 96, at 14 (“Although [a digital analyzer] device is also capable of intercepting both the numbers dialed from the cellular phones and the voice (wire) communications to and from cellular telephones, the digital analyzer is programmed so it will not intercept cellular conversations or dialed numbers when it is used for the limited purpose of seizing ESNs and/or the cellular telephone’s number.”); see also Electronic Surveillance Unit, *Electronic Surveillance Manual: Procedures and Case Law Forms*, U.S. DEP’T OF JUSTICE 40 (2005), <http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf> (“Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.”).

<sup>100</sup> *In re Application of the United States of America for an Order Authorizing the Use of a Cellular Telephone Digital Analyzer*, 885 F.Supp. at 201-02.

<sup>101</sup> *Id.* (citing 18 U.S.C. §§ 3123(b), 3126).

<sup>102</sup> *Id.*

<sup>103</sup> *Id.* at 201.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

granted the government’s request, even “in an abundance of caution.” By granting an order pursuant to a statute whose definitional elements did not conform to the surveillance technique at issue, the court risked giving: (1) a potentially incorrect interpretation of a statute; or worse (2) judicial approval of a surveillance technique that Congress appeared neither explicitly to authorize or prohibit under the statutory authority presented in the government’s application—all without the corresponding accountability mechanisms that Congress mandated in the statute cited in the government’s application.

Though it expressed concern about the surveillance capabilities of this technology, the court could not restrain its use by law enforcement. Ironically, the court’s denial of the government’s application likely reinforced DOJ’s stance that it did not need any court authorization for future use of a digital analyzer.<sup>104</sup> At least in this instance, however, it was clear to the court exactly *what* it was being asked to authorize. A more recent opinion suggests that courts are being asked to grant applications for the use of StingRays in criminal investigations without appropriate knowledge about what the technology actually does—information that is necessary to determine both whether the Pen/Trap statute authorizes its use and whether the use of a StingRay constitutes a search under the Fourth Amendment.

### 2. 2012 *StingRay* Magistrate Opinion

By 2005, if not earlier, DOJ had adopted the position that the Pen/Trap statute, as amended by the 2001 PATRIOT Act, “appears to encompass all of the non-content information passed between a cell-phone and the provider’s tower.”<sup>105</sup> Accordingly, DOJ advised prosecutors to seek a Pen/Trap order for all non-content data that agents acquired directly.<sup>106</sup> This was a significant change to DOJ’s earlier 1997 guidance, which had interpreted the law to permit unmediated surveillance (e.g. performed directly via cellular surveillance technology rather than with the assistance of carriers) without the necessity of a Pen/Trap or other court order.

In 2012, a federal magistrate judge from Texas issued an order denying an application submitted by agents from the Drug Enforcement Agency for the use of a StingRay.<sup>107</sup> The case involved a surveillance target

<sup>104</sup> See *Electronic Investigative Techniques*, *supra* note 96, at 14.

<sup>105</sup> See *2005 Electronic Surveillance Manual*, *supra* note 99, at 45.

<sup>106</sup> *Id.* at 47-48.

<sup>107</sup> *In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*, 890 F. Supp. 2d 747, 748 (S.D. Tex. 2012).

that switched from using a phone known to agents to an unknown phone.<sup>108</sup> The government therefore sought a Pen/Trap order “to detect radio signals emitted from wireless cellular telephones in the vicinity of the [Subject] that identify the telephones.”<sup>109</sup> The agents submitted their application pursuant to the Pen/Trap statute<sup>110</sup> and 18 U.S.C. § 2703(c)(1), a provision of ECPA’s Stored Communications Act,<sup>111</sup> and the government informed Magistrate Judge Owsley that it was “based on a standard application model and proposed order approved by [DOJ].”<sup>112</sup>

Since the subject was known to law enforcement (whereas the phone number the target was using was unknown), agents planned to identify the phone by capturing device identification data “at various locations in which the [subject’s] telephone [would] reasonably [be] believed to be operating.”<sup>113</sup> After reviewing the application, the judge conducted an *ex parte* hearing where an agent leading the investigation indicated that the “equipment designed to capture the cell phone numbers was known as a [S]ting[R]ay.”<sup>114</sup>

Ultimately, the court denied the government’s application.<sup>115</sup> Judge Owsley expressed concern that the application did not adequately explain the technology or “how many distinct surveillance sites they intend[ed] to use, or how long they intend[ed] to operate the [S]ting[R]ay equipment to gather all telephone numbers in the immediate area.”<sup>116</sup> Moreover, the court noted that no explanation was given, either in writing or verbally, as to what would be done with the “innocent . . . information” collected from the phones of uninvolved individuals who just happened to be in the vicinity of

---

<sup>108</sup> *Id.*

<sup>109</sup> *Id.*

<sup>110</sup> 18 U.S.C. §§ 3122(a)(1), 3127(5) (2012).

<sup>111</sup> It is not clear from the 2012 magistrate opinion what purpose this citation to ECPA’s Stored Communications Act served in terms of providing additional authority of unmediated, direct collection of non-content data in this investigation. The 2005 Guidance indicated that only a Pen/Trap order was required for use of devices to collect non-content data directly. *See 2005 Electronic Surveillance Manual, supra* note 99, at 47-48. DOJ may, however, have provided updated guidance reflecting a different or more nuanced legal position. As of the writing of this Article this new guidance, if it exists, is not publically available. The citation to the Stored Communications Act does have a strange similarity to the prospective location data “hybrid order.” *See* discussion *supra* Part III.A.

<sup>112</sup> *In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 749 (S.D. Tex. 2012).

<sup>113</sup> *Id.* at 748.

<sup>114</sup> *Id.*

<sup>115</sup> *Id.* at 752.

<sup>116</sup> *Id.* at 749.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

the surveillance target.<sup>117</sup> Finally, the court expressed concern that neither the prosecutor nor the DEA agent appeared to understand the technology at issue and “seemed to have some discomfort in trying to explain it.”<sup>118</sup>

At a 2013 symposium at Yale Law School, Judge Owsley suggested that:

The practice of the feds’ not making clear the planned use of a StingRay when seeking surveillance authorization could be widespread. . . . I may have seen them before and not realized what it was, because what they do is present an application that looks essentially like a pen register application . . . . So any magistrate judge that is typically looking at a lot of pen register applications and not paying a lot of attention to the details may be signing an application that is authorizing a Sting[R]ay.<sup>119</sup>

Indeed, a StingRay or similar tracking device appeared to be used in a case that made its way to the Seventh Circuit.<sup>120</sup> Because the circuit court opinion and underlying district court opinion<sup>121</sup> never refer to such a device, whether by a specific or generic name or other identifying description, the only real indication that the Pen/Trap order authorized law enforcement use of a StingRay-type device was through DOJ’s disclosure of a copy of the opinion in response to a Freedom of Information Act (FOIA) request

---

<sup>117</sup> *Id.*

<sup>118</sup> *Id.*

<sup>119</sup> Ryan Gallagher, *Feds Accused of Hiding Information From Judges About Covert Cellphone Tracking Tool*, SLATE, Mar. 28, 2013, [http://www.slate.com/blogs/future\\_tense/2013/03/28/StingRay\\_surveillance\\_technology\\_used\\_without\\_proper\\_approval\\_report.html](http://www.slate.com/blogs/future_tense/2013/03/28/StingRay_surveillance_technology_used_without_proper_approval_report.html); see also Jennifer Valentino-Devries; Jennifer Valentino-Devries, *‘Stingray’ Phone Tracker Fuels Constitutional Clash*, WALL ST. J., Sept. 22, 2011, <http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html> (reporting that when a prosecutor was asked by the judge how a court order or warrant could be obtained without telling the judge what technology was being used, the prosecutor responded “it was standard practice, your honor”).

<sup>120</sup> *United States v. Amaral-Estrada*, 509 F.3d 820, 822 (7th Cir. 2007) (explaining that “the DEA sought and received a court order from a magistrate judge for the application and use of a pen register and trap-and-trace device, and to determine certain telephone information using the cellular telephone number on Sosa-Verdeja’s phone.”).

<sup>121</sup> *United States v. Bermudez, et al.*, 2006 WL 3197181, at \*1 (S.D. Ind. June 30, 2006) (explaining that “by using an electronic device and the cellular site information obtained based on a court order signed by Magistrate Judge Foster, [a law enforcement officer] was able to pinpoint the multi-unit residence located at 5352 West Deming Place as the precise location of a particular cell phone”).

regarding StingRay devices filed by one of this Article's authors.<sup>122</sup> Moreover, additional documents obtained from an ACLU FOIA request indicate that Pen/Trap applications presented to magistrate judges in the Northern District of California did not make law enforcement's intended use of StingRays "explicit."<sup>123</sup>

Notwithstanding his broader concerns, Judge Owsley's decision to deny the application appears to stem from a definitional problem he identified in the Pen/Trap statute that, ultimately, the government did not adequately address. While recognizing that the PATRIOT Act broadened the Pen/Trap definitions, "amplify[ing] the various types of information that are available such as routing and signaling information,"<sup>124</sup> Judge Owsley read language contained in Section 3123(b)(1) of the statute as "straightforward in that a telephone number or similar identifier is *necessary* for a pen register."<sup>125</sup> Accordingly, he found that the language in the statute "mandate[s] that this Court have a telephone number or some similar identifier before issuing an order authorizing a pen register."<sup>126</sup> Because the government did not provide any support to the contrary suggesting that the statute authorized collection of non-content data from *unidentified* devices, Judge Owsley denied the application without prejudice.<sup>127</sup>

#### IV. WARNINGS FOR LEGISLATORS

Together, these two magistrate opinions (one pre- and the other post-PATRIOT Act) raise questions as to whether the Pen/Trap statute can properly be interpreted as authorizing the use of a StingRay or similar

<sup>122</sup> Letter from Kenneth Courter, Acting Chief, FOIA/PA Unit, Criminal Division, U.S. Dep't of Justice, to Christopher Soghoian (Sept. 30, 2013) <http://files.cloudprivacy.net/stingray-FOIA-7th-Circuit-doc.pdf>.

<sup>123</sup> See email from Miranda Kane to USACAN-Attorneys-Criminal, U.S. Dep't of Justice (May 23, 2011, 11:55 AM),

[https://www.aclu.org/files/assets/doj\\_emails\\_on\\_stingray\\_requests.pdf](https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf) (indicating that magistrate judges in the Northern District of California raised collective concerns about whether a pen register is sufficient to authorize use of StingRay and TriggerFish technology that simulates a cell tower and can be placed inside a van to help pinpoint an individual's location with and that the Pen/Trap applications presented to magistrates were not making law enforcement's intended use of the technology "explicit").

<sup>124</sup> *In re* Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747, 751 (S.D. Tex. 2012).

<sup>125</sup> *Id.* (emphasis added).

<sup>126</sup> *Id.*

<sup>127</sup> *Id.* at 751-52.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

unmediated surveillance technology to acquire non-content communications data. Beyond parsing the statutory language, however, these opinions illustrate how the government seeks to accommodate the use of new and powerful surveillance technologies through aggressive interpretation of existing statutory language that neither directly authorizes nor prohibits their use.

More critically, for legislators looking at how they can create or improve a process for regulating and overseeing law enforcement use of new surveillance technologies and collection methods, the 1995 digital analyzer opinion illustrates the limited ability a magistrate judge has to constrain government surveillance that is neither authorized nor prohibited directly by statutory language. The court's sense of futility is manifest in the conundrum of whether it is appropriate to authorize government use of a new technology merely "in an abundance of caution." By denying the government's Pen/Trap application essentially on the grounds that it was unnecessary, Judge Edwards likely reinforced DOJ's view that no form of judicial oversight was necessary for law enforcement use of the surveillance technology. While this may have been the appropriate legal answer, it raises significant oversight concerns.

As previously indicated, when a digital analyzer or StingRay collects data, no corresponding third party records are created—the information intercepted is in the sole possession of the agents using the StingRay.<sup>128</sup> If there is no judicial oversight, then there is no trace or record of StingRay surveillance in a particular case other than law enforcement's own elective record keeping systems. While it is not impossible for the information to surface as part of the discovery process of a criminal prosecution,<sup>129</sup> such disclosures would depend on how discovery rules were applied in particular cases. In other words, records production in the context of the criminal discovery process is not a solid, reliable avenue for legislators to learn, in a timely fashion, about law enforcement use of new surveillance technologies and government legal interpretations supporting their use.

Conversely, the 1995 digital analyzer opinion also illustrates how congressional authority and oversight can be short circuited if a court, "in an abundance of caution," grants an application for use of a new invasive surveillance technology when that method is not directly authorized by statute and is not apparent to a legislator through a common sense reading of the statutory text. In this instance, a court risks giving judicial imprimatur to a new surveillance technology in the context of a system in which, as

---

<sup>128</sup> See *supra* Part II.

<sup>129</sup> See *United States v. Rigmaiden*, 2013 WL 1932800 (D. Ariz. May 8, 2013).

Judge Smith has explained, appellate review of ECPA *ex parte* surveillance orders is rare.<sup>130</sup> The appellate process is thus unlikely to expose law enforcement use of the technology or government interpretations of the statutes purportedly authorizing such use within anything approaching a timely notice period that would facilitate either congressional oversight or legislative action.<sup>131</sup> Moreover, as Judge Owsley has noted, it is possible that magistrate judges have authorized law enforcement use of StingRays in various cases without even knowing or understanding what they were authorizing. If true, this practice adds an additional layer of complication to congressional notice and oversight, since only elements of the Executive branch may know about law enforcement use of new surveillance technologies in criminal investigations.

## V. SUGGESTIONS FOR REFORM

After many months of almost weekly disclosures about classified NSA intelligence programs, we have begun to understand how, at times, government agencies will interpret statutory language to authorize bulk, indiscriminate collection in a way that is not apparent from a plain reading of the statutory text. While some members of Congress were aware of this type of collection in the context of the Section 215 metadata program, we have argued that the StingRay has significantly expanded the government's surveillance capabilities in criminal investigations while it has, nevertheless, gone largely unnoticed and unregulated. Indeed, a plain reading of the Pen/Trap statute would not put a legislator on sufficient notice that the government was interpreting the statute to authorize StingRay surveillance.<sup>132</sup> While we are not suggesting that no congressional

---

<sup>130</sup> See *supra* Part III.A.

<sup>131</sup> See discussion, *supra*, Part III.A.

<sup>132</sup> DOJ's conclusion that Pen/Trap now encompasses all non-content data between a cell phone and a cell tower relies, in part, on its analysis of the relevant but "scant" legislative history which suggested that the new definitions were intended to apply to "all communications media, instead of focusing on traditional telephone calls." *2005 Electronic Surveillance Manual*, *supra* note 99, at 46. Examining, for example, House language referencing "a packet requesting a telnet session—a piece of information passing between machines in order to establish a communication session for the human user," DOJ suggests that the term "provides a close analogy to the information passing between a cell phone and the nearest tower in the initial stages of a cell phone call." *Id.* at 46-47. Moreover, in contrast to earlier Pen/Trap definitions that referenced the attachment of a Pen/Trap device to a phone line, the House Report recognized that Pen/Trap devices could "collect information remotely." *Id.* at 47. We find it difficult to conclude from DOJ's analysis of this "scant" legislative history that Congress had specific and sufficient notice regarding

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

staffer or Member of Congress is aware of the StingRay family of technologies and their capabilities, there is no public evidence that Congress has formally evaluated the privacy implications of law enforcement use of such unmediated, indiscriminate surveillance methods.<sup>133</sup> Moreover, given the scant number of published cases illustrating a court's analysis and interpretation of statutes that may authorize law enforcement use of the StingRay family of technologies, it would be unrealistic to expect judicial review to facilitate meaningful notice to Congress in anything approaching a timely fashion.<sup>134</sup> The StingRay, therefore, illustrates a larger gap in congressional oversight insofar as new, invasive surveillance technologies and collection methods not directly authorized by Congress can be used, often for decades, without any reliable notice to Congress about their use. Simply put, before Congress can begin to regulate new surveillance technologies and methods, it must have some notice of their nature and actual or likely use. An authoritative, reliable mechanism is needed to produce information that can provide such notice.

As part of the Administration's response to the summer 2013 Snowden disclosures, which began with the revelation of the 215 metadata program, President Obama announced his intention to convene an outside group of experts to conduct a full review of NSA surveillance programs and issue a report about how these programs impact security, privacy and foreign policy.<sup>135</sup> This expert panel has since issued its report, which provided, among other things, recommendations about possible reforms to

---

the privacy implications of the StingRay and, in amending the Pen/Trap statute, knowingly authorized law enforcement use of this technology.

<sup>133</sup> The one exception we know of is a January 28, 2014 public State Congressional oversight hearing (meeting) in the Minnesota House of Representatives House Civil Law Committee that explored state and local law enforcement use of cellular interception devices. See Minn. H.R. Civil Law Committee Audio & Video Archives, [http://www.house.leg.state.mn.us/audio/archivescomm.asp?comm=88003&ls\\_year=88](http://www.house.leg.state.mn.us/audio/archivescomm.asp?comm=88003&ls_year=88). The hearing took place because a bi-partisan group of State legislators' concerns about the technology were not satisfied by written correspondence from the Minnesota Public Safety Commissioner. See Camey Thibodeau, *Cell Phone Tracking Devices Available to Police*, FARIBAULT DAILY NEWS, Feb. 4, 2014, [http://www.southernminn.com/faribault\\_daily\\_news/news/local/article\\_b6719fc2-2656-51c4-89e3-861e6179b2fe.html](http://www.southernminn.com/faribault_daily_news/news/local/article_b6719fc2-2656-51c4-89e3-861e6179b2fe.html) ("Privacy concerns related to the devices were addressed at an oversight hearing held this week by the Minnesota House Civil Law Committee.").

<sup>134</sup> See cell phone location tracking discussion, *supra* Part II.A.

<sup>135</sup> See *Transcript: President Obama's August 9, 2013 news conference at the White House*, WASH. POST, Aug. 9, 2013, [http://articles.washingtonpost.com/2013-08-09/politics/41225505\\_1\\_civil-liberties-oversight-board-open-debate-surveillance-programs](http://articles.washingtonpost.com/2013-08-09/politics/41225505_1_civil-liberties-oversight-board-open-debate-surveillance-programs) (outlining steps, post-Snowden disclosures, to foster debate and reform of intelligence collection programs including the President's intent to convene an outside group of experts to review surveillance technologies and capabilities).

the Section 215 metadata program.<sup>136</sup> A far more detailed report focusing on the Section 215 metadata program was subsequently released by the Privacy and Civil Liberties Oversight Board (PCLOB).<sup>137</sup> The PCLOB is an independent, bi-partisan Executive Branch agency authorized by Congress in the context of the “war on terrorism” to ensure, among other things, that “liberty concerns are appropriately considered in the development and implementation of laws, regulations, and policies related to efforts to protect the Nation against terrorism.”<sup>138</sup>

While Congress has currently authorized PCLOB oversight only of government efforts to protect the nation from terrorism (and the recent PCLOB report on Section 215 and the operations of the FISC is part of that oversight effort), there is no impediment to congressional expansion of the PCLOB’s mandate to review, advise, and counsel more generally on surveillance technologies and methods that permeate current criminal investigations (or those that could reasonably be predicted to do so in the future), even if they do not necessarily relate to government efforts to protect the Nation against terrorism. Congress could, for example, task the PCLOB with studying the specific surveillance technologies and methods that are in use or reasonably likely to be used by various law enforcement agencies in criminal investigations and the legal authorities the government believes authorizes or, conversely, does not prohibit their use. The goal of such an assessment should be the production of written recommendations by the PCLOB to Congress specifying which technologies are in need of

---

<sup>136</sup> Notably, the report recommended that bulk records collected under the 215 metadata program should no longer be held by the government, but rather, by a private third party. See LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT’S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 25 (2013), <http://www.lawfareblog.com/wp-content/uploads/2013/12/Final-Report-RG.pdf>.

<sup>137</sup> See *supra* note 8. The PCLOB’s Chairman, David Medine, when referring to the summer 2013 disclosures stated that “Our [the PCLOB’s] challenge is to understand exactly how these programs work, but speak about them publicly in a way that Americans can understand the programs and evaluate them. We will work in some cases to have information declassified, if it permits us a greater opportunity to explain how these programs work . . . . Our view is to try to enhance counterterrorism efforts but also enhance Americans’ privacy and civil liberties.” Cogan Schneier, *Privacy and Civil Liberties Board Works to Inform Public on NSA Leaks*, FED. NEWS RADIO, July 25, 2013, <http://www.federalnewsradio.com/411/3400357/Privacy-and-Civil-Liberties-board-works-to-inform-public-on-NSA-leaks>.

<sup>138</sup> 42 U.S.C. § 2000(c)(2) (2012). Some aspects of the PCLOB’s report pertaining to the Section 215 metadata program and dissenting views from two PCLOB Members are discussed in the Introduction and accompanying footnotes.

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

direct authorization or prohibition, and which statutory authorities need to be updated and amended to accommodate or prohibit their use.

In service of this goal, Congress should further direct the PCLOB to write public reports at regular intervals (which could also, if necessary, include non-public or classified addenda) making such recommendations and directly identifying privacy issues associated with law enforcement's use of new surveillance technologies or collection methods, as well as old technologies like the StingRay, whose current or likely future use gives rise to new privacy concerns.<sup>139</sup> Moreover, for purposes of conducting the investigation and analysis leading to its written recommendations, Congress should both direct and empower the PCLOB to talk with all relevant government agencies, surveillance technology manufacturers, outside technologists and any other parties or entities that would provide relevant information.<sup>140</sup>

The StingRay and its capabilities invoke several important questions that should guide the PCLOB in making recommendations about technologies and methods Congress should regulate directly. This brief list is illustrative, though in no sense exhaustive, of some inquiries the PCLOB should consider:

- (1) Is the technology or technique in question invasive of common and legal conceptions of personal privacy?;

---

<sup>139</sup> We would suggest that once Congress expands PCLOB's mandate and authorizes additional funding and staff for this purpose, PCLOB be given a year to produce the first report, followed by intervals of three years for new reports so that, following the first report, there is a sufficient period of time to assess how law enforcement may be using new technologies or collection methods and the privacy implications associated with such use.

<sup>140</sup> Under current statutory authority, for example, the PCLOB has the power to: "procure the temporary or intermittent services of experts and consultants," 42 U.S.C. § 2000(j)(3); "have access from any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element, to all relevant records, reports, audits, reviews, documents, papers, recommendations, or other relevant material, including classified information consistent with applicable law;" "interview, take statements from, or take public testimony from personnel of any department, agency, or element of the executive branch, or any Federal officer or employee of any such department, agency, or element;" "request information or assistance from any State, tribal, or local government" and; "at the direction of a majority of the members of the Board, submit a written request to the Attorney General of the United States that the Attorney General require, by subpoena, persons (other than departments, agencies, and elements of the executive branch) to produce any relevant information, documents, reports, answers, records, accounts, papers, and other documentary or testimonial evidence." *Id.* at § 2000(g)(1)(A)-(D).

- (2) Does it challenge a common-sense understanding of the statutory text that the government interprets to authorize its use?;
- (3) Is it an indiscriminate collection method that intercepts data from innocent cell phones in the coverage area of the mobile device being targeted?;
- (4) Is it an unmediated surveillance method that leaves no trace of its use beyond internal government agency records?; and
- (5) Might it, without such oversight or other regulation, otherwise remain hidden from any degree of public perception or scrutiny?

These questions suggest what we would describe as a minimal examination of the privacy implications and potential need for regulation of law enforcement use of any new technology or novel technique, particularly an unmediated surveillance device like the StingRay. The lines of inquiry encompass the interaction between a specific surveillance technology or technique and relevant cultural norms regarding the expectation of privacy, the specific legal interpretations the government would employ to support its use, the scope of the data collection involved, as well as the physical index, if any, present during its use and the record or trace, if any, it leaves afterwards.

## **VI. CONCLUSION**

Knowledge and perception must precede oversight. Congress cannot understand or regulate a surveillance technology it cannot “see” clearly, whether through conceptual understanding of its operation before the fact or actual analysis of the history of its use. The StingRay is a law enforcement surveillance technology that has, for nearly two decades, evaded direct congressional scrutiny, much less informed authorization or regulation. Moreover, the StingRay illustrates how law enforcement agencies can use surveillance technologies and methods, justified by expansive and potentially problematic interpretations of existing statutes, for years before they ever come to the attention of Congress—if they ever do. We have thus argued that an authoritative, reliable procedure must be established to put Congress on notice about the functions, capabilities and historical use, if any, of new surveillance technologies and methods if the law is ever to keep pace with technological change. As they are for the

## A LOT MORE THAN A PEN REGISTER, AND LESS THAN A WIRETAP

newest of technologies, the need for such procedures is applicable even to decades-old technologies like the StingRay, whose expanding surveillance capabilities, combined with its increasing frequency of use by law enforcement at ever-descending costs,<sup>141</sup> invoke privacy implications not heretofore appreciated.

Indeed, we are entering an era where law enforcement agencies have the technical capability to hack into the computers and phones of surveillance targets, allowing them covertly to activate webcams and microphones, search through documents, and obtain a person's web browsing history.<sup>142</sup> These capabilities have been acquired and used without

---

<sup>141</sup> For a discussion of the declining costs of cellular interception technology and corresponding frequency of use by law enforcement, see generally Pell & Soghoian, *supra* note 25.

<sup>142</sup> See Jennifer Valentino-DeVries and Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J., Aug. 3, 2013, <http://online.wsj.com/article/SB10001424127887323997004578641993388259674.html> (“Law-enforcement officials in the U.S. are expanding the use of tools routinely used by computer hackers to gather information on suspects . . . . With such technology, the bureau can remotely activate the microphones in phones running Google Inc.’s Android software to record conversations, one former U.S. official said. It can do the same to microphones in laptops without the user knowing.”); see also Craig Timberg and Ellen Nakashima, *FBI’s search for ‘Mo,’ Suspect in Bomb Threats, Highlights Use of Malware for Surveillance*, WASH. POST, Dec. 6, 2013, [http://www.washingtonpost.com/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98\\_story.html](http://www.washingtonpost.com/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html) (“Such high-tech search tools, which the FBI calls “network investigative techniques,” have been used when authorities struggle to track suspects who are adept at covering their tracks online. The most powerful FBI surveillance software can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers, say court documents and people familiar with this technology. . . . The FBI has been able to covertly activate a computer’s camera — without triggering the light that lets users know it is recording — for several years, and has used that technique mainly in terrorism cases or the most serious criminal investigations, said Marcus Thomas, former assistant director of the FBI’s Operational Technology Division in Quantico.”); see also Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED, Sept. 13, 2013, <http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/> (“[T]he FBI yesterday acknowledged that it secretly took control of Freedom Hosting last July, days before the servers of the largest provider of ultra-anonymous hosting were found to be serving custom malware designed to identify visitors. . . . Security researchers dissected the [FBI] code and found it exploited a security hole in Firefox to identify users of the Tor Browser Bundle, reporting back to a mysterious server in Northern Virginia.”).

For examples of actual court documents pertaining to law enforcement hacking, see Search Warrant Application, 1:12-sw-05685-KMT (D. Colo. Oct. 9, 2012) (application from the ATF for a warrant seeking permission to use a “Network Investigative Technique” to remotely search the computer of an individual believed to be making bomb threats); *In re*

16 YALE J.L. & TECH. 134 (2013)

2013-2014

any public congressional hearings or other open debate, much less any explicit legislative mandate. As it hints at technological disruptions to come and how the legal disorder they bring may unfold, the StingRay offers strong evidence that now is the time to establish a reliable mechanism that will be a continuous source of useful guidance to Congress as more powerful surveillance tools emerge and evolve to challenge the very notion of privacy as they strengthen the ability of the government to monitor and control the lives of its citizens. For more new and powerful surveillance tools shall certainly emerge in the coming age than are “dreamt of in [our] philosophy” of personal privacy or its current practical expression in our laws.<sup>143</sup>

---

Warrant to Search a Target Computer at Premises Unknown, No. H-13-234M (S.D. Tex. Apr. 22, 2013), <http://files.cloudprivacy.net/Order%20denying%20warrant.MJ%20Smith.042213.pdf> (court order denying an application from the FBI to surreptitiously install data extraction software on the computer of a target). Reporter Jennifer Valentino-Devries noted that “[t]he judge’s order said the data the FBI could obtain includes ‘search terms that the user entered into any Internet search engine, and records of user-typed Web addresses.’ The government also is seeking email contents, documents and chat-messaging logs on the computer, as well as to take photographs for 30 days using the computer’s built-in camera, the document states.” *Judge Denies FBI Request to Hack Computer in Probe*, WALL ST. J., Apr. 24, 2013, <http://online.wsj.com/article/SB10001424127887324743704578443011661957422.html>.<sup>143</sup> “There are more things in heaven and earth Horatio, Than are dreamt of in your philosophy.” WILLIAM SHAKESPEARE, *HAMLET* act 1, sc. 5.