Volume 119 | Issue 3 Article 6

April 2017

Stingray Technology, The Exclusionary Rule, and the Future of Privacy: A Cautionary Tale

Shawn Marie Boyne
Indiana University School of Law

STINGRAY TECHNOLOGY, THE EXCLUSIONARY RULE, AND THE FUTURE OF PRIVACY: A CAUTIONARY TALE

*Shawn Marie Boyne**

I. INTRODUCTION

Sometime in 2017, smartphone ownership in the United States will exceed 222 million users, which will be equivalent to a market penetration rate of over 85%.[1] Although millions of individuals in the United States enjoy the convenience of using smartphones, it is likely that few of those citizens understand that government agencies have used those same phones to track the location of individuals in real time as well as to access the significant and

* Shawn Marie Boyne is a Professor of Law at Indiana University's Robert H. McKinney School of Law. She is a graduate of the University of Wisconsin-Madison (Ph.D.), Justus-Liebig-Universität (L.L.M.), the University of Southern California (J.D.), and Cornell University (B.A.). She would like to thank Melanie Reid for inviting her to participate in a panel at SEALS 2016 and the staff of the *West Virginia Law Review.*

[1] Greg Sterling, *Smartphone Ownership Just Shy of 80 Percent [comScore]*, MARKETINGLAND (Mar. 3, 2016, 8:49 PM), http://marketingland.com/167275-167275.

previously private information stored on those devices without a warrant. The public's general lack of awareness of the intrusiveness of current law enforcement surveillance is but one factor responsible for creating this knowledge gap. Another root of the gap, however, is that the judicial institutions that we entrust with protecting our rights cannot preemptively adjust constitutional doctrines to parallel technological change.[2] Indeed, judicial institutions have typically adopted a cautious approach to adjusting constitutional doctrines to technological developments. For example, although Apple introduced the iPhone in January 2007, it took seven years for the Supreme Court to hold that government agents must obtain a warrant to search smartphones seized incident to arrest.[3]

Many scholars viewed the decision in *Riley v. California* as a victory in the battle to protect privacy interests in an age in which technology has dramatically changed not only how we communicate with each other, but also in how we acquire and store knowledge both about ourselves, but also the world.[4] However, the trajectory of post-*Riley* decisions troublingly demonstrates that the decision has not constrained the State's appetite for obtaining cellphone data.[5] Most notably, police may still access cellphone data without a warrant if they can argue that the exigent circumstances exception to the Fourth Amendment applies.[6] A larger problem lies with the limits of the exclusionary rule itself. Evidence obtained illegally may only be suppressed if the State files criminal charges, discloses that evidence, and actually intends to use that evidence at trial.[7] In addition, because the rule itself is not found in the Constitution, but rather is a judicial creation, the Supreme Court has the power to craft exceptions to the rule itself. In addition, if the State conducts a search without the knowledge of the individual being searched, it is possible that a suspect will never discover that the police built their case on the foundation of an illegal search. Put another

---

2 Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 502, 531 (2011) (arguing that courts cannot keep up with technological change).

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

4 *See, e.g.*, Richard M. Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUSBLOG (Jun. 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/.

5 Adam M. Gershowitz, *The Post-*Riley *Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 590 (2016) (arguing that magistrate judges continue to issue broad warrants that authorize a search of the entire contents of the phone with no restrictions whatsoever or have authorized searches of applications and data for which no probable cause existed).

6 In *Riley*, the Court noted that the government did not argue that the exigent circumstances doctrine applied. *Riley*, 134 S. Ct. at 2494 n.2.

7 Melanie D. Wilson, *An Exclusionary Rule for Police Lies*, 47 AM. CRIM. L. REV. 1, 24 (2010) (stating that the Supreme Court has continued to narrow the exclusionary rule's application to focus on only those criminal cases where the exclusion of evidence will deter police conduct).

way, courts will only apply the fruit of the poisonous tree doctrine if the defendant "finds" the poisonous tree. Finally, the exclusionary rule does not protect us in situations where state agencies elect to acquire information and use that information for a non-criminal use.[8]

One might argue that the limits of the exclusionary rule, as well as the rule's narrowing scope, has facilitated the weakening of privacy rights in the age of hand-held computers. As cellphone manufacturers have worked to improve the storage capacities and processing speeds of smartphones, government agencies have increasingly taken steps to acquire technology that will access the data stored on those devices.[9] Today, many federal, state, and local law enforcement agencies possess specialized technology that allows those agencies to remotely search cellphone data without the phone's user even knowing that the search occurred.

Using so-called StingRay tracking devices, government agencies may track the location of a particular cellphone, access content such as text messages, as well as record phone conversations.[10] By mimicking the signals emitted by cellphone towers, these briefcase-sized devices "catch" the international mobile subscriber identity ("IMSI") of cellphones within a certain distance from the device.[11] Using the IMSI, government employees may also find out who is paying for a particular phone's service and download data captured from voice communications, texts, and other data "stored" on that phone onto a computer.[12] Federal agencies began using advanced technology to capture cell phone signals in the mid-1990s, and since then state and local police agencies have begun to use the technology even in routine criminal investigations.[13] According to a 2014 report in the *Wall Street Journal,* the federal government currently uses Cessna

---

8 Catherine Y. Hancock, *The Exclusionary Rule, in Investigation and Police Practices Twenty-Eighth Annual Review of Criminal Procedure: I,* 87 GEO. L.J. 1097, 1253 (1999) (stating that the exclusionary rule is a judicially constituted remedy used in criminal cases to suppress evidence obtained by the government in violation of the Fourth, Fifth, and Sixth Amendments to establish the defendant's guilt).

9 Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force,* 81 MISS. L.J. 1229, 1231 (2012) (stating that law enforcement is quick to exploit the enhanced capabilities that new technologies provide to access data).

10 Kim Zetter, *Turns Out Police StingRay Spy Tools Can Indeed Record Calls*, WIRED (Oct. 28, 2015, 3:00 PM), https://www.wired.com/2015/10/StingRay-government-spy-tools-can-record-calls-new-documents-confirm/.

11 For purposes of simplicity, I will use the StingRay name to identify all forms of IMSI catchers. Other popular brands include: Triggerfish, KingFish, AmberJack, Harpoon, and Hailstorm.

12 Zetter, *supra* note 10.

13 Declan McCullagh, *FBI Prepares to Defend "'Stingray" Cell Phone Tracking*, CNET (Mar. 27, 2013, 4:57 PM), https://www.cnet.com/news/fbi-prepares-to-defend-StingRay-cell-phone-tracking/.

airplanes that can cover most of the American population to gather cellphone data.[14]

Currently, law enforcement agencies in at least 23 states, as well as 13 federal agencies, use StingRay devices to track cellphone locations and access cellphone data.[15] Despite their intrusive capabilities, to use these devices, law enforcement officers in most states need only to obtain a low-level court order called a PEN register, also known as a "trap and trace," to obtain permission for their use.[16] The development and deployment of this technology by the government enables agencies to indiscriminately search all cellphones within a certain radius of the devices.[17] Even in cases where the information may enable the police to target a specific criminal defendant, it may be difficult for a defense counsel to find out whether the police actually used the technology. For this reason, the warrantless use of these devices seriously threatens individual privacy rights and, arguably, our First Amendment rights.

Although both the FBI and the Department of Homeland Security currently require their employees to obtain a search warrant before using the StingRay technology, in many states, law enforcement agencies use the technology without a warrant.[18] In many cases where investigators have actually secured a warrant to snoop on cellphones, the affidavit written in support of the warrant has only vaguely referred to some type of trap and trace device failing to inform courts that the device permits police to conduct broad sweeps of cellphone users in the absence of probable cause.[19] In addition, news reports suggest that government agencies have begun to use the technology to monitor and harass individuals exercising their First Amendment rights. Activists claim to have detected StingRay use at the Dakota Pipeline Access protests in North

---

[14] Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, WALL ST. J. (Nov. 13, 2014, 8:22 PM), http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533?tesla=y&mg=reno64-wsj.

[15] *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/StingRay-tracking-devices-whos-got-them (last visited Apr. 6, 2017).

[16] Nicky Woolf & William Green, *IRS Possessed Stingray Cellphone Surveillance Gear, Documents Reveal*, GUARDIAN (Oct. 26, 2015 8:25 AM), https://www.theguardian.com/world/2015/oct/26/stingray-surveillance-technology-irs-cellphone-tower.

[17] *Id.*

[18] Sascha Meinrath & Jeff Landale, *Opinion: The FCC Needs to End Warrantless Cellphone Spying*, CHRISTIAN SCI. MONITOR (Nov. 30, 2016), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/1130/Opinion-The-FCC-needs-to-end-warrantless-cellphone-spying.

[19] Robert Kolker, *What Happens When the Surveillance State Becomes an Affordable Gadget?*, BLOOMBERG BUSINESSWEEK (Mar. 10, 2016 11:05 AM), http://www.bloomberg.com/news/articles/2016-03-10/what-happens-when-the-surveillance-state-becomes-an-affordable-gadget.

Dakota,[20] Black Lives Matter protests in Chicago,[21] as well as the protests in Baltimore in response to Freddie Gray's death.[22]

Although our Founders crafted the Fourth Amendment to limit the government's ability to intrude on individual privacy rights, in key ways, advancements in technology have critically undercut the Amendment's ability to accomplish that objective. Moreover, the weakness of the Fourth Amendment's analytical framework, in particular the Supreme Court's use of a balancing test framed around the concept of reasonableness, may ultimately threaten not just our privacy rights, but also First Amendment rights as well.[23] As government agencies acquire personal information without probable cause, and in many cases without a target's knowledge, it threatens not only our privacy, but our basic autonomy as well. Consistent with the development of Fourth Amendment case law, the front lines of the battle to restrict the State's use of technology to pierce our privacy are located in the nation's courtrooms.

Consider the recent decision of the Seventh Circuit Court of Appeals in case of *United States v. Patrick*.[24] In that case, the court held that police did not violate the defendant's Fourth Amendment right to privacy when they "found" Patrick by using a StingRay device. Like other similar cases,[25] when law enforcement agents approached a magistrate judge to obtain a warrant prior to the defendant's arrest, the agents did not inform the court about the nature of the technology they intended to deploy. In fact, the defendant did not even learn that law enforcement officers had used the device to find him until after his appellate counsel had filed his initial brief. Although it is tempting to blame the secrecy surrounding the use of the device on the malevolent intent of law enforcement officers, court filings and FOIA requests indicate that manufacturers of these devices have required state agencies to sign non-disclosure agreements prior to

---

20 Larae Meadows, *Dead End Surveillance—StingRays and Civil Rights*, NATIVE NEWS ONLINE.NET (Oct. 7, 2016), http://nativenewsonline.net/currents/dead-end-surveillance-StingRays-civil-rights/.

21 Fruzsina Eördögh, *Evidence of "StingRay" Phone Surveillance by Police Mounts in Chicago*, CHRISTIAN SCI. MONITOR (Dec. 22, 2014), http://www.csmonitor.com/World/Passcode/2014/1222/Evidence-of-StingRay-phone-surveillance-by-police-mounts-in-Chicago.

22 Ian Duncan, *FBI Admits Providing Air Support to Baltimore Police During Freddie Gray Unrest*, BALT. SUN (May 7, 2015), http://www.baltimoresun.com/news/maryland/crime/bal-fbi-admits-providing-air-support-to-baltimore-police-during-freddie-gray-unrest-20150506-story.html.

23 David D. Cole, *Preserving Privacy in a Digital Age: Lessons of Comparative Constitutionalism*, *in* FERGAL DAVIS, NICOLA MCGARRITY & GEORGE WILLIAMS, SURVEILLANCE, COUNTER-TERRORISM AND COMPARATIVE CONSTITUTIONALISM 95–116, 104 (New York: Routledge 2013).

24 No. 13-CR-234, 2015 WL 106158 (E.D. Wis. Jan. 7, 2015), *aff'd*, 842 F.3d 540 (7th Cir. 2016).

25 McCullagh, *supra* note 13.

using the devices.[26] In some cases, prosecutors have either dropped pending charges or offered lenient plea deals to keep the technology secret.[27]

In Part I of this Article, I will highlight the evolution of the use of StingRay technology in criminal investigations in the United States and the efforts by privacy rights organizations to elevate the standard of judicial scrutiny of those devices. In Part II, I examine two ground-breaking 2016 court decisions in which courts, for the first time, suppressed evidence obtained through the use of cell-site simulator technology. Although *United States v. Lambis*[28] is the first instance where a federal court suppressed StingRay-related evidence, the decision of the Maryland Court of Special Appeals in *State v. Andrews*,[29] is the first state appellate decision to uphold a trial court's cell-site simulator technology-related suppression order. Finally, in Part III, I will argue that the history of the government's use of cell-site simulator ("CSS") technology demonstrates that in a common law system restricted to litigating current cases and controversies, the judicial branch standing alone cannot adequately protect individual privacy rights.

II. THE BUMPY ROAD OF JUDICIAL AND LEGISLATIVE OVERSIGHT

One key feature of the American judicial system is that courts may only rule on the cases and controversies currently before them. Although this prohibition constrains judicial power, in an age of rapidly developing surveillance technology this constraint also allows law enforcement agencies to deploy new technology before a court rules on the legality of that technology. It may take years before attorneys have the knowledge, resources, and interest to challenge the use of that technology in court.[30] Even when that challenge is filed, because of the limits on the exclusionary rule, a decision may not change the outcome of a conviction. Consider the Supreme Court's opinion in *Riley v.*

---

[26] Jose Pagliery, *FBI Lets Suspects Go to Protect "'StingRay" Secrets*, CNN TECH (Mar.18, 2015, 3:15 PM), http://money.cnn.com/2015/03/18/technology/security/police-StingRay-phone-tracker/.

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

[28] 197 F. Supp. 3d 606 (S.D.N.Y. 2016).

[29] 134 A.3d 324 (Md. Ct. Spec. App. 2016).

[30] Statistics show that more than 80% of those charged with felonies are indigent and thus rely on the representation of public defenders. Because of excessive caseloads and underfunding, 95% of criminal cases result in a plea bargain. Alexa Van Brunt, *Poor People Rely on Public Defenders Who Are Too Overworked to Defend Them*, GUARDIAN (Jun 17, 2015, 7:30 AM), https://www.theguardian.com/commentisfree/2015/jun/17/poor-rely-public-defenders-too-overworked.

California.[31] While scholars and the media lauded the Court's decision to require law enforcement to secure a warrant before searching a cellphone seized incident to an arrest, the decision did not set the defendant free.[32] In this Part, I will highlight the reasons why government agencies have been able to use CSS technology in criminal investigations for over two decades with little effective judicial oversight. Section A discusses how law enforcement agencies hid the use of CSS technology for decades from judicial review. In Section B, I discuss the pivotal efforts of Daniel Rigmaiden, a pro se defendant, who used his time in pretrial detention to file numerous discovery requests in an effort to obtain information on the use of CSS technology. Finally, Section C discusses the 2015 policy change made by the Federal Bureau of Investigation ("FBI") which now requires agents to secure a warrant to authorize the use of CSS technology in most cases.

A. The Shell Game

Although American courts have only recently begun to examine the issue of whether law enforcement agencies may use CSS technology without a warrant, the FBI began using that technology back in 1995.[33] There is some evidence to suggest that state and local police agencies were able to begin using the technology with little government oversight because the manufacturer mislead the Federal Communications Commission about the technology's capabilities and widespread use.[34] In addition, some law enforcement agencies, for example the Miami-Dade Police Department in Florida, only sought permission to use the devices after they had used the devices in the field.[35] A significant reason why agencies sought to keep the devices secret is that the manufacturer of the devices, the Harris Corporation and the FBI, forced agencies

---

31 134 S. Ct. 2473 (2014).

32 Kristina Davis, *Won Battle, Lost War in Cellphone Search Case*, SAN DIEGO UNION-TRIBUNE (Aug. 1, 2015, 11:00 AM), http://www.sandiegouniontribune.com/sdut-riley-cellphone-searches-warrants-gangs-ruling-2015aug01-htmlstory.html.

33 Kris Hermes, *Law Enforcement Uses StingRays to Spy on Americans and Lies About It*, HUFFINGTON POST (Sept. 26, 2016), http://www.huffingtonpost.com/kris-hermes/law-enforcement-uses-stin_b_12080634.html.

34 Nathan Freed Wessler & Nicole Ozer, *Documents Suggest Maker of Controversial Surveillance Tool Misled the FCC*, ACLU (Sept. 17, 2014, 10:15 AM), https://www.aclu.org/blog/documents-suggest-maker-controversial-surveillance-tool-misled-fcc?redirect=blog/national-security/documents-suggest-maker-controversial-surveillance-tool-misled-fcc.

35 *Id.* It is important to note that the FCC has little statutory power to regulate CSS devices. The sole basis of the agency's authority is a requirement that requires users to obtain a license to transmit signals and a prohibition against devices that cause "harmful interference" to cell service.

to sign non-disclosure agreements.[36] Despite the fact that the judicial branch plays an integral role in guarding the boundary between law enforcement activities and privacy in this country, the non-disclosure agreements sought to prohibit agencies from informing judicial officers that those agencies planned to use the technology.[37]

To maintain the secrecy required by these non-disclosure agreements, prosecutors and government agencies used applications for "pen register" or "trap and trace devices" to authorize the use of CSS technology instead of obtaining a search warrant.[38] Because pen register and trap and trace devices simply record the numbers of all outgoing[39] or incoming[40] calls, rather than collect the content of a call, in a number of cases government investigators obtained a court order without fully disclosing the full scope of their intended search or meeting the standard of probable cause required to obtain a search warrant.[41] Indeed, under the Electronic Communications Privacy Act, an applicant need only show that "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency" to obtain an order.[42] Although the Supreme Court held in *Smith v. Maryland* that individuals do not have an expectation of privacy in the phone numbers that they call or receive,[43] the information received by CSS technology is far more extensive and intrusive than the mere collection of phone numbers. In some cases involving StingRay devices, because law enforcement agencies were not forthright in disclosing the actual technology they sought to deploy, judges

---

36 *See, e.g.*, *Text of FBI Non-Disclosure Agreement for Harris Corporation StingRay*, CTR. FOR HUM. R. & PRIVACY (June 29, 2012), https://www.cehrp.org/text-of-fbi-non-disclosure-agreement-for-harris-corporation-stingray/.

37 *Id.* The agreement prohibited disclosure of the device "in press releases, in court documents, during judicial hearings, or during other public forums or proceedings." *Id.*

38 *See, e.g.*, Kim Zetter, *Police Contract With Spy Tool Maker Prohibits Talking About Device's Use*, WIRED (Mar. 14, 2014, 4:34 PM), https://www.wired.com/2014/03/harris-stingray-nda/ (claiming that the Tucson Police Department did not seek a warrant to use the device in over 200 cases).

39 "[T]he term 'pen register' means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3) (2012).

40 "[T]he term 'trap and trace device' means a device or process which captures 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." *Id.* § 3127(4).

41 *Pen Trap*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/pen-trap (last visited Feb. 27, 2017); *see also* 18 U.S.C. § 3123(a).

42 18 U.S.C. § 3122(b)(2).

43 442 U.S. 735, 743 (1979).

approved Pen Register Act requests without knowing that law enforcement officers intended to use CSS technology.[44]

A prime example of this strategy to hide the use of CSS technology can be found in *United States v. Patrick*.[45] At first glance, the facts of the case appeared to mirror those of a run-of-the-mill arrest. The case began when police in Milwaukee, Wisconsin, arrested Mr. Patrick during a traffic stop in a public place.[46] At the time of his arrest, a court had issued a warrant for his arrest on the grounds that he had violated the terms of his parole.[47] When police found Patrick, he had a semi-automatic weapon in his possession, despite the fact that he had previously been convicted of a felony. The U.S. Attorney's Office subsequently charged and convicted Patrick of one count of felon in possession of a firearm, contrary to 18 U.S.C. § 922(g)(1). Although Patrick's counsel moved to suppress the gun, a district court denied the motion after a pre-trial evidentiary hearing.[48] Curiously, the police reports used a series of ambiguous phrases to explain what information had led them to Patrick's location. The reports claimed that the police had "'obtained information' of Patrick's location; . . . had 'prior knowledge' that Patrick was occupying the vehicle; . . . [and] 'obtained information from an unknown source' that Patrick was inside the vehicle at that location."[49] According to a report from the Electronic Frontier Foundation, six months after the police arrested Patrick, the government "revealed they'd tracked him through his cellphone"[50] and "implied they'd gotten location information directly from the cellphone service provider."[51] When Patrick's attorney cross-examined a police officer at the evidentiary hearing, the officer stated that they had received "electronic information" about Patrick's location.[52] When questioned further about that information, the officer only revealed that it

---

44 According to emails obtained by the ACLU, police officers in Sarasota, Florida, would attribute the information obtained by CSS technology to an unnamed confidential informant. *See* Maria Kayanan, *Internal Police Emails Show Efforts to Hide Use of Cell Phone Tracking*, ACLU (June 19, 2014, 9:01 PM), https://www.aclu.org/blog/internal-police-emails-show-efforts-hide-use-cell-phone-tracking.

45 842 F.3d 540 (7th Cir. 2016).

46 *Id.* at 541–42.

47 *Id.*

48 *Id.*

49 Jennifer Lynch, *EFF and ACLU Expose Government's Secret Stingray Use in Wisconsin Case*, ELECTRONIC FRONTIER FOUND. (Apr. 22, 2016), https://www.eff.org/deeplinks/2016/04/eff-and-aclu-expose-governments-secret-stingray-use-wisconsin-case.

50 *Id.*

51 *Id.*; *see also* United States v. Patrick, No. 13-CR-234 (E.D. Wis. May 5, 2016) (denying defendant's Rule 33 motion), http://www.leagle.com/decision/In%20FDCO%2020160506E87/U.S.%20v.%20PATRICK#.

52 Lynch, *supra* note 49.

involved "tracking [a] cellphone."[53] Despite those disclosures, the court denied Patrick's motion to suppress. He pled guilty and preserved his right to appeal.[54]

It turned out that the government's disclosure in the district court proceedings were not completely accurate. After Patrick filed his opening brief in the Seventh Circuit, the American Civil Liberties Union ("ACLU") and the Electronic Frontier Foundation filed an amicus brief alleging that logs obtained from the Milwaukee Police Department showed that the police had used a StingRay on the day of Patrick's arrest.[55] The brief also detailed that the Milwaukee Police Department had signed a non-disclosure agreement with the manufacturer of the device in which the department agreed to dismiss any case if a court forced the state to reveal information about the device.[56] Ironically, only after the amicus brief was filed, did Patrick's counsel learn precisely how law enforcement officers had found the defendant.[57]

The problem with using applications for "pen register" or "trap and trace devices" to authorize the use of cell-site simulators is that by using CSS technology, law enforcement may collect more information than a list of phone numbers dialed or received by a particular phone number. Indeed, the technology allows investigators to obtain the numbers of all cellphones with a certain radius of the device, the location data of particular cellphones, and, in some cases, the content of phone calls themselves. One problem with using pen register orders to obtain judicial permission to use StingRay technology is that, in order to obtain such an order, federal law requires that law enforcement officers specify a particular telephone number or similar identifier. In most cases where law enforcement seeks to use CSS technology, the agents may only know a general location where a phone has been used and not know the particular number.

Despite the non-disclosure orders, it became more difficult to hide the use of the technology from defense counsel, nonprofit organizations, and the media. In some cases, in order to avoid disclosing information about the technology, prosecutors offered generous plea bargains.[58] In other cases, investigators seeking approval of pen register applications encountered resistance from federal magistrate judges. Notably, beginning in 2005, a number of magistrate judges held that law enforcement agents had to meet the higher standard of probable cause rather than the Pen Register Act's mere relevance

---

53 *Id.*

54 *Patrick*, No. 13-CR-234 (denying defendant's Rule 33 motion).

55 Lynch, *supra* note 49.

56 *Id.*

57 *Patrick*, No. 13-CR-234 (denying defendant's Rule 33 motion).

58 Jason M. Weinstein et al., *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729, 742 (2015) (describing a prosecutor who offered a generous plea deal to avoid disclosing information about the technology).

standard before using CSS technology.[59] However, the decisions in the federal courts were not unanimous in requiring that the State meet a probable cause standard.[60]

B. United States v. Rigmaiden

Surprisingly, it took the work of an obsessive and reclusive criminal, who represented himself pro se, to expose the fact that government agencies were using StingRay technology to find criminal suspects.[61] In 2008, federal agents arrested Daniel Rigmaiden who prided himself on living "off the grid." A grand jury later indicted Rigmaiden on 73 counts of fraud, identity theft, and conspiracy. After finding himself in federal custody, Rigmaiden filed numerous discovery requests and over 1000 motions as he attempted to discover how agents had found him.[62] Possessing a high school education and an innate sense of curiosity, Rigmaiden discovered how the government tracked his location using a device.[63] After Rigmaiden finally convinced the principal technologist

---

59 *See, e.g.*, *In re* Application of United States, 497 F. Supp. 2d 301, 304 (D.P.R. 2007); *In re* United States for an Order Authorizing the Release of Prospective Cell Site Information, 407 F. Supp. 2d 134, 134–35 (D.D.C. 2006); *In re* Application of the United States, No. 1:06-MC-6, 2006 WL 1876847 (N.D. Ind. July 5, 2006); *In re* Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecommunications Records, 439 F. Supp. 2d 456 (D. Md. 2006); *In re* Application of the United States of America, 416 F. Supp. 2d 390 (D. Md. 2006); *In re* Application of the United States of America, 415 F. Supp. 2d 211 (W.D.N.Y. 2006); *In re* Application of the United States, 441 F. Supp. 2d 816, 827–37 (S.D. Tex. 2006); *In re* United States for an Order Authorizing the Disclosure of Prospective Cell Site Information, No. 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006); *In re* Applications of the U.S.A. for Orders Authorizing the Disclosure of Cell Cite Information, No. 05-403, 2005 WL 3658531 (D.D.C. Oct. 26, 2005); *In re* Order Authorizing the Use of a Pen Register, 384 F. Supp. 2d 562 (E.D.N.Y. 2005) (holding that § 103(a)(2) of the Communications Assistance for Law Enforcement Act (CALEA), 42 U.S.C.S. § 1002(a)(2)(B), required a showing of probable cause to obtain a subscriber's location information) *on reconsideration sub nom.*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005).

60 *See, e.g.*, *In re* Application for an Order Authorizing the Extension and Use of a Pen Register Device, No. 07-SW-034-GGH, 2007 WL 397129 (E.D. Cal. Feb. 1, 2007); *In re* Application of the United States for an Order for Prospective Cell Site Location Information, 460 F. Supp. 2d 448 (S.D.N.Y. 2006); *In re* U.S. for an Order, 433 F. Supp. 2d 804 (S.D. Tex. 2006); *In re* Application for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

61 Matt Sledge, *Stingray Cellphone Tracking Warrant In Daniel David Rigmaiden Case Was Proper, Judge Rules*, HUFFINGTON POST (May 9, 2013, 3:42 PM), http://www.huffingtonpost.com/2013/05/09/StingRay-cellphone-tracking_n_3247309.html.

62 *Tax Scammer Rigmaiden Pleads Guilty, Gets Time Served*, ARIZ. REPUBLIC (Apr. 8, 2014, 10:26 AM), http://www.azcentral.com/story/news/politics/2014/04/07/rigmaiden-tax-scammer-pleads-guilty/7448151/.

63 Eric Markowitz, *This Hacker Uncovered a Massive Police Surveillance Dragnet While Serving Time In Prison*, INT'L BUS. TIMES (Feb. 5, 2016, 11:04 AM), http://www.ibtimes.com/hacker-uncovered-massive-police-surveillance-dragnet-while-serving-time-prison-2294505.

for the ACLU, that he was not some tin-foiled hat wearing conspiracy theorist, ACLU lawyers joined the case.[64] To understand why the use of the Stingray technology has raised Fourth Amendment issues, it is important to understand the role that technology may play in a criminal investigation.

Unlike the typical criminal who may be tracked through his or her address, social security number, credit cards, or family connections, Rigmaiden actively sought to "hide" from law enforcement while committing crimes. Ironically, the technology that Rigmaiden used to make his living by filing false tax returns, namely a wireless aircard,[65] ultimately led to his capture. FBI investigators began their search for Rigmaiden by identifying the ISP accounts that their suspect used to wirelessly file tax returns.[66] Agents obtained this initial information by serving subpoenas on Verizon to identify the Verizon aircard used to file the returns.[67] Agents secured an order from a district court to install a pen register and trap and trace device to obtain information about the cell towers accessed by the suspect's aircard.[68] By using this information and a map, a government agent was used to narrow the location of the aircard to an area under one-quarter of a square mile.[69] At this point, the government secured a tracking warrant that authorized agents to use a StingRay device to communicate with the defendant's aircard.[70]

Even with the formidable legal assistance provided by the ACLU, Rigmaiden eventually lost his quest to suppress the evidence seized during a search of his apartment.[71] Although it is true that the investigators did use a pen trap and trace device to search for the suspect, there is a key difference between this case and many other cases where government agencies used these devices in a criminal case investigation. Critically, the government agents in this case did secure a search warrant authorizing the use of the cell site simulator. Although the affidavit in support of that warrant may not have described the device in detail,[72] the fact that the agents had secured a warrant led the District Judge to deny Rigmaiden's motion to suppress. In addition, the federal investigators who

---

64 *Id.*

65 An aircard is a device used to connect a computer to a wireless network.

66 Order at 3, United States v. Rigmaiden, CR 08-814-PHX-DGC (D. Ariz. 2012), ECF 1009 [hereinafter Rigmaiden Order], https://www.scribd.com/document/140453993/Rigmaiden-Suppression-Order.

67 *Id.* at 4.

68 *Id.*

69 *Id.*

70 *Id.* at 5.

71 *Id.* at 2.

72 In an amicus brief, the ACLU argued that the warrant was deficient because it failed to describe in detail the capabilities of the StingRay device. *See* [Proposed] Brief for Daniel Rigmaiden as Amici Curiae Supporting Motion to Suppress at 1, United States v. Daniel Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. 2:08-CR-00814-DGC), 2012 WL 7767586.

eventually located the defendant did rely solely on the cell site simulator to find him.[73] In denying the motion, the court found that:

(1) Because the defendant obtained his apartment, computer devices, and Internet access by using fraudulent identities, he did not possess a legitimate expectation of privacy in his apartment or those devices.[74]

(2) The government lawfully obtained information about the aircard's historical cell-site, sector, and distance information as well as destination IP address pursuant to an order under the Stored Communications Act ("SCA").[75]

(3) Even if the government had violated the relevant provisions of the SCA, the SCA does not provide the remedy of suppression.[76]

(4) Before the government even located the aircard with the cell-site simulator, the government obtained data from the apartment's security system where the defendant resided showing when the occupant of unit 1122 had entered and exited the complex.[77] The government obtained that information by using a subpoena issued by an Arizona Grand Jury.[78]

(5) Although the defendant argued that the use of cell-site information for a 38-day period was unreasonable, the court held that because the information was obtained from a third party under the SCA, and the government had to perform mathematical calculations to "locate" the location of the aircard within a 0.25 mile radius, this information was not equivalent to the data provided by a tracking device.[79]

---

73 Rigmaiden Order, *supra* note 66, at 23.

74 *Id.* at 13.

75 *Id.* at 15. According to provisions of the Stored Communications Act, if a "governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation," 18 U.S.C. § 2703(d) (2015), a court may grant the government an order that requires "a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber or customer of such service." *Id.*

76 Rigmaiden Order, *supra* note 66, at 15.

77 *Id.* at 15–16.

78 *Id.*

79 *Id.* at 17–18.

The court also held that Rigmaiden did not have a reasonable expectation of privacy in the device that the cell-site simulator had tracked, namely an aircard, because he had obtained the aircard using a fraudulent name.[80] The Rigmaiden case, however, led the ACLU, as well as the Electronic Privacy Information Center ("EPIC"), to file FOIA requests nationwide in an effort to discover the reach of the technology's use.[81] When the FBI stalled in responding to those requests, EPIC sued the FBI[82] forcing the agency to begin to release files documenting the nationwide use of the device by law enforcement and the federal government.[83]

C. Change in Department of Justice Policy

As the media and nonprofit organizations began to report and challenge the use of CSS devices, federal prosecutors themselves began to question the wisdom of using applications under the Pen Register Act to deploy the technology. As one example, in a 2011 email to Assistant U.S. Attorneys in the Northern District of California, the Chief of the Criminal Division noted:

> As some of you may be aware, our office has been working closely with the magistrate judges in an effort to address their collective concerns regarding whether a pen register is sufficient to authorize the use of law enforcement's WIT technology (a box that simulates a cell tower and can be placed inside a van to help pinpoint an individual's location with some specificity) to locate an individual. It has recently come to my attention that many agents are still using WIT technology in the field although the pen register application does not make that explicit . . . . While we continue work on a long term fix for this problem, it is important that we are consistent and forthright in our pen register requests to the magistrates.[84]

Faced with a rising number of adverse decisions, the Department of Justice ("DOJ") changed course in 2015 and began requiring agents to obtain search warrants to use the technology rather than simply filing an application under the

---

80 *Id.* at 13. The defendant used the aircard to connect his laptop to a wireless network.

81 Markowitz, *supra* note 63.

82 Elec. Privacy Info. Ctr. v. Fed. Bureau of Investigation, 80 F. Supp. 3d 149 (D.D.C. 2015).

83 *See* Ryan Gallagher, *FBI Documents Shine Light on Clandestine Cellphone Tracking Tool*, SLATE: FUTURE TENSE (Jan. 10, 2013, 2:14 PM), http://www.slate.com/blogs/future_tense/2013/01/10/stingray_imsi_catcher_fbi_documents_shine_light_on_controversial_cellphone.html.

84 E-mail from Miranda Kane, Crim. Div. Chief, U.S. Attorney's Office Northern District of Ca., to U.S.A.C.A.N.-Attorneys-Criminal (May 23, 2011, 11:55 AM), https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf.

Pen Register Act.[85] However, as I detail in the next part, despite the fact that law enforcement agencies have used CSS technology without a warrant thousands of times,[86] only recently have courts begun to suppress evidence seized through the warrantless use of that technology.

III. CELL SITE SIMULATORS AND THE EXCLUSIONARY RULE

Although the Fourth Amendment protects individuals from warrantless searches, courts have rebuffed attempts to categorize the use of CSS technology as a search. As detailed above, the main reasons for that reluctance is that courts have concluded that individuals do not have a reasonable expectation of privacy in the location of their cellphone, either because the cellphone is located in public space or because cellphone users have abdicated their privacy in their location data through the third-party doctrine. Additionally, other courts have held that, because CSS technology is not significantly different than pen register/trap and trace technology, government agents need only show that the information that they seek to obtain may be relevant to a criminal investigation to obtain a court order authorizing the use of CSS technology. In the subsections below, I examine the reasoning used by the *Lambis*[87] and *Andrews*[88] courts to exclude evidence gathered through the use of CSS technology. To situate these rulings in their factual context, I begin in Section A by briefly explaining the role played by CSS technology in both of the cases. Section B reviews how law enforcement agencies attempted to shield the use of CSS technology from judicial review contrary to the intent of the Fourth Amendment. In Section C, I examine why the courts in *Lambis* and *Andrews* held that it was inappropriate for members of law enforcement to use pen register/trap and trace orders to authorize the use of CSS technology. Taking that argument forward, Section D details why these two courts determined that the use of this technology qualified as a Fourth

---

85 *See* Press Release, U.S. Dep't of Justice, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators, (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators (announcing that law enforcement agents must now obtain a search warrant supported by probable cause before using a cell-site simulator unless exigent circumstances exist); *see also* Richard W. Downing, Acting Deputy Assistant Attorney Gen., U.S. Dep't of Justice, Statement Before the Committee on Oversight and Government Reform U.S. House of Representatives (Mar. 2, 2016), https://www.justice.gov/opa/file/830026/download ("The Department recognizes the importance of considering individual privacy interests when obtaining different types of geolocation information.").

86 Associated Press, *Maryland Appeals Court Rules Against Cellphone-Surveillance Device*, BALT. SUN (Mar. 2, 2016, 9:21 PM), http://www.baltimoresun.com/news/maryland/crime/bs-md-ci-police-surveillance-20160302-story.html (stating that Baltimore police used a StingRay device in thousands of cases in 2015).

87 United States v. Lambis, No. 15-CR-724, 2016 WL 3870940 (S.D.N.Y. July 12, 2016).

88 State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

Amendment search. In Section E, I explain why the courts rejected the government's argument that, by using cellphones, individuals "consent" to the release of their location data under the third party doctrine. Finally, Section F explores why the *Lambis* and *Andrews* courts rejected some of the same arguments advanced by government lawyers in *United States v. Rigmaiden.*[89]

A. Case Facts

In the case of Raymond Lambis, the Drug Enforcement Agency ("DEA") first attempted to locate the suspect by using pen register and cell site location information ("CSLI")[90] for Lambis's cellphone in the midst of an investigation into a drug-trafficking organization.[91] Using that information, the agents discovered that the cellphone was located in the general vicinity of a specific neighborhood in New York City.[92] However, this information could not pinpoint the phone's location to a specific apartment building.[93] At this point, the DEA agents sent a technician with a CSS device to the intersection of 177th Street and Broadway to pinpoint the phone's location by forcing the cellphone to transmit "pings" to the device.[94] The technician initially tracked the phone to a specific apartment building and then to a specific apartment within the building.[95] Later that day, DEA agents knocked on the door of the apartment and obtained consent to search Lambis's room.[96] In this case, the government actually obtained a warrant authorizing the use of the CSLI, however the warrant did not specifically authorize the use of a CSS device to track the location of the suspect's phone to his residence.[97]

The role played by CSS technology in *State v. Andrews*,[98] was similar to its use in *Lambis*. Baltimore police began looking for Andrews after a witness to a shooting selected his photo out of a photographic array.[99] After obtaining

---

89 Rigmaiden Order, *supra* note 66.

90 *Lambis*, 2016 WL 3870940, at *1 ("CSLI is a record of non-content-based location information from the service provider derived from "'pings'" sent to cell sites by a target cell phone. CSLI allows the target phone's location to be approximated by providing a record of where the phone has been used.").

91 *Id.*

92 *Id.*

93 *Id.*

94 *Id.*

95 *Id.*

96 *Id.*

97 *Id.* at *2.

98 134 A.3d 324 (Md. Ct. Spec. App. 2016).

99 *Id.* at 327. Ironically, during the pre-trial period, the prosecutor assigned to the case disclosed that the police had on two occasions used Andrews's photo in an array in which he was not identified as the shooter. *Id.* at 330.

Andrews's cellphone number from a confidential informant, Baltimore police successfully secured an order pursuant to the Maryland Pen Register statute to install a Pen Register/Trap & Trace and Cellular Tracking Device.[100] After receiving that order, the police asked the cellphone provider, Sprint, to provide (1) subscriber information attached to that number, (2) 30 days of CSLI to cover the period surrounding the shooting, (3) pen register data for 60 days, and (4) precision GPS data from Andrews's phone.[101] Using the precise, real-time GPS locations provided by Sprint, detectives then proceeded to the general area where Andrews's phone was reportedly located.[102] It was at this point that the detectives, like the DEA agents in *Lambis*, proceeded to use a CSS device to locate the residence where Andrews's cell was located.[103] Officers then arrived at that residence and found Andrews sitting on the living room couch.[104] Although the officers arrested Andrews pursuant to a valid arrest warrant, they never obtained a warrant authorizing the use of the CSS device itself.[105]

B. Tackling Non-Disclosure

Although the law enforcement agencies in these two cases both used CSS technology to locate the suspects, it was only in *Andrews* where the investigating agents went to great lengths to try to "hide" the use of that technology from the defense as well as the court. In *Andrews*, this effort extended well after the defense had filed a supplemental discovery motion in an attempt to find out how the police had found Andrews at that particular address.[106] The prosecutor initially responded to that request stating that the "State does not possess information related to the method used to locate [Andrews] at 5032 Clifton Avenue."[107] Five months later, the prosecutor reported to the defense that "ATT used a stingray to locate[] your client via his cellphone."[108] Indeed, it was not until the defense filed a motion to suppress the cellphone evidence that the State filed a supplemental disclosure that identified that the police had used the CSS technology to locate Andrews.[109] At the subsequent evidentiary hearing held to address the motion to suppress, the State finally disclosed how the CSS technology operated:

---

100 CJP § 10-4B-01 et seq.; *Andrews*, 134 A.3d at 327–28.

101 *Andrews*, 134 A.3d at 328–39.

102 *Id.* at 329.

103 *Id.*

104 *Id.*

105 *Id.* at 327.

106 *Id.* at 329.

107 *Id.*

108 *Id.*

109 *Id.* at 329–30.

> [DEFENSE COUNSEL]: Tell me what the Hailstorm does.
>
> [DETECTIVE HALEY]: What we get from the phone company is the subscriber information. So, when we get the subscriber information, it has a [sic] identifier on there, if you will, a serial number. We put that into the Hailstorm equipment. And the Hailstorm equipment acts like a cell tower. So, we go into a certain area, and basically, the equipment is looking for that particular identifier, that serial number.
>
> [DEFENSE COUNSEL]: Okay. And so, if a person is inside of a home, that equipment peers over the wall of the home, to see if that cellphone is behind the wall of that house, right?
>
> [DETECTIVE HALEY]: Yes.
>
> [DEFENSE COUNSEL]: And it sends an electronic transmission through the wall of that house, correct?
>
> [DETECTIVE HALEY]: Yes. [110]

A key difference between *Andrews* and *Lambis* is that the DEA agents in *Lambis* did not intentionally commit any misconduct.[111] By attempting to adhere to the terms of the non-disclosure agreement with the manufacturer of the device, however, they deployed the CSS technology without approval of a neutral magistrate. Ironically, in the *Lambis* opinion, the court commented that the agents in all likelihood had sufficient probable cause to obtain a warrant to use the technology.[112]

A final noteworthy point regarding the disclosure process is that the three judge panel that issued the *Andrews* opinion criticized the non-disclosure agreements that many police agencies had signed with the manufacturer of the CSS devices and the FBI. The panel remarked:

> We observe that such an extensive prohibition on disclosure of information to the court—from special order and/or warrant application through appellate review—prevents the court from exercising its fundamental duties under the Constitution. [113]

---

110 *Id.* at 331.

111 United States v. Lambis, No. 15-CR-734, 2016 WL 3870940, at *5 (S.D.N.Y. July 12, 2016).

112 *Id.* at *3.

113 *Andrews*, 134 A.3d at 338.

C. *CSS Technology Is Qualitatively Different from a Pen Register or Trap and Trace Device*

The first key point made by both cases is that CSS technology is qualitatively different from pen register or trap and trace technology. In *Lambis*, the court found that the StingRay technology differed from a pen register because a cellphone user has no control over the fact that a cellphone emits information to a CSS device.[114] The emission is involuntary and automatic.[115] Similarly in *Andrews*, the panel found that CSS technology is different from pen register technology[116] and that Maryland's Pen Register Act did not authorize the use of CSS technology.[117] Because the Maryland statute at issue in *Andrews* paralleled the federal statutory scheme, the panel used the federal framework to point out that the federal statute does not authorize the disclosure of cellphone location information.[118] Notably, the panel explained:

> Looking then, at the federal statutory scheme, we note that the federal Communications Assistance for Law Enforcement Act ("CALEA"), which delineates a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, provides that "with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18), *such call-identifying information shall not include any information that may disclose the physical location of the subscriber* (except to the extent that the location may be determined from the telephone number)." [119]

It follows then that, because CSS technology is qualitatively different than pen register technology, the lower evidentiary standard of relevance used by law enforcement to obtain pen register or trap and trace orders is not sufficient to authorize the use of CSS technology.[120]

---

114 *Lambis*, 2016 WL 3870940, at *6.

115 *Id.* at *6–7.

116 *Andrews*, 134 A.3d at 358–59.

117 *Id.* at 354.

118 *Id.* at 356.

119 *Id.* (citing 47 U.S.C. § 1002 (2015) (emphasis added)).

120 *Id.* at 406; *see also Lambis*, 2016 WL 3870940, at *6 (stating that the use of a cell-site simulator to obtain more precise information about the target phone's location was not contemplated by the original warrant application).

D. *The Use of CSS Technology Qualifies as a Search*

Since the Supreme Court's decision in *Katz v. United States,*[121] the Court has tied the concept of a reasonable expectation of privacy to the distinction between private and public space. The development of technology, notably technology's ability to penetrate physical barriers to "see" and "track" individuals, has challenged the utility of the *Katz* reasonableness framework. In both cases discussed here, the court noted that even though the use of CSS technology does not constitute physical intrusion by the police into a home, the use of the technology still qualifies as a search under the Fourth Amendment. In drawing on the language of *Kyllo v. United States,*[122] the *Lambis* court stated: "Where . . . the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[123] Relying on *Kyllo*, the judges in *Lambis* reasoned that, because the cell-site simulator tracked the "pings" from Lambis's cellphone, and that technology is not widely available to the public, the use of the technology qualifies as an unreasonable search.[124]

E. *The Third-Party Doctrine Does Not Apply to Cellphone Location Information*

One of the key stumbling blocks that defense attorneys have faced in seeking to suppress cellphone related evidence has been the hurdle erected by the third-party doctrine. According to the third-party doctrine, when an individual voluntarily conveys information to a third-party, such as a bank or cellphone carrier, the individual forfeits his or her reasonable expectation of privacy in that information.[125] In both *Lambis* and *Andrews*, however, the judges found that because a CSS functions different from a pen register or trap and trace device, the third-party doctrine did not apply. Critically, while the pen register device at issue in *Smith v. Maryland* simply recorded ingoing and ongoing calls, a CSS device emits a constant "ping" that seeks out cellphones. Although the Supreme Court held in *Smith* that the user of the phone had no legitimate expectation of privacy in the numbers he dialed on his phone,[126] in the *Andrews* and *Lambis* decisions, the courts found that cellphone users do not consent to

---

121 *See generally* Katz v. United States, 389 U.S. 347 (1967).

122 533 U.S. 27 (2001).

123 *Id.* at 33.

124 *Lambis*, 2016 WL 3870940, at *6.

125 *See* Smith v. Maryland, 442 U.S. 735, 736–37 (1979).

126 *Id.* at 742.

warrantless government access to their movements simply by virtue of the fact that they choose to carry a cellphone.[127]

F. *What Changed from* United States v. Rigmaiden*?*

The *Lambis* and *Andrews* decisions by themselves are not enough to signal a permanent change in the Fourth Amendment jurisprudence regarding CSS technology. In addition to jurisdictional limitations, the fact that the CSS technology located both suspects in their living spaces limits the reach of the cases. Under the Fourth Amendment's post-*Katz* public/private space framework, an individual's right to privacy is greatest within the confines of his or her home. When law enforcement agents use CSS technology to track a suspect's location in a public space, courts may be more reluctant to find that the suspect's expectation of privacy in the location of her cellphone was a reasonable one.[128] Indeed, using the logic of *United States v. Knotts*, it seems plausible that courts might find that the short-term warrantless use of CSS devices to track an individual's movements in public does not violate the Fourth Amendment. A key limiting factor would be whether the length of time surrounding the warrantless deployment of that technology was reasonable given the Supreme Court's holding in *United States v. Jones*.[129]

A more significant change between the *Patrick* decision and the two cases discussed here is that in the period in between *Patrick* and the 2016 cases, the DOJ, as well as the Department of Homeland Security, announced a significant policy change—namely, that agents would seek warrants before using CSS technology. Indeed, both the *Lambis* and *Andrews* courts referenced the change in DOJ policy within the pages of their opinions.[130]

Even taking note of these differences, privacy advocates can find grounds for optimism in these two opinions: by finding that (1) CSS technology is qualitatively different from pen register or trap and trace devices and (2) the use of the technology constitutes a search, these two judicial bodies have attempted to push back on law enforcement's secretive and unrestricted use of a new technology.

---

127 State v. Andrews, 134 A.3d 324, 349–50 (Md. Ct. Spec. App. 2016) (citing United States v. Graham, 796 F.3d 332, 355 (4th Cir. 2015), *rev'd en banc*, 824 F.3d 421 (4th Cir. 2016)).

128 *See* United States v. Knotts, 460 U.S. 276 (1983) (holding that the use of a GPS device to track the location of a car was reasonable).

129 565 U.S. 400 (2012) (Alito, J., concurring) (finding that the use of a GPS tracking device for four weeks was unreasonable).

130 *See* United States v. Lambis, No. 15-CR-734, 2016 WL 3870940, at *5–6 (S.D.N.Y July 12, 2016); *Andrews*, 134 A.3d at 357–58.

IV. CONCLUSION: LOOKING FORWARD

The fact that law enforcement agencies have been able to use intrusive technology in this country for almost two decades without a warrant raises the question as to the Fourth Amendment's efficacy in protecting citizens' privacy rights in an age of rapid technological change. Looking beyond the structure of Fourth Amendment jurisprudence, the tale of the use of CSS technology is not a story of the strength of the judicial branch, but rather of its weakness. Although American citizens look to the judicial branch to protect our fundamental rights, in this case, the actions of the executive branch, coupled with private industry, undercut the ability of the public to not only understand how this technology worked, but also how extensively government agencies were deploying it. Today, the best hope that we have that this technology will not be used without a warrant lies not with the future actions of judicial agents, but rather with the actions of state legislatures and the DOJ's continued adherence to its own policies.[131]

Two federal agencies, the Federal Communications Commission ("FCC") and the FBI, played instrumental roles in subordinating the role of the courts in monitoring the actions of law enforcement. In cooperating with private industry to keep the use of CSS technology secret from the courts, the FBI, as well as numerous local police agencies, sought to surreptitiously prevent judicial review of the device. The appellate panel in *Andrews* detailed the danger of that secrecy:

> We observe that such an extensive prohibition on disclosure of information to the court—from special order and/or warrant application through appellate review—prevents the court from exercising its fundamental duties under the Constitution. To undertake the Fourth Amendment analysis and ascertain the reasonableness in all the circumstances of the particular governmental invasion of a citizen's personal security, it is self-evident that the court must understand why and how the search is to be conducted. The reasonableness of a search or seizure depends on a balance between the public interest and the individual's right to personal security free from arbitrary interference by law officers. The analytical framework requires

---

[131] The Department of Homeland Security has adopted a policy similar to the DOJ's policy. *See* U.S. DEPT. HOMELAND SECURITY, NO. 047-02, DEPARTMENT POLICY REGARDING THE USE OF CELL-SITE SIMULATOR TECHNOLOGY (Oct. 19, 2015), https://www.dhs.gov/sites/default/files/publications/Department%20Policy%20Regarding%20the%20Use%20of%20Cell-Site%20Simulator%20Technology.pdf (one notable difference with the DOJ policy is that the DHS mandates that its agents be candid with the court); *see also* Cyrus Farivar, *DHS Now Needs Warrant for Stingray Use, But Not When Protecting President*, ARS TECHNICA (Oct. 21, 2015, 10:30 PM), http://arstechnica.com/tech-policy/2015/10/dhs-now-needs-warrant-for-stingray-use-but-not-when-protecting-president/.

> analysis of the functionality of the surveillance device and the range of information potentially revealed by its use. A nondisclosure agreement that prevents law enforcement from providing details sufficient to assure the court that a novel method of conducting a search is a reasonable intrusion made in a proper manner and justified by the circumstances, obstructs the court's ability to make the necessary constitutional appraisal.[132]

Although the FCC possessed the ability to restrict, if not scuttle, the use of this technology, the FCC failed to adequately investigate whether the manufacturer's representations concerning the devices' potential use and their capabilities.[133] In addition, the FBI's initial decision to cooperate with device manufacturers to mandate that law enforcement agencies not disclose their use of the device to courts, defense attorneys, or the public greatly undercut the ability of the judicial branch to review whether use of the device was constitutional. Ironically, although both the DOJ and the DHS now have in place policies that mandate that agents secure a warrant before deploying CSS technology except in the case of exigent circumstances, only the DHS policy mandates that its agents be completely honest with the courts about the use of the technology.[134]

To date, the legislatures in 16 states have enacted legislation that requires law enforcement agencies to obtain a warrant before using CSS technology to track the real-time location of a suspect.[135] Although similar federal legislation has stalled,[136] in response to public concerns about the use of CSS technology, the U.S. House of Representatives Committee on Oversight and Government Reform (Committee) conducted extensive hearings from April 2015 through 2016 that examined the use of cell-site simulator technology by law enforcement agencies.[137] The Committee's final report stated:

---

132 *Andrews*, 134 A.3d at 338–39 (internal quotations and citations omitted).

133 Ernesto Falcon, *FCC Helped Create the Stingray Problem, Now It Needs to Fix It*, ELECTRONIC FRONTIER FOUND. (Oct. 6, 2016), https://www.eff.org/deeplinks/2016/08/fcc-created-stingray-problem-now-it-needs-fix-it.

134 *See* Farivar, *supra* note 131.

135 Those states include: California [CAL. PENAL CODE § 1546 (West 2016)], Colorado, Florida, Illinois [725 ILL. COMP. STAT. ANN. 137 (West 2016)], Indiana, Maine, Maryland, Minnesota, Montana, New Hampshire, New Jersey, Tennessee, Utah [UTAH CODE ANN. § 77-23c-102 (LexisNexis 2016)], Virginia [VA. CODE ANN. §19.2-70.3 (2016)], Washington [WASH. REV. CODE § 9.73.260 (2016)], and Wisconsin.

136 *See generally* Location Privacy Protection Act of 2015, S. 2270, 114th Cong. (2015).

137 *See generally* HOUSE OVERSIGHT COMMITTEE REPORT ON LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES, 114TH CONG., LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS (2016)

> While law enforcement agencies should be able to utilize technology as a tool to help officers be safe and accomplish their missions, absent proper oversight and safeguards, the domestic use of cell-site simulators may well infringe upon the constitutional rights of citizens to be free from unreasonable searches and seizures, as well as the right to free association. Transparency and accountability are therefore critical to ensuring that when domestic law enforcement decide to use these devices on American citizens, the devices are used in a manner that meets the requirements and protections of the Constitution.[138]

Consistent with the themes of this Article, the Committee concluded that Congress, not the judiciary, is in the best position to establish limits on the government's use of the technology that are consistent with the Constitution.[139] In reaching this conclusion, the Committee ironically cited the *Jones* opinion, which preceded the Committee's report by four years:

> To ensure that the use of cell-site simulators and other similar tools does not infringe on the rights guaranteed in the Constitution, the use should be limited, and a high degree of transparency is critical. Furthermore, there must be a universal and well-understood standard by which these technologies are deployed.
> Congress is best positioned to ensure that appropriate safeguards are put in place. As Justices Alito, Ginsburg, Breyer, and Kagan pointed out in a concurring opinion in *Jones:*
> "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[140]

In the case of the warrantless deployment of CSS technology in the United States, decisions made by executive agencies in collusion with corporate interests infringed on the privacy rights of American citizens. Critically, the collusion between the FBI and the device manufacturers to keep the use of the technology secret hampered the ability of state and federal legislative bodies to weigh in on the proper use of the device. Moreover, these efforts at secrecy underscore the constraints that the judicial branch faces in attempting to balance

---

https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL-bipartisan-cell-site-simulator-report.pdf.

138 *Id.* at 2.

139 *Id.* at 35.

140 *Id.* (citing United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring)).

the government's use of technology within the framework of an antiquated structure of Fourth Amendment doctrine.