Taking the Sting Out of the Stingray: The Dangers of Cell-Site Simulator Use and the Role of the Federal Communications Commission in Protecting Privacy & Security

Jason Norman*

TABLE OF CONTENTS

* J.D., The George Washington University Law School, 2016; B.A. Political Science and International Studies, University of South Florida, 2013. *Senior Managing Editor* of the Federal Communications Law Journal 2015-16. Special thanks to the hard working staff of the FCLJ for keeping me honest, to Professors Karen Thornton and Dawn Nunziato for their dedication to the success of the FCLJ, to Prof. Jodie Griffin for her guidance throughout my Note process, and to Professors Natalie Roisman and Ryan Wallach for inspiring my continued interest in Telecom Law.

I. INTRODUCTION

"The decisions we make about communication security today will determine the kind of society we live in tomorrow."

- *Whitfield Diffie, Cryptography Pioneer, May 11, 1993.*[1]

Data-driven law enforcement has increased at an alarming rate in post-9/11 America. The revelations of widespread data collection programs run by the National Security Agency ("NSA"), in the wake of classified information leaked by Edward Snowden, have given rise to serious public concern that government officials are covertly eroding the privacy of law abiding citizens in the name of national security.[2] The electronic surveillance culture that emerged in the wake of the 9/11 terrorist attacks has given credence to privacy invasion at all levels of law enforcement.

One pervasive surveillance tool is the Stingray.[3] The Stingray can intercept all cellular communications, voice and data, within its broadcast range. This interception can include conversations, locations, email, contacts, and any other private data that the phone has stored in its local memory, all without the user's knowledge or consent.[4] In a bygone era, the distribution and use of Stingrays were the sole providence of government agencies, but the decrease in cost combined with the increase in publicly available knowledge of the capabilities of the device have put the United States in a dangerous situation.[5] Setting aside for a moment the abusive uses of the Stingray by law enforcement that have recently come to light, and looking solely at the privacy and national security implications of having an insecure cellular network, there is an urgent need for a comprehensive security solution. The most sensible and efficient solution is for the Federal Communications Commission ("FCC") to mandate that wireless carriers

1. Whitfield Diffie, *The Impact of Secret Cryptographic Standard on Encryption, Privacy, Law Enforcement and Technology*, Congressional Testimony (May 11, 1993), http://cpsr.org/prevsite/program/clipper/diffie-testimony.html/.

2. Mirren Gidda, *Edward Snowden NSA Files Timeline*, The Guardian (Aug. 21, 2013), http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

3. Kate Klonick, *Stingrays: Not Just for Feds*, Slate (Nov. 2014), http://www.slate.com/articles/technology/future_tense/2014/11/stingrays_imsi_catchers_how_local_law_enforcement_uses_an_invasive_surveillance.html.

4. *See* Nathan Freed Wessler, *VICTORY: Judge Releases Information about Police Use of Stingray Cell Phone Trackers*, ACLU (June 3, 2014), https://www.aclu.org/blog/national-security-technology-and-liberty/victory-judge-releases-information-about-police-use.

5. *See* Sean Hollister, *Hacker Intercepts Phone Calls with Homebuilt $1,500 IMSI Catcher*, Engadget (July 31, 2010), http://www.engadget.com/2010/07/31/hacker-intercepts-phone-calls-with-homebuilt-1-500-imsi-catcher/.

utilize stronger encryption protocols to secure their networks, and that they enable customer access to existing security features that have been disabled by the SIM card manufacturers at the request of the service providers.

This note will provide background on how Stingrays work, discuss the impact they have on privacy and security, explain why their use undermines our justice system, and review the statutory authority that the FCC has to regulate them. Finally, this note will argue that the FCC should enact rules that mandate stronger wireless encryption standards and allow consumers to have access to existing security features to protect themselves against insecure transmissions.

II. BACKGROUND

A. What is an IMSI Catcher, and How is it Used?

An International Mobile Subscriber Identity ("IMSI" (/ˈɪmziː/)) catcher, the most popular brand of which is the Stingray, emulates a cellphone tower in a way that is impossible for a cellphone to distinguish from an authentic tower.[6] This allows the Stingray to capture any data that a cellphone would normally send to, or request from, a valid tower.[7] This data can include the cellphone's location, numbers dialed, text messages sent, websites requested, and any other data normally transmitted via airwaves. The use of these devices has become widely known in recent years in light of several lawsuits filed by the American Civil Liberties Union ("ACLU") and other watchdog organizations. As a result, it was uncovered that the warrantless use of Stingray devices by the Federal Bureau of Investigations ("FBI") and other agencies has been ongoing for approximately twenty years.[8] If not for the increased use of Stingrays for investigating domestic criminal activity, their rampant use might remain unknown to the public.

The FBI refuses to release the specific capabilities of the device, even going as far as requiring state and local agencies to sign a non-disclosure agreement ("NDA") before they are allowed to purchase a Stingray.[9] This begs the question, if the Stingray's capabilities are so sensitive, why are local law enforcement agencies allowed to use them for domestic criminal investigations since the evidence that they garner will necessarily require disclosure to a defendant in a criminal trial?

---

6. *See* Jennifer Valentino-Devries, *How 'Stingray' Devices Work*, WALL ST. J. (Sept. 21, 2011), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/.

7. *Id.*

8. *See* Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cellphone Tracking*, WIRED (Mar. 3, 2014).

9. *See* Craig Timberg, *FBI Gags State and Local Police on Capabilities of Cellphone Spy Gear*, WASH. POST (Sept. 23, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/23/fbi-gags-state-and-local-police-on-capabilities-of-cellphone-spy-gear/.

Until recently, public perception was that the capabilities of IMSI catchers were similar to devices known as pen registers, which connect to hard-wired telephone lines and record information such as the time, duration, source, and destination of incoming and outgoing phone calls to or from a specific number.[10] This is partly because the government has repeatedly obtained warrants authorizing the use of Stingrays under the dated Pen Register and Trap and Trace statutes, which implies that the technology serves the same purpose.[11]

In 2012, at a technology security conference known as DefCon, Kristin Paget conducted a demonstration using a basic laptop computer and about $1,500 worth of antennas and broadcast equipment, which showed that Stingrays are capable of much more than a simple pen register.[12] Paget configured a laptop to run a freely available software program called OpenBTS, which is an open source version of a cellular base tower station.[13] Paget successfully tricked thirty cellphones into connecting to the fake tower, at which time the IMSI catcher disabled the encryption on the phones, collected text messages, intercepted *actual phone calls,* not just the numbers dialed, and captured the encrypted keys used to authenticate the phone to a valid tower.[14] A simple software technique will break the encryption keys, allowing the same laptop to connect to a valid cell tower to receive incoming call data as well. Once the tower verifies the IMIS and encryption key of the signal, the cellphone provider cannot distinguish the false signal from the real one, meaning that there is little to no risk that both phones will attempt to connect to a valid tower simultaneously potentially triggering an alert.[15] This demonstration clearly showed that Stingrays have a much broader range of capabilities than law enforcement officials have led us to believe.

B. Advanced IMSI Catcher Capabilities

IMSI catcher capabilities include the ability to monitor content as well as location, and the user has no reasonable method of detection. Until 2010, it was thought that when a cellphone was connected to a Stingray for the purpose of data interception that the phone would display being connected to a 2G (second-generation) tower, and the user would see that this has

10. *See* 18 U.S.C. § 3127 (defining pen register).

11. *See, e.g.*, Justin Fenton, *ACLU Joins Md. Federal Case over Cellphone Tracking*, BALT. SUN (Nov. 26, 2014) (citing a Baltimore police dept. pen reg. app'n authorizing a broad Stingray search using a lower standard than probable cause).

12. *See* Chris Paget, *Practical Cellphone Spying*, YouTube (Mar. 17, 2012), https://www.youtube.com/watch?v=xKihq1fClQg.

13. *See OpenBTS App'n Suite User Manual*, Range Networks (Apr. 15, 2014), http://openbts.org/site/wp-content/uploads/2014/07/OpenBTS-4.0-Manual.pdf.

14. Chris Paget, *supra* note 12.

15. *Id.*

occurred because the 3G connection indicator would disappear.[16] This is no longer accurate. Modern cell-site simulators can trick a cellphone into reporting a 3G connection, which would normally use stronger encryption to secure its transmissions, while actually transmitting data in the less secure 2G format.[17] The mode of security that a cellular device uses is determined by the tower providing the uplink at the time, and so the Stingray downgrades the strength of encryption by sending a simple command to the device it seeks to access.[18] The type of network a cellphone connects to is important, because a 2G connection often sends data over the airwaves in "plain text", technically known as A5/0 format, which means that the data is not encrypted and can be read by a Stingray without needing to be decrypted first. The major issue with this is that the user has no way to disable 2G mode on his device, meaning that he cannot prevent insecure connections from being established.

Because the cell-site tells a cellphone what encryption format to use and the user cannot disable an insecure protocol, there is no method available to prevent the transmission of unencrypted data upon a cell tower's request. There is an existing function on the Subscriber Identity Module ("SIM") card which, when enabled, will display a warning when a cellphone connects to an unencrypted tower. However, "GSM providers consider such a warning [to be] confusing for the users, so the ciphering indication is usually disabled directly from the SIM card settings."[19] Additionally, wireless carriers deliberately disable a consumer's access to this security feature so that she cannot choose a more secure configuration for her device, even though the function exists.[20] Despite the best efforts of researchers, no alternative method to enable this functionality through the device software appears to exist. In the current market, only the makers of a device dubbed the CryptoPhone lay claim to the ability to detect cell-site simulators and to notify the user of any unencrypted connections, but with a price tag in excess of $3,000, this brand of security falls well beyond the reach of the average consumer.[21]

This security flaw is unlikely to be resolved without federal regulation. Among the major cellular providers, AT&T will not phase out the antiquated

16. *See* Darlene Storm, *Are Your Calls Being Intercepted? 17 Fake Cell Towers Discovered in One Month*, COMPUTER WORLD (Sept. 2, 2014).

17. *Id.*

18. *See* Felician Alecu & Paul Pocatilu, *Enabling the Ciphering Indicator on Android*, 6 J. OF MOBILE EMBEDDED & DISTRIBUTED SYS. 52, 55 (2014), http://www.jmeds.eu/index.php/jmeds/article/viewFile/Enabling_the_Ciphering_Indicator_on_Android/pdf_4.

19. *Id.*

20. *See id.* at 55-57 ("there is no API to be used to access the Administrative Data restricted SIM card area").

21. *See* Kim Zetter, *Phone Firewall Identifies Rogue Cell Towers Trying to Intercept Your Calls*, WIRED (Sept. 3, 2014).

2G security protocol until 2017, and Verizon is supporting 2G until 2020.[22] With security upgrades coming along so slowly, it is likely that by the time the change does happen, the 3G and 4G technologies that are scheduled to replace 2G as the new baselines for security will have already been breached in a similar manner. In fact, Harris Corporation, which manufacturers the Stingray, is already selling a device named Hailstorm, which upgrades the Stingray, thereby making it 3G/4G/LTE compatible.[23] Moreover, a manufacturer in China sells GSM IMSI catchers purportedly capable of monitoring conversations on 3G networks for $1,800 per unit over the Internet.[24] CDMA[25], which is the transmission format used by Verizon and Sprint, was initially not thought to be prone to the security issues prevalent in GSM[26] technology, but according to a 2006 release from Harris Corp., a device that they also manufacture named the Kingfish is capable of performing similar functions as the Stingray across both GSM and CDMA platforms.[27]

As part of the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), telecommunications carriers are required to design or modify their equipment in a manner that allows law enforcement agencies to conduct surveillance on the communications that flow across their networks.[28] The statute requires in part that:

> [A] telecommunications carrier shall ensure that its equipment, facilities, or services […] are capable of (1) expeditiously isolating and enabling the government, *pursuant to any court order or other lawful authorization*, to intercept, to the exclusion of any other communications, all wire and electronic communications […] *except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices [], such call-identifying information shall not include any information that may disclose the physical*

22. Thomas Gryta, *AT&T to Leave 2G Behind*, WALL ST. J. (Aug. 2, 2012); Mike Dano, *Verizon Wireless to Sunset 2G and 3G CDMA Networks by 2021*, FIERCE WIRELESS (Oct. 10, 2012).

23. *See* Cyrus Farivar, *Cities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, ARS TECHNICA (Sept. 1, 2014).

24. PKI 1600 IMSI Catcher Purchase Information, Alibaba.com (last visited Apr. 9, 2015), http://www.alibaba.com/product-detail/IMSI-catcher_135958750.html.

25. Code Division Multiple Access is a channel access method used by various radio communications technologies.

26. Global System for Mobile Communications, originally Groupe Special Mobile, a standard for cellular communications developed by the European Telecommunications Standards Institute.

27. Richard Roosa, *Letter from Richard Roosa, Harris Wireless Products Group, to Manuel Diaz - City of Miami PD* (Nov. 29, 2006) (marketing the new Kingfish device to the police dept. for man portable surveillance of both GSM and CDMA devices), http://egov.ci.miami.fl.us/Legistarweb/Attachments/34768.pdf.

28. *See* 47 U.S.C. § 1002(a) (listing the requirements of telecom providers to be able to quickly provide law enforcement with access to communications data).

> *location of the subscriber* (except to the extent that the location may be determined by the telephone number).[29]

The plain statutory language demonstrates that Congress did not intend to grant law enforcement agencies the ability to track citizens' locations using their private communications data beyond the information collection that is warranted under the pen register and trap and trace device statute, or other "court order or lawful authorization."[30]

One of the primary purposes of an IMSI catcher is to identify the location of the cellphone subscriber who is under investigation. Law enforcement officials have doggedly refused to disclose Stingray's technical capabilities, and a deeper examination of the CALEA and the Pen Register Statute provide the reasons why.[31] A full accounting of the Stingray's capabilities before a judicial panel would quickly lead to severe limitations on its use for violating the Fourth Amendment as well as multiple federal statutes.

Congress is aware that Stingrays are capable of much more than simply tracking the location of a cellular device. On Capitol Hill in 2012, computer scientist and privacy advocate Christopher Soghoian demonstrated IMSI catcher technology to congressional staffers by having them make phone calls while Kurtis Heimerl, a Berkeley communications researcher, used an IMSI catcher in the room.[32] Soghoian then had the staffers end their calls, and proceeded to replay their conversations, which the device had recorded.[33] In addition to recording their calls, the cell-site simulator was able to download "all the data from their phones - emails, contact files, music, videos – whatever was on them."[34] Soghoian's demonstration removed any doubt that IMSI catchers are capable of far more advanced surveillance than the limited uses of tracking cellphone locations and collecting dialed phone numbers. Law enforcement agencies want the public to view Stingrays as simple devices because that protects the status quo, and under the current regulatory and legislative system, the status quo equals zero oversight. There are no legal checks and balances in place to ensure that the

---

29. 47 U.S.C. §§ 1002(a), (a)(1) (emphasis added).

30. *See* 18 U.S.C. § 3121 (Pen registers and trap and trace devices are used by law enforcement to record incoming and outgoing routing information about phone calls including primarily the phone numbers themselves which can then be used to identify the location, and possibly the identity of the person(s) receiving the call(s) using a reverse lookup directory. These statutes do require that the warrant affidavit particularize the specific phone number of the person against whom the warrant is being issued, which differentiates them from how a Stingray operates.)

31. *See generally* 18 U.S.C. §§ 3121-3127 (The Pen Register and Trap and Trace Device Statute); 47 U.S.C. §§ 1001-1010 (Communications Assistance for Law Enforcement Act).

32. Jeff Stein, *New Eavesdropping Equipment Sucks All Data Off Your Phone*, NEWSWEEK (June 22, 2014).

33. *Id.*

34. *Id.*

use of Stingrays comports with the Fourth Amendment and other privacy protection statutes. Additionally, if the public interest and awareness of Stingrays increases, then the pressure on elected officials to pierce the veil of secrecy surrounding government use of this technology will begin to mount. Should the truly invasive nature of this technology become widely known, the public outcry would result in enhanced oversight, which is directly adverse to the interests of law enforcement agencies who are used to operating without a leash.

Stephanie Pell, an Affiliate Scholar at the Stanford Law School Center for Internet and Society and Cyber Ethics Fellow at West Point's Army Cyber Institute, wrote, "[t]he communications of Americans will only be secured through the use of privacy enhancing technologies like encryption, not with regulations prohibiting the use or sale of intercepting technology."[35] This sentiment rings true given the relative ease with which anyone with moderate means and the will to do so can procure and use an IMSI catcher for nefarious ends. The threat that unfettered surveillance poses to liberty, privacy, and national security far outweigh the benefits to domestic law enforcement. Given the current state of cellular technology, and the slow pace at which wireless carriers are upgrading their security protocols, our most sensitive communications at both the individual and governmental level are quite literally floating around in the wind. A recent Pew Research Center study on public perceptions of privacy and security found that only nine percent of people surveyed felt very secure in cellular communications, forty-six percent felt either not very secure or not secure at all, but fifty-four percent felt that the content of their phone conversations was very sensitive.[36] This dichotomic result illuminates an expansive divide between public interest and public policy, and could have a chilling effect on protected speech.

If our wireless communications network are vulnerable to anyone with a few thousand dollars and a disregard for the law, then the dangers of leaving our cellular infrastructure in its current insecure state are immense. The crimes of identity theft and credit card fraud plague the United States. The 2012 Bureau of Justice Statistics report on identity theft estimates that the direct and indirect costs of the 16.6 million recorded incidents between the two crimes totaling a staggering $24.7 billion dollars for that year alone.[37] For an identity thief, the temptation to use a $1,500 IMSI catcher to gobble up data from potentially hundreds, or even thousands of cellphones with negligible risk of detection would be irresistible. CNBC reported last year

35. Stephanie Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cellphone Surveillance and its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 6 (Fall 2014).

36. Mary Madden et al., *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RES. CENTER FOR INTERNET, SCI., & TECH (Nov. 12, 2014), http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

37. ERIKA HARRELL & LYNN LANGTON, VICTIMS OF IDENTITY THEFT 2012, BUREAU OF JUSTICE STATISTICS (Dec. 2013), http://www.bjs.gov/content/pub/pdf/vit12.pdf.

that 34% of owners do nothing to secure their sensitive information on their cellphones, not even a pin code to unlock the screen. Stingrays avoid even that minimal security protection entirely by emulating a trusted service provider and connecting to the phone invisibly over the airwaves.[38] Though research is scarce on this subject, it makes sense that the possibility of a thief snatching sensitive identity information out of thin air does not even register on the security radar for an overwhelming majority of Americans. It is essential that the FCC act to secure wireless infrastructure in order to prevent widespread abuse of the existing security holes.

III. LEGAL LANDSCAPE OF STINGRAY USE

There is growing concern about the widespread use of IMSI catchers, particularly in local law enforcement efforts directed at minor criminal activity. For several years, there have been increasingly frequent news reports of the employment of invasive surveillance techniques for minor offenses. Increasing public awareness, combined with reluctance by law enforcement agencies to divulge the surveillance methods used to collect evidence in criminal cases, has raised questions about the legality and frequency of Stingray use.

A. Exponentially Expanding Use of Technology in Law Enforcement

Technology has historically advanced at a faster pace than legislation or regulation can keep pace with, but the continual threat of terrorism has led to unprecedented levels of funding for new technology under the umbrella of national security. The U.S. Department of Homeland Security ("DHS") reported in 2011 that since fiscal year 2003 more than $31 billion in grant money passed from federal coffers to state and local governments "to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism."[39] State and local governments have heavily invested these federal funds in devices designed to collect and analyze data for the stated purpose of providing safety and security, however, the more common use for this technology is for domestic tracking and surveillance.[40] The secrecy surrounding the procurement and deployment of

38. Herb Weisbaum, *Most Americans Don't Secure their Smartphones*, CNBC (Apr. 26, 2014), http://www.cnbc.com/id/101611330#.

39. DEPT. OF HOMELAND SECURITY, IMPLEMENTING 9/11 COMM'N RECOMMENDATIONS: PROGRESS RPT. 2011, at 42 (2011), http://www.dhs.gov/xlibrary/assets/implementing-9-11-commission-report-progress-2011.pdf.

40. *See* Kade Crockford, *State Secrecy and Opaque Funding Programs Cloud Public's Understanding of Federal Grants for Surveillance Gear*, ACLU (July 18, 2013), https://www.aclu.org/blog/national-security-technology-and-liberty/state-secrecy-and-opaque-funding-programs-cloud.

IMSI catchers at all levels of government makes it impossible to know the exact amount invested in surveillance technology. The troubling truth of the matter is that these technologies do little to further anti-terrorism efforts, and much to increase government monitoring of law-abiding citizens. This raises serious concerns that the government is increasingly engaged in activities that violate the Fourth Amendment protection against unreasonable searches and seizures.

Government officials use computerized license plate readers, "powerful cameras that . . . enable the government to perform society-wide, retroactive, and warrantless tracking of motorists,"[41] to scan the records of the vehicle's owner for moving violations, outstanding arrest warrants, and even to check whether the owner has a concealed carry weapon permit.[42] Every time a vehicle drives through a tollbooth, under certain bridges, passes a red light camera, or drives by a police cruiser equipped with a reader, the system uploads the information and stores it in a database for future reference, and use in a criminal prosecution if necessary.[43] While the overt use of video surveillance and tracking systems by law enforcement raises significant privacy concerns, the trend toward the covert use of interception devices such as the Stingray is even more disturbing.

The Department of Justice ("DOJ") released a report in 2012 that shows a massive increase in warrantless electronic surveillance between 2003 and 2011.[44] The document was obtained through extensive litigation between the ACLU and the DOJ over Freedom of Information Act ("FOIA") requests, which the DOJ did not want to honor.[45] The report shows that the number of individuals whose phones were subjected to pen register or trap and trace surveillance tactics[46] nearly tripled between 2009 and 2011 alone, and the quantity of email and network data being monitored increased by 361% in the same time period.[47] The DOJ's reluctance to comply with the FOIA requests does raise questions about how much transparency the American public is entitled to, but more importantly it begs the question, what is the DOJ hiding? One such tactic used by the Department is the covert,

---

41. *Id.*

42. *See* Victor Li, *Law Enforcement's Latest Highway Tech Speeds Up Info-Gathering, but Critics Say it Violates Privacy*, A.B.A. J., at 17 (Oct. 1, 2014).

43. *See id.*

44. Naomi Gilens, *New Justice Dept. Documents Show Huge Increase in Warrantless Electronic Surveillance*, ACLU (Sept. 27, 2012), https://www.aclu.org/blog/national-security-technology-and-liberty/new-justice-department-documents-show-huge-increase.

45. *Id.*

46. Pen register and trap and trace surveillance are methods of tracking and tracing the numbers dialed to and from a particular phone number, but that do not allow recording of the content of a communications, only of the addressing information.

47. *See* Gilens, *supra* note 44; *see also* 18 U.S.C. § 3121 (2012) (defining pen registers and trap and trace devices as those connected to a specific telephone number for the purpose of monitoring source, destination, duration, and time of calls placed to and from that specific number).

and often warrantless, searches of the cellphone communications of American citizens.

B. Judicial History of Cellular Communications Privacy

Although IMSI catchers have only recently made their way into mainstream news, their use has been sufficiently pervasive to enlighten, and irritate, both judges and legislators. The abuse of these devices by law enforcement officials has had the odd effect of putting law enforcement agencies at odds with a judiciary that has been largely pro-law enforcement on surveillance issues since 9/11.[48] Available records show that federal agencies believe that the more widely the capabilities of the Stingray are disclosed in legal proceedings, the shorter the odds are that their use will be allowed. The capacity for abuse in such a powerful device, and the inherent requirement by its design that the rights of innocent citizens will be violated by its use, make it very likely that judges or Congress will strictly constrain its applications. The government's position is that disclosing the capabilities of the Stingray in litigation will rapidly degrade its effectiveness for fighting crime, because the more widely the capabilities of the Stingray are known, the better prepared the criminal element will be to defend against it.[49] However, that argument is moot given the vast amount of technical information that is readily available about the device in the public sphere, as discussed throughout this note.

1. *United States v.* Rigmaiden – An Early Stingray Criminal Case

There have been several civil and criminal cases involving the use of Stingray devices in recent years. An early example is *United States v. Rigmaiden*, a 2008 criminal case in which federal authorities arrested Daniel Rigmaiden on charges of leading an identity theft ring in Arizona.[50] The authorities utilized undisclosed technology to track Rigmaiden's Verizon AirCard, a device enabling a laptop to connect to the Internet via Verizon's cellular data network, which led directly to the discovery of his location and his arrest.[51] Rigmaiden argued that his Fourth Amendment rights entitled him to additional discovery regarding the surveillance methods used by the

48. *See* ADMIN. OFFICE OF THE U.S. COURTS, WIRETAP RPT. 2013; *see also* Tim Cushing, *US Courts' Wiretap Report Shows Wiretaps Are For Drugs and Warrants Are Rejected Only .03% Of The Time*, TECH DIRT (July 7, 2014).

49. *See* Kim Zetter, *Feds Admit Stingrays Can Disrupt Cell Service of Bystanders*, WIRED (Mar. 1, 2015).

50. *See* 844 F. Supp. 2d 982, 987 (D. Ariz. 2012) ("The government located and arrested Defendant, in part, by tracking the location of an aircard connected to a laptop computer that allegedly was used to perpetuate the fraudulent scheme.").

51. *Id.* at 1.

federal authorities, and that without it he could not effectively argue his Fourth Amendment claim.[52]

The government opposed this motion, claiming qualified law enforcement privilege, as established in *Roviaro v. United States*, and the court denied Rigmaiden's motion.[53] Since that denial, information surfaced suggesting that the device used to locate Rigmaiden's AirCard was, in fact, a Stingray.[54] The DOJ argued for more than a year that the use of Stingrays to track suspects does not conflict with the Fourth Amendment because people do not have a reasonable expectation of privacy in wireless communications.[55] However, upon prompting by a federal judge to disclose more details about how the Stingray works, the DOJ backtracked its position "conced[ing] that its tracking methods did indeed constitute a Fourth Amendment search and seizure", but that the search was warranted under a previously issued tracking order from Northern California that was used to procure real-time tracking information from Verizon.[56]

This reversal of position demonstrates the lengths that the DOJ is willing to go to in order to prevent the public disclosure of the Stingray's capabilities. It also raises an important question. If the Stingray was used solely to collect location data about Rigmaiden's AirCard, and the authorities already had a warrant that covered real-time tracking data from Verizon, then why did they need to go to the trouble of setting up a Stingray sting, so to speak, in order to track Rigmaiden in order to facilitate his arrest? That information was available directly from Verizon under the existing warrant. Perhaps authorities used the Stingray to gather more information than just Rigmaiden's location, which could have been determined very easily and much more affordably in traditional ways. A Yale Law Journal article analyzing the various costs associated with tracking a suspect's location on an hourly basis determined that using a wireless carrier to track a suspect costs between $0.04 and $5.21 per hour, while using an IMSI catcher costs $105.00 per hour.[57] If the government's claim of an already existing search warrant were valid, then conducting additional warrantless surveillance would duplicate the same result, would be unnecessary, more expensive and would potentially undermine their case if the evidence were suppressed as a result. Without an additional and valuable benefit to the investigation, using

52. *Id.*

53. *Id.* at 1-2.

54. Amor Tor, *DOJ: Stingray Cellphone Tracking Device Falls Under Fourth Amendment, but Don't Ask About It*, ENGADGET (Nov. 6, 2011).

55. *Id.*

56. *Id.* (conceding that tracking Rigmaiden was a search protected by the Fourth Amendment, but that the pre-existing tracking warrant 08-90330-MISC-RS (N.D.Cal.) authorized the additional real-time tracking in Arizona. The actual warrant document has not been located for reference.).

57. Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, Yale L.J. (Jan. 09, 2014).

a Stingray is an illogical tracking method in this situation, given the cheap and effective alternative methods that are readily available.

2. Judicial Reclassification of Stingrays as Mobile Tracking Devices That Are Subject to Fourth Amendment Scrutiny

The government in *Rigmaiden* attempted to classify Stingrays as Pen Register devices[58], however, the District Court for the Southern District of Texas, citing *Rigmaiden*, held in a 2012 pen register warrant denial order that Stingrays are *not* pen register *or* trap and trace devices as defined by the statute.[59] The Order focused on the plain language of the statute, which requires that a pen register device necessarily attach to a "*specific telephone number*."[60] Stingray devices do not attach to a specific number, but rather broadcast a signal in an attempt to catch as many cellphones in the "net" as possible, including those of law-abiding citizens.[61] The purpose of the warrant application in the Texas case was to determine what cellphone number a suspected narcotics trafficker was using to conduct his business.[62] The implication is that the government did not know the *specific* number of the suspect. In order to find out which number the suspect was using, it would be necessary to catch *all* cellular traffic in the given area, and to analyze every device individually to determine the suspect's information. To accomplish this, all cellphone data captured by the Stingray, including call records, times, durations, and locations, would require analysis in order to narrow the batch of numbers down to the one that the suspect was using. A pen register warrant must be limited to a particular telephone number, which the government did not have in this case. In order to get that number, the government must necessarily conduct a search for it in a way that violates the Fourth Amendment rights of all the cellphone users other than the one in question.

The Fourth Amendment implications in this activity are apparent. Stingray surveillance involves the warrantless search of innumerable citizens' cellphone activity, and leaves those whose rights are violated with no readily available recourse. There is no requirement under the Pen Register Statute that the government notify individuals when their information has been collected by a Stingray, and in most cases, those whose information was gathered illegally will never even know. There are no federal statutes explicitly governing the use of Stingrays, so there is no legally binding

58. 18 U.S.C. § 3127(3) (defining the term Pen Register); 18 U.S.C. § 3123 (regulating the use of Pen Registers).

59. In Re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 2012 WL 2120492, at *5-6 (S.D. Tex. Jun. 2, 2012) (denying the app'n because Stingrays are not pen registers as contemplated in the statute) [hereinafter In Re App'n].

60. *Id.* at *2-3.

61. *Id.*

62. *Id.* at *1.

requirement to destroy information after it is collected. Barring state law to the contrary, federal and state agencies could store the information indefinitely for use in future investigations.

Rigmaiden and *In Re Application* raise three important findings that are relevant to future Stingray litigation. First, cell-site simulators are mobile tracking devices, not pen registers or trap and trace devices, which means that a search warrant should be required for their use.[63] Second, the federal government has acknowledged that the use of a Stingray device is properly analyzed as a Fourth Amendment search and seizure.[64] Third, because the Stingray is not a pen register or trap and trace device, the statute that law enforcement relies on to authorize its use, 18 U.S.C. § 3123, is not applicable.

C. Questionable Legality of Law Enforcement Practices

Federal and local law enforcement officers have found a simple way around the pesky Fourth Amendment warrant clause. They use deceptive information on reports and depositions related to criminal proceedings which involve Stingray use, such as referring to any information obtained by a Stingray as having come from a "confidential source" when submitting warrant applications.[65] This tactic denies defendants their right to challenge the constitutionality of surveillance methods used by police investigators. As is easily imagined, this tactic has had a very cold reception by members of the legal community.

1. U.S. Marshals Service Requests That State and Local Police Departments Deceive Judges

In a series of e-mails leaked from the North Port, Florida Police Department, Sgt. Ken Castro stated that rather than disclose to the court that Stingray devices were used to track the location of a suspect, that, at the request of the U.S. Marshals Service, all reports or depositions referred to information obtained by Stingrays as having been "received from a confidential source."[66] He also states, "to date this [practice] has not been challenged, since it is not an integral part of the actual crime that occurred."[67] Naturally, there have been no challenges to this practice. The agencies tasked with submitting sworn documentation of the arrest procedures have

63. *See id.*

64. *Id.*

65. Kim Zetter, *Emails Show Feds Asking Florida Cops to Deceive Judges*, WIRED (Jun. 19, 2014).

66. E-mail from Kenneth Castro, Sargent of the North Point Police Dept., to Terry Lewis, Tom Laughlin, Curt Holmes and Paul Sutton (Apr. 15, 2009, 11:25 AM), http://www.wired.com/wp-content/uploads/2014/06/ACLU-Florida-Stingray-Police-Emails.pdf.

67. *Id.*

eliminated all references to warrantless surveillance, which by the DOJ's own admission constitutes a Fourth Amendment search requiring advance judicial review.[68]

Why would a court think to question police tactics of which it has no knowledge? When the ACLU requested the documentation from the North Port Police Department, the U.S. Marshals Service "swooped in at the last minute to grab the records, claiming they belong to the U.S. Marshals Service and barring the police from releasing them."[69] Their official justification was that the Marshal Service deputized the detective and therefore the documents belonged to the federal government rather than the police department.[70] The ACLU promptly sought an injunction to prevent further release of documents to the Marshal Service, but the Florida state court, having no authority to demand release of documents held by a federal agency, was unable to demand production of the seized documents.[71]

The practice of hiding information about Stingray use has spread to police departments across the United States. The Los Angeles Police Department refused to discuss Stingray use in the department in the wake of documents obtained by the LA Weekly proving that the department spent more than $340,000 on "Stingray II equipment."[72] The Oakland Police Department has used Stingrays in its Criminal Investigative Division.[73] Stingrays are in use by state and local agencies in twenty-three states and the number is growing rapidly.[74] The ACLU has confirmed that at least fifty-eight police departments use Stingrays as part of their investigative process, but the number is almost certainly much higher because the procurement of this hardware is a closely guarded secret in many instances.[75]

2. The FBI and the DOJ Go to Extraordinary Lengths to Protect the Secrets of the Stingray

In addition to the actions taken by the U.S. Marshals Service to prevent the capabilities of the Stingray from becoming public through legal proceedings, the FBI has also taken extra-legal steps to that end. In 2012, the

68. *See* In Re App'n, *supra* note 59.

69. *See* Kim Zetter, *U.S. Marshals Seize Cops' Spying Records to Keep Them From the ACLU*, WIRED (June 3, 2014).

70. *Id.*

71. *Id.*

72. Jon Campbell, *LAPD Spy Device Taps Your Cell Phone*, LA WEEKLY (Sept. 13, 2012).

73. Stephen Lawson, *California Police Criticized for 'Stingray' Cellphone Trackers*, PC WORLD (Mar. 13, 2014).

74. *See* ACLU, *Stingray Tracking Devices: Who's Got Them?* (last visited Nov. 9, 2015), https://www.aclu.org/map/stingray-tracking-devices-whos-got-them; *see also* Michael Bott & Thom Jensen, *9 Calif. Law Enforcement Agencies Connected to Cellphone Spying Technology*, KXTV (Mar. 6, 2014); Bob Sullivan, *Pricey 'Stingray' Gadget Lets Cops Track Cellphones Without Telco Help*, NBC NEWS (Apr. 3, 2014).

75. *See* ACLU, *supra* note 74.

ACLU received a document as part of a FOIA request showing that the FBI required the Tacoma, Washington police department to sign an ironclad non-disclosure agreement ("NDA") before granting permission for the department to purchase a Stingray.[76] A NDA is now standard protocol before any state or local police agency can procure a Stingray.[77] By requiring this agreement, the FBI has created a rift between law enforcement agencies and the judiciary. Law enforcement officers are now required by the FBI to hide, mask, or outright lie about the true source of their evidence in judicial proceedings. This calls into question the results of any investigation in which a Stingray was used without a warrant, and mars the credibility of the officers who are put into an awkward and potentially contemptuous position before the court.

An officer that collects evidence using a Stingray is under pressure from four dissimilarly interested groups: (1) the prosecutors, who want to punish criminal defendants; (2) the FBI and the DOJ concerned with protecting the secrecy of the Stingray's capabilities; (3) the criminal defendant, who is entitled to be informed of the evidence against him and the methodologies used to gather that evidence; and (4) the judges who balance all of these competing interests under the law. Law enforcement officers have demonstrated that they are willing to hide the truth on warrant applications regarding the true source of the information they gather by referring to the Stingray as a confidential source.[78] Prosecutors have shown that they will withdraw evidence from a criminal trial at the risk of putting a criminal back on the street, rather than following a judge's order to reveal the Stingray's capabilities.[79] The DOJ has admitted in court that the use of a Stingray is a search within the meaning of the Fourth Amendment, yet they still use them without obtaining a warrant.[80] None of these practices are acceptable.

They deny criminal defendants due process by preventing proper constitutional challenges to the surveillance methods employed, they potentially violate the Fourth Amendment rights of many citizens in the process, and the practice requires law enforcement officers to deceive the very courts the laws of which they are employed by the taxpayers to enforce.

---

76. Timberg, *supra* note 9.

77. *See id.*

78. *See* Justin Fenton, *Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods*, BALTIMORE SUN (Nov. 17, 2014); *contra* F.R. CRIM. P. 16(a)(1)(E)(i) (2014).

79. *See* CJ Ciaramella, *How the Justice Dep't Keeps Its Cell Phone Snooping a Secret*, VICE (June 16, 2014).

80. This practice has purportedly been abandoned following the recent DOJ public policy change regarding Stingray use, although the policy leaves considerable gaps in the coverage of the new self-imposed warrant requirement. The policy and its implications are discussed in more detail below.

All perspectives on Stingray use reveal its corrosive effect on the integrity of the judicial system.

3. Judges and Legislators Have Responded Zealously to the Covert Use of Stingray Devices for Ordinary Criminal Law Enforcement Functions

Far afield from the lofty purpose of protecting national security, the Baltimore police department came under fire by a defense attorney in November 2014 for refusing to disclose the technology used to track his client who was a suspect in a robbery case.[81] When pressed as to how he tracked the defendant, Detective John Haley denied using a Stingray and refused to reveal the technology used to track the suspect citing the NDA the department had signed with the FBI.[82] Judge Barry Williams of the Baltimore Circuit Court reminded Det. Haley that there is no NDA with the court, and threatened to hold Haley in contempt if he did not respond to the attorney's questions.[83] Rather than force Haley to disclose the details of the technology, the Baltimore prosecutor withdrew key evidence from the case, including the cellphone and a handgun found at the defendant's home.[84] Wessler, the spokesman for the ACLU, commented that "a secret written agreement does not invalidate the Maryland public records law [and] does not invalidate due process requirements of giving information to a criminal defendant."[85] There is very little mystery as to whether the device in question in this case was a Stingray, yet the prosecutor felt so compelled to maintain the thinly veiled secret of its use that he withdrew key evidence from a criminal prosecution.

A similar case arose in Tallahassee, Florida when police used Stingray surveillance, and subsequently refused to disclose their method of surveillance at trial.[86] The defendant faced an airtight charge of robbery with a deadly weapon, which carries a mandatory four-year prison sentence. However, because police would not disclose how they obtained evidence using the Stingray to the defense attorney when ordered to do so by the presiding judge, the evidence was excluded and the prosecutor was forced to offer a plea bargain of six months of probation.[87]

In Charlotte, a judge has unsealed more than *five hundred* criminal cases tried between 2010 and 2014 that involved Stingray surveillance and

81. Fenton, *supra* note 78.
82. *Id.*
83. *Id.*
84. *Id.*
85. *Id.*
86. Ellen Nakashima, *Secrecy Around Police Surveillance Equipment Proves a Case's Undoing*, WASH. POST (Feb. 22, 2015).
87. *Id.*

flagged them for review for due process and Fourth Amendment violations.[88] The police had requested that the case files remain sealed because "they were worried about criminal suspects avoiding detection."[89] The district attorney's office must now review all of the cases to see the department withheld any information from the defendants in violation of due process, and will then forward any such documents to their attorneys.[90] This will assuredly result in the reopening and appeal of many of the cases, at immense taxpayer expense, thereby denying the due process rights of the defendants. In cases where improper evidence resulted in a defendant's conviction, the charges may be dismissed altogether, potentially putting dangerous criminals back on the streets. Perhaps the most disturbing revelation is that it is entirely unknown "whether police actually obtained authorization [to use the Stingray] [. . .] because those records were not among the 529 documents."[91]

In December 2014, eleven U.S. Senators submitted a letter to Attorney General Eric Holder, and Secretary of Homeland Security Jeh Johnson, inquiring about the U.S. Marshals Service's use of cell-site simulators called DRTBoxes which were attached to fixed wing airplanes that "collect[ed] the information of thousands of Americans, potentially infringing on the Fourth Amendment and disrupting normal cellphone usage."[92] The device works like a Stingray, but covers a much broader area in a manner designed to assist in hunting fugitives. According to the letter, in addition to the Marshal Service, the DOJ, Drug Enforcement Agency, DHS, and Immigration and Customs Enforcement are also using the devices.[93] The Senators expressed the sentiment that, "given the extreme lengths to which federal agencies have gone to keep surveillance technologies like this a secret, it is vital that their use be subject to strict oversight by the courts and Congress."[94] It remains unclear how judicial or congressional oversight would be effective, or even possible, if the law enforcement agencies tasked with disclosing the use of the devices are actively concealing their use.

Some State legislatures have started to take action to limit the use of IMSI catchers within their borders. The Supreme Courts of Florida and Michigan held that warrants are required before police can conduct real-time tracking of cellphone data.[95] The Illinois, Indiana, Maryland, Minnesota,

88. *See* Fred Clasen-Kelly, *Mecklenberg County District Attorney's Office to Review Surveillance Cases*, CHARLOTTE OBSERVER (Nov. 20, 2014).

89. *Id.*

90. *See id.*

91. Matthew Keys, *Judge Unseals Hundreds of Court Records on Stingrays*, THE BLOT MAGAZINE (Nov. 25, 2014).

92. Letter from Jon Tester, United States Senator et al. to Att'y Gen. Eric Holder and Sec. Homeland Security Jeh Johnson (Dec. 9, 2014), http://www.scribd.com/doc/249798493/Tester-s-letter-to-Attorney-General-Holder-and-DHS-Secretary-Johnson.

93. *Id.*

94. *Id.*

95. Hanni Fakhoury, *Stingrays Go Mainstream: 2014 in Review*, ELECTRONIC FRONTIER FOUNDATION (Jan. 2, 2015).

Tennessee, Utah, Virginia, and Wisconsin legislatures have passed statutes requiring that police obtain a warrant to track a cellphone in real-time.[96] From this information, it seems likely that this trend will continue to spread to other states, and perhaps the process will shine some light on the secrecy of the Stingray. However, requiring warrant applications for real-time tracking of cellphones at the state level does not address some major issues, such as: the lack of disclosure of capabilities that go beyond location tracking, the use of the devices by non-governmental entities, or by federal authorities who are not subject to state warrant requirements. A meaningful public debate about the insecurity of American cellular networks against both governmental and criminal intrusion requires transparency, and the argument that publicly admitting the full range of Stingray capabilities would undermine law enforcement efforts is severely weakened by the breadth of technical information that is now available from a wide variety of sources.

It is unclear exactly why law enforcement agencies are so averse to disclosures regarding the use of Stingrays. The known capabilities of IMSI catchers are already broad in scope. It is hard to think of any function that is so critically important that it warrants withdrawing key evidence from criminal prosecutions in order to protect the secret. Anne Weismann, chief counsel of Citizens for Responsibility and Ethics, stated that she "question[s] what possible legitimate federal interest [] the FBI and U.S. Marshals have in preventing the public from learning how local law enforcement authorities conduct surveillance."[97]

How constitutionally invasive must the functions of a Stingray be if they are unfit for disclosure during criminal judicial proceedings? More importantly, if the local police are using these devices so commonly, what is there to stop criminals, foreign intelligence services, or terrorists from using Stingrays in the same manner to breach our national security, steal our secrets, our identities, or commit other crimes?

4. *Riley v. California* – the Supreme Court Unanimously Holds That the Search of a Cellphone by Law Enforcement Requires a Warrant

In June 2014, the Supreme Court issued its opinion in *Riley v. California*. The Court unanimously held that in order to search the contents of a cellphone, law enforcement officers must first obtain a warrant.[98] This decision is both timely and consequential when juxtaposed against the continued use of Stingrays in apparent contravention of this principle. Because federal authorities have made the capabilities of the Stingray such

96. *Id.*

97. CJ Ciaramella, *How the Justice Dep't Keeps Its Cell Phone Snooping a Secret*, VICE (June 16, 2014).

98. Riley v. California, No. 13-132, 573 U.S. ___ (June 25, 2014).

a closely guarded secret, courts have little knowledge of whether or not the use of these devices conflicts with the recent Supreme Court decision in *Riley*.[99]

The DOJ conceded in *Rigmaiden* that the use of a Stingray constitutes a Fourth Amendment search.[100] This concession when viewed in light of *Riley* should automatically require the issuance of a search warrant before a Stingray can be used in an investigation. However, because a Stingray searches all devices in its range in order to locate its target, the Fourth Amendment rights of all citizens whose data is collected is violated, not just the rights of the suspect. If the target device ID is unknown, then the data from all of the devices must be searched to locate the one suspect device, but a search warrant for one person does not grant the right to search all. To engage in this type of "door-to-door" searching is akin to the issuance of general warrants like those of King George, which were the very reason the founders drafted the Fourth Amendment.

There is zero judicial oversight in place to protect the rights of the individuals who are not the subjects of an investigation against having their privacy violated in this manner. This practice is functionally the same as allowing law enforcement officers to kick in the door of every house in a neighborhood to search for evidence of a crime that may or may not have been committed by those citizens. Then when the time comes to try the case, the evidence suddenly is not important enough to use because to do so would require admitting how it was obtained, even though the practice is public knowledge. The only feasible remedy for this type of Fourth Amendment violation goes to the criminals who end up on trial, because they have standing to benefit from the exclusionary rule to suppress illegally obtained evidence. For ordinary citizens who have had their private communications monitored and collected, the only remedy available is to file a very costly and time consuming civil rights action under § 1983. This remedy is inherently problematic. The only way in which surreptitious data collection of this type would come to light would be for the subject of the collection to be informed by the government that this action had taken place.

There is no legal requirement imposed on the government to give notice that a Stingray has seized a person's data, unlike some sections of the Electronic Communications Privacy Act ("ECPA") which do require this type of notice.[101] Unfortunately, the part of the ECPA on which the government relies in Stingray use cases,[102] the Pen Register Statute, does not have a notice requirement because it was not intended to govern the mass

99. *See* Fenton, *supra* note 78.

100. *See Rigmaiden*, 844 F. Supp. 2d at 987.

101. *See* 18 U.S.C. § 2518(8)(d) (2012) Procedure for Interception of Wire, Oral, or Electronic Communications (requiring notice be given to a monitored individual within a reasonable time but no longer than 90 days after termination of an interception unless otherwise ordered by a court).

102. *See, e.g.*, *Rigmaiden*, *supra* note 100.

collection of phone records, which is the precise activity that it is being used to justify.

The Supreme Court in *Riley* states, "[m]odern cellphones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'"[103] In an increasingly networked world, we are gradually but consistently trading privacy for convenience. This tradeoff is generally a personal choice made by an individual in exchange for a benefit, but given the secrecy surrounding Stingray use, the public is entirely excluded from the negotiations. If society is to accept a new type of widespread invasion into its private communications, the proposal should be vigorously debated and legislated in order to limit its use, and subject to sufficient oversight to prevent its abuse. Currently, there is insufficient transparency for a useful public debate, minimal oversight to limit the use and abuse of this surveillance practice, and while there has been some inquiry by Congress there is no active legislation on the matter.

The Court in *Riley* made an important break from *Katz* in that it made no mention of a reasonable expectation of privacy test.[104] This could be a watershed moment for privacy legislation, because the reasonable expectation test is necessarily subjective and given the rate at which Americans are trading their privacy for convenience, a court could easily erode the few remaining privacy rights under the justification that society has deemed the loss reasonable.

If *Riley* is an indicator of future results from the Court, then perhaps the judiciary is moving away from the subjective view of privacy adopted in *Katz v. United States* and toward an objective privacy view similar to that of *United States v. Jones*, which followed the traditional trespassory notion of privacy.[105] Fourth Amendment challenges to Stingray use under the *Riley* standard would be more likely to succeed than under *Katz*. *Katz* supports the argument that individuals do not have a reasonable expectation of privacy in wireless communications because they travel on public airwaves.[106] Congress codified this concept in the Wiretap Act, which states in part, "it shall not be unlawful […] for any person to intercept or access an electronic communication made through an electronic communications system that is

---

103. *Riley*, *supra* note 98 (citing *Boyd v. United States*, 116 U.S. 616 (1886)).

104. *See* Susan Landau, *What the Court Didn't Say in Riley May be the Most Important Thing of All*, LAWFARE (June 30, 2014).

105. *See* United States v. Jones, 132 S. Ct. 945 (2012) (holding that GPS tracking device placed on vehicle violated Fourth Amendment protections); *see also* Katz v. United States, 389 U.S. 347 (1967) (adopting the reasonable expectation of privacy test for Fourth Amendment applications).

106. *See Katz*, 389 U.S. at 360 (Harlan, J., concurring) (setting forth the reasonable expectation of privacy test). Under the *Katz* test, it is unlikely that a court would find that a person using a device that communicates signals through public airwaves could have reasonably believed that those communications would remain private; Shaina Hyder, *The Fourth Amendment and Gov't Interception of Unsecured Wireless Comm'ns*, 28 BERK. TECH. L.J. 937, 938 (2013).

configured so that such electronic communication is readily accessible to the general public."[107]

The *Katz* test, and later the Wiretap Act, have been the foundation of government interception of radio communications for almost fifty years, and the premise is starting to show its age in the digital era. Even when a person makes a cellphone call from the privacy of their home, a constitutionally protected area, the communications necessarily traverse public airwaves in non-constitutionally protected areas. Interception is no longer conducted at the endpoints of a communication as was the case with pen register and trap and trace devices, which linked to a landline that connected directly to a person's home, or to a phone booth as was the case in *Katz*.[108] With a Stingray, the interception takes place directly from the air, and can be conducted from anywhere within the broadcast range of the device. It stands to reason that the *Riley* standard, which does not appear to rely on the reasonable expectation of privacy test, could functionally replace the *Katz* test as the new norm for analyzing Fourth Amendment privacy issues related to digital communications. At the very least, *Riley* appears to indicate that the Court is leaning toward an objective privacy analysis methodology which is more likely to extend Fourth Amendment protections to cover over-the-air communications, and as such would transitively apply Fourth Amendment rules to Stingray surveillance.

D. Department of Justice Releases Enhanced Federal Cell-Site Simulator Use Policy

The DOJ Office of Public Affairs released a statement on September 3, 2015 outlining its "enhanced" policy regarding the use of Stingrays in federal law enforcement investigations and proceedings ("the Policy").[109] The contents of this document are more telling for what is absent than for what is explicit. The DOJ reiterates its long-held position that cell-site simulators used by the federal government are configured only as pen registers, and do not collect any location data directly from the cellphones being monitored.[110] If that is the only purpose for which the federal government is purchasing Stingrays, then these are the most expensive caller ID machines ever designed.[111] Pen registers and trap and trace devices, as discussed in more detail above, are devices that have the sole capability of

107. 18 U.S.C. § 2511(2)(g)(i) (2012).

108. *Katz*, *supra* note 105, at 348.

109. U.S. DEP'T OF JUSTICE, DEP'T OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY, No. 15–1084 (Sept. 3, 2015) [hereinafter DOJ STINGRAY POLICY], http://www.justice.gov/opa/file/767321/download.

110. *Id.* at 2.

111. *See Wireless Products Group Harris GCSD Price List*, HARRIS CORP. (Sept. 2008) (showing that a single Stingray II device costs between $148,000 and $356,400), https://assets.documentcloud.org/documents/810742/845-harris-price-list-amberjack-stingray-kingfish.pdf.

recording the routing and identification information at the endpoints of a line of communication.[112] To add any other features to the device changes it in such a way that it is no longer a simple pen register, and therefore does not satisfy the statutory definition as contemplated by Congress.

1. Stingray Data Collection Policy

The Policy further states that department devices "may not be used to collect the contents of any communication [. . .] contained on the phone itself" including "emails, texts, contact lists, images, or any other data from the phone."[113] It does not state that the devices *cannot* collect such information from phones, only that the department *may* not do so. This lends credence to the popular belief that Stingrays can, in fact, access and collect data stored on phones from a remote location.[114]

Strangely, the policy also states that "Department cell-site simulators do not provide subscriber account information (for example, an account holder's name, address, or telephone number)."[115] The fact that the DOJ's policy limits its Stingray configuration to only the functions of a pen register contradicts previous evidence of how the DOJ has used the tool. The sole statutorily defined purpose of a pen register is to collect routing information, i.e. telephone numbers, of incoming and outgoing communications.[116] It is contradictory for the Policy to state that neither telephone numbers nor subscriber account information (which also includes IMSIs) are collected using department Stingrays, because if that statement is true, then the sole function that the device is purportedly capable of providing does the precise thing that the Policy does not allow. Parsing the language of the Policy reveals that this is actually not what the Policy says, it says rather that cell-site simulators "do not provide" the information.[117] If the various federal law enforcement agencies did not have such a well-established record of surreptitious behavior designed to conceal even the mere existence of Stingrays from public scrutiny, then it would be less problematic to take agency officials at their word.

There is one major problem with the Department "coming clean" about their use of Stingrays. While the Policy takes positive steps toward protecting civil liberties, aside from the description of the pen register function and the legal authority supporting its use, there were no disclosures

112. *See* 18 U.S.C. § 3127(3) ("'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, provided, however, that such information shall not include the contents of any communication.").

113. DOJ STINGRAY POLICY, *supra* note 109, at 2.

114. *See* Stein, *supra* note 30 (describing the demonstration of an IMSI catcher by Chris Soghoian before congressional staffers of the very features listed here).

115. DOJ STINGRAY POLICY, *supra* note 109, at 2.

116. *See* 18 U.S.C. § 3127 (2012).

117. *Id.*

about what technology is allegedly disabled.[118] Fortunately, while American companies are still extremely resistant to public disclosure of the technical capabilities of IMSI catchers, Israeli based company Ability Limited has no such compunction. Ability manufactures many varieties of cellular interception devices, but the product most similar to the Stingray is the IBIS, or In-Between Interception System, which is also an active interception system.[119] Ability's product datasheet for IBIS lists features including:

- bi-directional interception of encrypted GSM communication in real-time;
- decryption of A5/1, A5/2 and A5/3 encryption protocols;
- voice and data recording to hard disk;
- downgrading of service area encryption from A5/2 to A5/1;
- selective jamming of network services;
- ability to interrupt ongoing calls or to selectively prevent calls;
- data extraction including IMSIs and phone numbers;
- making and receiving phone calls and SMS on behalf of target phones;
- presence detection and direction finding; and
- invisible and undetectable operation.[120]

It is reasonable to assume that the Stingray provides many, if not all, of the features in this list. If not, this article would need an eye-catching new title about the grave constitutional threat posed by IBIS instead of Stingray.

2. Exigency Includes the Absence of Exigency

A positive addition made by the Policy is the requirement that all federal law enforcement agencies obtain a search warrant prior to using a Stingray to collect a target's cellphone data.[121] It is arguable that the growing collection of judicial precedent regarding Stingray use had already established that a search warrant is required, and that the DOJ simply advanced the Policy to quell growing unrest by members of Congress and to stave off a less predictable legislative solution to cellular surveillance regulation.[122] The Policy raises significant points of concern regarding the

118. *See generally id.*

119. IBIS PRODUCT DATASHEET, ABILITY LTD. (last accessed on Sept. 30, 2015), http://www.toplinkpac.com/pdf/IBIS_Brochure.PDF.

120. *Id.* at 1, 10.

121. DOJ STINGRAY POLICY, *supra* note 109, at 3.

122. *See* United States v. Rigmaiden, 844 F. Supp. 2d 982, 1001 (D. Ariz. 2012) ("[T]he government has already conceded the use of the mobile tracking device constituted a search under the Fourth Amendment.").

legal authority supporting the Policy's exigency and exceptional circumstances exceptions to the warrant requirement.[123]

a. *A New Mix and Match Exigency Paradigm?*

The Policy properly references the narrowly prescribed situations that either Congress or the Supreme Court has determined may require such immediate action as to forego the requirement to obtain prior judicial approval in the form of a search warrant. The need to protect human life or avert serious injury is certainly an exigent circumstance, as is the imminent destruction of evidence, hot pursuit of a fleeing felon, or the prevention of escape.[124] The problem, however, is that the Policy does not limit agencies to the carefully crafted and narrowly applied exceptions available within the context of the Fourth Amendment.

Even though the DOJ conceded in *Rigmaiden* and implied in the Policy that the use of a Stingray constitutes a search within the meaning of the Fourth Amendment that requires a search warrant, the Policy also allows agencies to conduct Stingray surveillance without a warrant to the extent allowed by the emergency circumstances described in the ECPA Pen Register Statute.[125] The Pen Register Statute exigencies include the Fourth Amendment exigency for immediate danger of death or serious bodily injury to any person, but they go further, adding "conspiratorial activities characteristic of organized crime; an immediate threat to a national security interest; or an ongoing [felonious] attack on a protected computer."[126] What the DOJ describes as a "subset of [the Fourth Amendment's] exigent situations," is actually an entirely different and considerably less restrictive set of allowances.

b. *Which Came First, the Conspiracy or the Exigency?*

In *Nabozny v. Marshall*, a case involving the kidnapping of a bank manager and the placement of a wiretap without a warrant, the Sixth Circuit Court of Appeals defined an organized crime conspiracy as requiring at least three people and traditional criminal activities as including extortion.[127] It is difficult to imagine a situation in which a mobile pen register would be helpful in determining if a) three or more people are conspiring to commit a crime, and b) that the crime they are involved in is one characteristic to organized crime, prior to actually using information collected by the device as the Pen Register Statute requires.[128] Additionally, if law enforcement

123. DOJ STINGRAY POLICY, *supra* note 109, at 3-4.

124. *Id.*

125. *Id.*; 844 F. Supp. 2d at 1001.

126. 18 U.S.C. § 3125 (Pen Register emergency circumstances relieving officers of the warrant requirement).

127. 781 F.2d 83, 85 (6th Cir. 1986).

128. 18 U.S.C. § 3125(a)(1)(B).

possesses knowledge of a criminal conspiracy prior to needing to use the Stingray, then there is no exigency precisely because of possessing that prior knowledge. Even in the case of a kidnapping, the criminal conspiracy exigency is not necessary because the danger to life and limb already justifies warrantless use of a Stingray.

Kidnapping, for the purpose of extortion, is an activity characteristic of organized crime and, as the Policy states, it is important to provide law enforcement with the best tools available to combat such offenses. However, it is conceivable that "conspiratorial activities characteristic of organized crime," from the perspective of a law enforcement officer, could include an activist at a Chicago political rally talking heatedly into her cellphone, or a young African-American man protesting excessive use of force by police officers in Baltimore because he could incite a riot.[129] It is easy to imagine an after-the-fact search warrant affidavit that embellishes the facts surrounding the use of a Stingray just enough to satisfy judicial review of the exigency application, thereby justifying the issuance of an *ex post* warrant legalizing a surveillance action that otherwise would not have survived a probable cause hearing. In fact, law enforcement officers and prosecutors both have a powerful motivation for doing so. If the affiant, upon judicial review of the *ex post* warrant application, does not satisfy the exigency requirements and he had actual knowledge of that fact, the affiant, be it the officer or the prosecutor, could be guilty of conducting illegal surveillance.[130] Because the Pen Register and Trap and Trace statutes are part of the ECPA, a person found to have violated the statute faces "imprisonment for not more than five years, […] a fine of up to $250,000," or both.[131] That is a powerful incentive to ensure that a warrant application withstands scrutiny.

c. *Immediate Threat to National Security According to Whom?*

The Policy also includes "immediate threats to national security interests" as an exigent circumstance justifying warrantless Stingray use.[132] In 2001, the USA PATRIOT Act expanded the definition of terrorism to include acts wholly domestic.[133] Under the amended language, a person commits an act of domestic terrorism if they do an act "dangerous to human

129. *See, e.g.*, Frank Main, *Chicago Police Fighing to Keep Cellphone Trackers Secret*, CHICAGO SUN-TIMES, Mar. 22, 2015; Michael Gould-Wartofsky, *5 Tools the Police Are Using in Their War Against Activists*, THE NATION, May 5, 2015, http://www.thenation.com/article/5-tools-police-are-using-their-war-against-activists/.

130. 18 U.S.C. § 3125(c); 42 U.S.C. § 1983.

131. 18 U.S.C. § 2511(4)(a) (defining punishments for violations of Title III).

132. DOJ STINGRAY POLICY, *supra* note 109.

133. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 802, 115 Stat. 272, 376 (2001) (defining the term "domestic terrorism") (emphasis added).

life" that violates any American criminal law and "*appears* to intimidate or coerce a civilian population."[134] Appearance is a very subjective and flexible concept to interpret, particularly when the decision justifies or denounces an intrusion upon a citizen's civil liberty, as is the case with Stingray use.

Video evidence discovered during the investigations into several high-profile law enforcement shootings of unarmed civilians have discredited the officers' attempts to justify their actions based on how the victim's behavior *appeared* to them.[135] Had there been no video of these incidents, it is very likely that the officers would not have faced charges, or been found liable in a wrongful death civil action, because of strong deference historically given to a law enforcement officer's statement. It is reasonable to extrapolate that given the high percentage of cases with video evidence that show the officer's statement to be either misleading or fabricated in its entirety, that the number of cases without video evidence in which this is also true is proportionately high.[136] There is no reason to think that the culture of "testilying" only pervades cases in which violence is a factor. In fact, there is mounting evidence demonstrating that law enforcement has been, and continues to be, engaged in pervasive deception in order to use Stingrays without oversight, some examples of which point to the policies of, or direction by, federal law enforcement agencies.[137]

When analyzing why the DOJ decided to add national security threats as an exigent circumstance that can justify warrantless surveillance, the Department's historical treatment of national security threats as a reason to justify surveillance exigency should also be examined for consistency. A 2005 DOJ document titled Electronic Surveillance Issues conducted an in depth analysis of the legal authority for the Department's treatment of various issues related to the use of electronic surveillance capabilities.[138] The

---

134. *Id.*

135. *See, e.g.*, Jay Hathaway, *Video of Sam DuBose's Death Drastically Different From the Police* Report, GAWKER, June 29, 2015, http://gawker.com/video-of-sam-duboses-death-drastically-different-from-t-1720896658; Matthew Dolan, *Cleveland Police Officer Who Shot Tamir Rice Said He Had 'No Choice,' Probe Finds*, WALL ST. J., June 13, 2015, http://www.wsj.com/articles/sherrifs-report-doesn't-say-whether-cleveland-boys-death-warrants-charges-against-police-1434224512; Michael Martinez, *South Carolina Cop Shoots Unarmed Man: A Timeline*, CNN NEWS, Apr. 9, 2015, http://www.cnn.com/2015/04/08/us/south-carolina-cop-shoots-black-man-timeline/.

136. *See* Amir Efrati, *Legal System Struggles With How to React When Police Officers Lie*, WALL ST. J. (Jan. 29, 2009) (quoting Judge Alex Kozinski, Ninth Circuit Court of Appeals, "it is an open secret long shared by prosecutors, defense lawyers and judges that perjury is widespread among law enforcement officers. [the exclusionary rule] sets up a great incentive for…police to lie."); *see also* Nick Malinowski, *Testilying: Cops Are Liars Who Get Away with Perjury*, VICE (Feb. 3, 2013) ("A 1987 study from Chicago found that 76 percent of officers agreed that they frequently bent the facts to establish probable cause; 48 percent also said that judges were right in tossing police testimony as untrustworthy.") .

137. *See, e.g.*, Zetter, *supra* note 65; Zetter, *supra* note 69; Ciaramella, *supra* note 97; Fenton, *supra* note 78.

138. STEPHEN L. HARWOOD, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE ISSUES (Nov. 2005),

report quotes the legislative history regarding the passage of the ECPA, which says "[i]nterceptions conducted primarily for national security purposes, rather than to enforce the criminal law, are regulated by FISA."[139] The DOJ report clarifies this, quoting the Hon. James Carr's treatise on the Law of Surveillance which says "[t]hough not repealed upon adoption of the Foreign Intelligence Surveillance Act, the authorization in [18 U.S.C. §] 2518(7) to conduct warrantless national security surveillance has been superseded by the more stringent requirement of prior notice to a judicial officer found in 1805(e) of FISA."[140]

If the FISA preempts the ECPA regarding national security surveillance, then the DOJ cannot use the ECPA Pen Register statute as grounds for claiming exigent circumstances justifying an *ex post* warrant, and the Policy is incorrect in this regard. FISA applies to surveillance in which one party to the communication is foreign.[141] It is unclear whether FISA also applies in instances of entirely domestic terrorism. Furthermore, if FISA does not apply in a domestic only situation, how would an officer or prosecutor know which law to apply, given that they can only know one end of the facts prior to conducting the surveillance? Logically, FISA should be the applicable law in a national security situation because of the uncertainty involved in determining whether one party to the communication is foreign. If law enforcement knows the identity of all parties to a communication before the exigency arise, then the situation should not qualify as an exigency because the agency was on notice of the activity in sufficient time to request a warrant. Waiting until an exigency arises that was, or reasonably should have been, anticipated, thereby creating a situation which was not exigent but for the agent's negligence, should not be an accepted or encouraged practice. This should not be acceptable even when the circumstances clearly establish legality, much less when there are important questions surrounding the authority for such an activity.

The civil liberties that the Fourth Amendment is designed to protect are not so fungible that law enforcement agencies should be allowed to act without clear statutory authority to do so, particularly when the actions result in the labeling of a citizen as a terrorist or threat to national security. Therefore, irrespective of the parties to a communication, the FISA statute should be the governing law in situations of national security threat surveillance, and the policy to use the ECPA Pen Register statute as the basis for establishing a national security exigency is improper.

---

http://www.justice.gov/sites/default/files/criminal/legacy/2010/04/11/elec-srvlnce-issuse.pdf.

139. *Id.* at 145 (quoting the legislative history of the Sentencing Reform Act, S. REP. NO. 98-225, 98th Cong., 1st Sess., (1983).

140. *Id.* (quoting Hon. James Carr, THE LAW OF SURVEILLANCE § 3-116).

141. 50 U.S.C. § 1805(a)(2).

d. *What is the Computer Fraud and Abuse Act Doing Here?*

The Pen Register Statute's final emergency circumstance is the "ongoing attack on a protected computer (as defined by 18 U.S.C. § 1030) that constitutes a crime punishable by a term of imprisonment greater than one year."[142] This is an odd place to come across this particular legislative language, but in the context of the *Rigmaiden* prosecution, it makes sense.

The lesson that the DOJ learned from *Rigmaiden* is that it needs a policy in place that allows prosecutors to claim an exception for using a Stingray without a warrant in cases involving computer crime. The *Rigmaiden* prosecution did not want to reveal the capabilities of the Stingray technology used to track Rigmaiden's location, and as a result, the prosecution had to concede that tracking his location using a Stingray was a search within the meaning of the Fourth Amendment, and therefore required a warrant or an exigency exception.[143] Had the government not had a pre-existing warrant to legalize the Stingray location tracking, the evidence would have been suppressed under the exclusionary rule. In order to avoid this result in the future, the DOJ has proclaimed that the Stingray is a pen register, and therefore the emergency exceptions to the Pen Register warrant requirement apply.[144] Fortuitously, those exceptions include an attack on a protected computer.[145]

The historical interpretation of the Computer Fraud and Abuse Act ("CFAA") definition of a "protected computer" is particularly broad. In relevant part, a protected computer includes "any computer which is used in or affecting interstate or foreign commerce or communication."[146] This definition is as far-reaching as the plenary power of Congress to regulate interstate commerce, and it includes almost any device that contains a microchip.[147] When Congress chose this language for the CFAA and the Pen Register statutes in 1986, the purpose was for law enforcement to be able to trace the source of a computer attack through a telephone line its physical location. At that time, a connection between two computers that were not in direct proximity to one another required one computer to connect to the other via a dial-up modem. Once law enforcement obtained the phone number that

142. DOJ STINGRAY POLICY, *supra* note 109, at 4; 18 U.S.C. § 1030 (2012) (defining protected computer as one exclusively used by a financial institution, the U.S. Government, or one that is used in or affecting interstate or foreign commerce.) Essentially a protected computer is any object that connects to the Internet, or contains a microchip and was manufactured in a different state.

143. *See Rigmaiden*, 844 F. Supp. 2d at 1001.

144. DOJ STINGRAY POLICY, *supra* note 109.

145. 18 U.S.C. § 3125 (2012).

146. 18 U.S.C. § 1030(e)(2)(B) (2012).

147. Orin Kerr, *Does the Federal Computer Hacking Law Apply to a Laptop Not Connected to the Internet?*, WASH. POST, Aug. 25, 2014, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/08/25/does-the-federal-computer-hacking-law-apply-to-a-laptop-not-connected-to-the-internet/.

the attacker was using, they could easily find the location through a reverse lookup directory and arrest the perpetrator.

There is a major problem, however, with using a Stingray in this context. Courts have repeatedly held that prospective real-time cell-site location data is tracking information, and any device that collects such information is a "tracking device" as defined by the ECPA.[148] A "tracking device" under the ECPA is "an electronic or mechanical device which permits the tracking of the movement of a person or object." Note that the definition does not require that the *intended* function of a device is to collect tracking information, only that it *permits* the collection of such data.[149] Given that a Stingray is, in fact, a portable cell-site, any data that it collects that "permits the tracking of a person or object" is subject to the same statutory regulations as all tracking devices under the ECPA. The government has argued that courts are interpreting the definition of a tracking device too broadly, and that Congress intended an electronic tracking device to be a one-way radio homing device.[150] Courts have rejected this logic because the language of the statute is not ambiguous, and does not include language differentiating various types of tracking devices.[151] Even if the Court had not rejected this argument, the definition the government posits for a tracking device describes the functionality of a Stingray exactly. In fact, the DOJ training manual on electronic surveillance repeatedly discusses the Stingray's predecessor, the TriggerFish, as a "tracking device," yet they would have the courts define cell-site simulators differently when it suits their purposes at trial.[152] As Judge Smith put it, "if the tracking device label is warranted in the one case, it is warranted in the other.[153] The label should not change merely because the equipment used to obtain the tracking data belongs to the service provider rather than law enforcement."[154]

Accepting that prospective cell-site location data collected by a Stingray is properly identified as tracking information under the ECPA, can the data be collected legally under the authority of an ECPA Pen Register warrant? The CALEA states the following:

> [W]ith regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined

148. *See, e.g.*, In re App'n for Pen Register and Trap/Trace Device with Cell Site Location Authority, No. H-05-557M, 396 F. Supp. 2d 747 (S.D. Tex. Oct. 14, 2015) [hereinafter 2005 S.D. Tex. Appl.]; United States v. Espudo, 954 F. Supp. 2d 1029 (S.D. Cal. 2013).

149. 18 U.S.C. § 3117(b) (defining "tracking device" as an electronic or mechanical device which permits the tracking of the movement of a person or object).

150. *See* S. REP. NO. 541, 99th Cong., 2d Sess., at 10 (1986), *reprinted at* 1986 U.S.C.C.A.N. 3555, 3564 (defining "electronic tracking device").

151. *See 2005 S.D. Tex. Appl.* at 754.

152. *See id.* at 755, n.12 (citing U.S. DEP'T OF JUSTICE, *Electronic Surveillance Manual*, at 44-45 (rev. June 2005)).

153. *Id.*

154. *2005 S.D. Tex. Appl.* at 755.

> in section 3127 of Title 18), **such call-identifying information shall not include the physical location of the subscriber** (except to the extent that the location may be determined from the telephone number).[155]

The statutory language of the CALEA unambiguously states that the government *cannot* obtain subscriber location information solely under a pen register warrant.[156] Therefore, the DOJ policy allowing the use of Stingrays to track the real-time location of a target cellphone solely on the authority of a pen register warrant is in violation of the CALEA and Pen Register statutes. Because a Stingray collects tracking information in real-time, the Stored Communications Act is not an applicable means to cure the aforementioned statutory deficiency, therefore a hybrid theory combining a Pen Register warrant for the cellphone activity monitoring with a warrant or judicial order authorizing location data disclosure under the SCA is inappropriate for prospective real-time tracking of a target.[157]

3. The Impossibility Exception

Finally, the Policy carves out an ambiguous exception for "other circumstances in which, although exigent circumstances do not exist, the law does not require a search warrant and circumstances make obtaining a search warrant impracticable."[158] In the interest of clarity as to the precise set of circumstances that could give rise to an invocation of this exception, the Policy language requires close examination.

What circumstances, in which locations, might necessitate the mobile interception of an individual's cellphone, or require tracking a person's location via their cellphone signal, yet require neither a search warrant, nor a pen register order under any applicable Federal or state statute? This is a puzzling riddle indeed, but the issue is even more complicated. In addition to the lack of any statutory requirement of judicial oversight while monitoring an individual's cellphone or tracking his movements, the agent who is engaged in these activities must also believe that it would be impossible to apply for a search warrant under the circumstances, even though the Policy only invokes this exception in cases where no exigency exists.[159]

---

155. 47 U.S.C. § 1002(a)(2) (emphasis added).

156. *See 2005 S.D. Tex. Appl.*

157. *See* In re United States for an Order Authorizing the Disclosure of Prospective Cell Site Information, 412 F. Supp. 2d 947, 957 (E.D. Wis. 2006) (rejecting the government's hybrid authority argument as "unpersuasive"); *but cf.*, *e.g.*, In re Appl. of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (supporting the hybridization theory).

158. DOJ STINGRAY POLICY, *supra* note 109, at 4.

159. *Id.*

To summarize, the "exceptional circumstance" requiring invasive Stingray surveillance is not an emergency that permits an exception, so the Policy does require the agent to obtain a search warrant. However, because the agent says that the situation is so urgent that it would be impossible for him to apply for one, it's ok to skip the warrant this time, even though the courts and Congress have unambiguously legislated the very limited situations in which it is acceptable to forego a warrant. Additionally, the agent "must first obtain approval from executive-level personnel at the agency's headquarters *and* the relevant U.S. Attorney, and then from a Criminal Division DAAG."[160] The logic driving this strange exception is suspiciously circular. Ultimately, if an agent can satisfy all of the requirements to establish an exceptional circumstance, and then successfully obtain approval from three DOJ executives to use the Stingray, then why is it impracticable to ask an agent to follow the proper warrant application procedures? The word they should have used instead of "impracticable" is "hassle," as in, "this warrant application form is a hassle, can't I just wait until after I find out if I actually need a warrant to fill it out instead?"

It seems that until the Supreme Court rules on whether cell-site simulator use constitutes a search within the meaning of the Fourth Amendment, in any situation when an agency thinks obtaining a warrant would be "impracticable," and obtaining a Pen Register warrant is not required by state law, the agency has the option to forego the warrant requirement. The only real obstacle to doing an end run around the mandatory warrant requirement set forth in the Policy is getting a nod from three people who are actively interested in pursuing an investigation. With no clarification as to what "impracticable" means in the real-time surveillance context, there is no way to claim that using the justification is improper. The situation does not require a search warrant by law, and internal DOJ policies are non-binding guidelines, so even if the issue is raised at court, there is no justification necessary by agency officials. If the meaning implied by the Policy is the standard Oxford definition, then situations covered by this exception are limited to those in which obtaining a warrant is "impossible in practice to do or to carry out."[161] Given how flexible the available options are to obtain a warrant in the information age via pay phone, cell phone, business phone, email, fax, over the Internet, or even by knocking on a magistrate's door, it should be a rare event indeed for the "impossibility exception" to ever be invoked. (Disclaimer: continuing to read this indemnifies me from any liability for damages to body or property incurred at the hands of said magistrate.) It will certainly be worth monitoring the coming years to see how many times the "impossibility exception" is used in practice, given how extremely narrowly tailored the circumstances should be in reality.

160. *Id.* (emphasis added).

161. *Oxford English Dictionary* (online ed. 2015) (last visited Oct. 4, 2015), http://www.oxforddictionaries.com/us/definition/american_english/impracticable.

IV. FCC REGULATIONS PROHIBIT CELLPHONE SIGNAL JAMMING BY STATE AND LOCAL LAW ENFORCEMENT AGENCIES

FCC regulations prohibit signal jamming in all but very narrowly proscribed federal law enforcement activities.[162] Stingray devices are capable of jamming cell signals as part of the mechanism used to force devices to connect to the simulated tower. By jamming other signals, the Stingray becomes the strongest tower signal available and devices automatically opt for the stronger signal to maintain connectivity.[163] This practice violates FCC rules prohibiting signal jamming, and there should be further investigation into the potential for the Stingray to interfere with wireless communications.

An enforcement advisory released by the FCC in December 2014 states that "[f]ederal law provides no exemption for use of a signal jammer by [. . .] police departments, or other state and local authorities. Only federal agencies are eligible to apply for and receive authorization."[164] If the speculation that Stingrays use signal jamming is accurate, then they are an illegal device and the FCC should enforce the prohibition of their sale to, and use by, state or local law enforcement agencies. However, therein lies the primary problem in determining whether Stingrays are legal or not, without a mechanism for judicial or congressional oversight of the capabilities of Stingrays, the legality of these devices is mere speculation.

While investigating a bank robbery case in New Jersey, Assistant U.S. Attorney Osmar Benvenuto submitted a pen register warrant application in 2012 for the authorization of Stingray surveillance, and in the sworn affidavit, he states "[b]ecause of the way the Mobile Equipment sometimes operates, its use has the potential to intermittently disrupt cellular service."[165] This sworn statement shows that there should be a heightened concern about the interference caused by Stingray use, and that the FCC should take more stringent action restricting the distribution of these devices to state and local officials due to their signal jamming potential.

---

162. *See* 47 U.S.C. § 302a(b).

163. *See* Cyrus Farivar, *Cities Scramble to Upgrade "Stingray" Tracking as End of 2G Network Looms*, ARS TECHNICA (Sept. 1, 2014) ("Handsets operating in 2G will readily accept comm. from another device purporting to be a valid cell tower, like a stingray. So the stingray takes advantage of this feature by jamming the 3G and 4G signals, forcing the phone to use a 2G signal.").

164. FCC, Enforcement Advisory No. 2014-05 (Dec. 8, 2014), https://apps.fcc.gov/edocs_public/attachmatch/DA-14-1785A1.pdf.

165.Cyrus Farivar, *To Locate Bank Robber FBI Unusually Asked for Warrant to Use Stingray*, ARS TECHNICA (Mar. 3, 2015).

V. THE FCC SHOULD REQUIRE WIRELESS CARRIERS TO FOLLOW THE ENCRYPTION STANDARDS ESTABLISHED BY THE COMMUNICATIONS SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL

The FCC regulates surveillance equipment for use by law enforcement under 47 C.F.R. § 15.511 pursuant to 47 U.S.C. § 301. The FCC has been under pressure to investigate the use of cell-site simulators for some time now[166], and has recently formed a task force to investigate potential abuses of cell-site simulators by foreign intelligence services and private individuals.[167] There has been no action taken to investigate abuses by government agencies that purchase the devices under the authority of the FCC.[168] Chairman Wheeler responded to concerns raised in a letter from Rep. Alan Grayson by deferring authority over the enforcement and legality of the use of Stingrays to the FBI, the Department of Homeland Security, and the Department of Justice.[169] This is an interesting position to take considering that the FCC issues the licenses for manufacturing and marketing of these surveillance devices.[170] It would appear to be within FCC jurisdiction to determine the legality of a device prior to issuing a license for its manufacture. Wheeler did state, however, that Title III of the Communications Act gives the FCC "statutory authority to address the threat posed by illicit IMSI catchers and to work closely with [the] industry on mechanisms to secure our nation's wireless networks and to ensure the privacy of consumers' conversations."[171] A key step toward both of these goals is to enhance the encryption standards and security features for all devices communicating over wireless networks.

166. Letter from Alan Grayson, House of Representatives, to Tom Wheeler, Chairman of the FCC (July 2, 2014) (submitting questions to the Chairman to determine what can be done to limit the danger of IMSI catchers).

167. *See* Craig Timberg, *Feds to Study Illegal Use of Spy Gear*, WASH. POST (Aug. 11, 2014).

168. See *id.*

169. *See* Letter from Tom Wheeler, Chairman of the FCC, to Alan Grayson, House of Representatives (Aug. 1, 2014).

170. *See* Letter from Julius Knapp, Chief of the Office of Engineering and Technology, FCC, to Christopher Soghoian, Center for Applied Cybersecurity Research (Feb. 29, 2012) (providing license ID numbers for Stingray and other Harris Corp. surveillance devices in response to a FOIA request), http://files.cloudprivacy.net/FOIA/FCC/fcc-stingray-reply.pdf.

171. *Id.*

A. Why the FCC Should Enact a Rule Requiring All New Cellular Devices to Comply with the Encryption Standards Established by the CSRIC Prior to License Issuance

The FCC has long been tasked with protecting the privacy interests of the American public. Under the Telephone Consumer Protection Act, the FCC and the FTC limit unsolicited telemarketing calls.[172] The FCC's caller ID rules mandate that consumers be able to block their phone numbers from being visible to the person receiving the call.[173] Another rule protects the privacy of personal telephone records.[174] One of the primary roles of the FCC is to protect the privacy of communications against unwanted intrusion, so it is reasonable to think that the agency has the authority to enact regulation preventing an unknown third party from accessing the data transmitted to or from a person's cellphone without his or her knowledge or consent.

In 2011, the FCC established the Communications Security, Reliability, and Interoperability Council ("CSRIC").[175] One of the directives of the CSRIC is to "develop and recommend best practices and actions the FCC can take to improve the security of mobile devices and networks."[176] The cybersecurity best practices established by the 2011 council state the following regarding encryption practices in the industry.

> [W]hen network operators, service providers, and equipment suppliers use an encryption technology in the securing of network equipment and transmission facilities, cryptographic keys must be distributed using a secure protocol that a) ensures the authenticity of the recipient; *b) does not depend upon secure transmission facilities, and c) cannot be emulated by a non-trusted source*.[177]

Given the widespread use of Stingrays, it is clear that industry leaders failed to implement these practices. If the industry had followed the CSRIC's encryption practices, then the Stingray would not be able to trick devices into connecting to the false signal because the encryption would be authenticated locally on the device and at the provider's network hub rather than at the cell tower. This would dramatically limit the possibility of over-

172. 47 U.S.C. § 227; *see also* PROTECTING YOUR PRIVACY, FCC (Mar. 31, 2014).

173. 47 C.F.R. § 64.1601(d) (mandating the use of *67 to block caller ID)

174. 47 C.F.R. § 64.2005 (governing the use of customer proprietary network information without customer approval).

175. *See generally* CHARTER OF THE FCC'S COMM. SECURITY, RELIABILITY, AND INTEROPERABILITY COUNCIL, FCC (Mar. 19, 2013), http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20Charter%20Renewal%202013.pdf.

176. *Id.*

177. FCC, CSRIC BEST PRACTICES: CYBERSECURITY & ENCRYPTION, No. 9-6-8028 (emphasis added).

the-air interception because without the decryption key, either the interceptor would have to spend significant time to crack the encryption, or the device owner or service provider would have to provide access. This modification to cellular technology would not only secure the networks against interception by nefarious parties, but would also act as a check and balance against the power of law enforcement in much the same way as the CALEA defines the standards telecom companies must follow in providing surveillance access. It is unfortunate that the findings of the CSRIC have been largely ignored by the telecom industry. The reasons why there is such reluctance to move toward better security are unclear. It is clear, however, that so long as cellular devices remain subordinate to cell-sites in determining what level of encryption to use, Stingrays will easily be able to bypass cellular security by instructing the device to use zero encryption, effectively undermining the entire security protocol.

Law enforcement agencies vehemently oppose enhanced security standards for cellular equipment. In 2014, when Apple and Google began configuring their new cellular devices with local encryption enabled by default that the manufacturer cannot decrypt, the FBI publicly expressed outrage at the idea that law enforcement would no longer have ready access to data from these devices, arguing that added security poses a significant threat to national security.[178] While local encryption does not directly impact the ability of the Stingray to intercept over-the-air communications, it is notable to see the fervor with which law enforcement agencies respond to companies increasing encryption security. They argue that increasing encryption poses a national security concern, given how much information is stored on a cellular device, and how helpful that information can potentially be in prosecuting criminal activity, including terrorism.[179] When considering the value of an additional layer of communication security, we must consider more than just law enforcement's desire for access to private information when we balance the risks against the rewards of such an advancement. It is also the case that should carriers implement end-to-end encryption as suggested by the CSRIC, that law enforcement would still be able to access encrypted communications, they would simply need to obtain a court order to do so as has been the case since the implementation of the CALEA.

The NSA is also gravely concerned about the mounting public pressure on and by lawmakers to strengthen encryption, which would have a dramatic impact on the agency's ability to intercept communications. Reports surfaced that in 2010, Gemalto, the SIM card manufacturer that provides chips to AT&T, Verizon, T-Mobile, and Sprint, was hacked into by Britain's Government Communications Headquarters ("GCHQ"), with support from the NSA, for the sole purpose of stealing SIM card encryption

178. Bob Orr, *Are Impenetrable Phones a Threat to National Security*, CBS NEWS (Oct. 16, 2014).

179. *See id.*

keys.[180] The presentation from GCHQ, which was leaked from the NSA by Edward Snowden, declares "GEMALTO – successfully implanted several machines and believe we have their entire network."[181] By stealing SIM card encryption keys, governments can decrypt communications in real-time, which affects billions of cellphone users around the world.[182] Perhaps this act by the NSA demonstrates how well encryption actually works. It is logical that if wireless carriers move their encryption authentication away from the cell towers as suggested by the CSRIC, then one of the largest security problems with wireless networks would be resolved, rendering Stingrays ineffective unless law enforcement possesses the encryption key for an individual user. This security method would not cause compliance problems with the CALEA because telecom companies can still provide either backbone access for legitimate government surveillance, or the decryption key for individual subscribers pursuant to a court order permitting mobile surveillance.

The FCC has taken important steps toward secure telecommunications by establishing cybersecurity best practices at the policy level through the efforts of the CSRIC. However, there are currently no mechanisms for enforcing the standards, and further, federal law enforcement agencies are publicly opposing the efforts made by companies who follow them. This sends mixed signals to the industry, and it is the FCC's role as an independent regulatory agency to require compliance with established standards, regardless of outside pressures. In this particular case, the FCC should issue a rule that requires carriers to adhere to the CSRIC encryption standard in order to have new device licenses approved. Prominent members of the telecom industry established the encryption recommendations, so it should not be onerous to require compliance. This would not require retrofitting all devices, and could be phased in over time allowing companies to adopt the new encryption protocol without significantly disrupting their business models.

B. Title II of the Communications Act Grants the FCC the Authority to Regulate the Encryption Standards of Cellular Device Manufacturers and Service Providers

With the adoption of the Open Internet Order by the FCC, Title II of the Communications Act now regulates mobile broadband service. This is critically important to the regulation of wireless services because in the near future a majority of wireless carriers will convert their voice networks to

180. Jeremy Scahill & Josh Begley, *The Great SIM Heist: How Spies Stole the Keys to the Encryption Castle*, THE INTERCEPT (Feb. 19, 2015).

181. Jeremy Scahill & Josh Begley, *CNE Access to Core Mobile Networks*, THE INTERCEPT (Feb. 19, 2015), https://firstlook.org/theintercept/document/2015/02/19/cne-access-core-mobile-networks-2/.

182. *See* Scahill, *supra* note 180.

strictly IP based communications (Voice over 4G/LTE).[183]This change will put all voice communications squarely under the purview of Title II because all cellular IP traffic travels across mobile broadband networks. Title II contains a provision requiring telecommunications carriers to protect the privacy of customer information.[184] 47 U.S.C. § 222(a) requires "every telecommunications carrier [. . .] to protect the confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers."[185] If "proprietary information" includes data like user account information, browsing records, text messages, and location data, then the FCC has an obligation to enforce the statute against wireless carriers in the form of baseline encryption standards because data that can easily be intercepted is not adequately protected. The most comprehensive method of enforcement would be mandatory adherence to the established CSRIC best practices for encryption of mobile communications, which would secure customer's proprietary information against interception by third parties as implicitly required by 47 U.S.C. § 222(a).

VI. THE FCC SHOULD REQUIRE SIM CARD MANUFACTURERS TO ENABLE CONSUMER ACCESS TO EXISTING SECURITY OPTIONS THAT ARE CURRENTLY DISABLED

The option to notify a wireless user when the device receives a request to connect to an unencrypted tower is available, but permanently disabled by the SIM card manufacturer at the request of wireless carriers.[186] The carriers appear to be unwilling to enable this option of their own accord because enabling the option increases the volume of customer support calls.[187] While it is clearly preferential to the carriers to do business this way, it is in the best interest of customer security and privacy to allow the consumer to choose to receive notification about encryption failures.

The FCC has forced carriers to enable existing functions in the past. In 2013, the FCC "reached a deal with [. . .] major U.S. wireless carriers that requires the carriers to disclose how and when cellphones on their network can be unlocked."[188] While the purported goal of that agreement was to foster innovation and consumer choice, it seems that improving consumer security

183. *See* Marguerite Reardon, *The New Age of Wireless Calling*, CNET (Aug. 30, 2014).

184. 47 U.S.C. § 222.

185. 47 U.S.C. § 222(a).

186. *See* Felician Alecu & Paul Pocatilu, *Enabling the Ciphering Indicator on Android*, 6 J. OF MOBILE EMBEDDED & DISTRIBUTED SYS. 52, 55 (2014), http://www.jmeds.eu/index.php/jmeds/article/viewFile/Enabling_the_Ciphering_Indicator_on_Android/pdf_4.

187. *See id.*

188. Dara Kerr, *The Ban on Unlocking Phones is Lifted as Regulators and Carriers Finally Work Out the Details of the New Policy*, CNET (Dec. 12, 2013).

is a goal that the FCC should be very interested in pursuing. Indeed, Congressman Grayson stated in a letter to Chairman Wheeler that:

> Americans have a reasonable expectation of privacy in their communications, and in information about where they go and with whom they communicate. It is extremely troubling to learn that cellular communications are so poorly secured, and that it is so easy to intercept calls and track people's phones.[189]

The rewards of enabling a notification option that alerts consumers before transmitting their data over an insecure network are vastly more beneficial than the minor task of flipping the on switch at the SIM card manufacturer. Device manufacturers can disable the option by default if they so choose, but ultimately, the consumer should be empowered to choose his or her own security level, rather than being forced into insecurity by a company's cost-avoidance tactic.

VII. CONCLUSION

Both federal and state governments, even in light of the recent DOJ Stingray Policy, are insistent on protecting the secrets of the Stingray from public scrutiny under the auspices of national security and criminal justice. However, if security and justice are their true motives, the policy of secrecy is an utter failure. Countless criminal convictions are now under scrutiny for due process violations because investigators did not disclose their surveillance methods not only to the judges, but also to the district attorneys that prosecuted the cases. Evidence obtained using a Stingray is often inadmissible in criminal trials because law enforcement agencies refuse to disclose their surveillance methodologies in violation of a defendant's rights, allowing criminals to walk free who would otherwise be in jail. The argument that allowing the capabilities of a Stingray to become public would make criminals harder to investigate is fallacious if the evidence gathered to convict those very criminals is left out of the trial once they are caught, or worse, results in a reversal or appeal of the conviction at massive taxpayer expense. That is to say nothing of the privacy concerns that widespread use of covert surveillance raises for law-abiding citizens, or the potential for civil rights violations stemming from unsanctioned and unmonitored surveillance by the government.

Since its inception, the United States has placed a high value on strong protections against intrusions by the government, whether it was opposition to general warrants under the rule of King George, or objections to the modern federal government intruding on private communications using covert technology. Americans still value their privacy. It may seem

189. Letter from Alan Grayson, House of Representatives, to Tom Wheeler, Chairman of the FCC (July 2, 2014) (submitting questions to the Chairman to determine what can be done to limit the danger of IMSI catchers).

that the opposite is true in the age of Facebook, Instagram, and twitter, but there is a clear distinction between an individual having an option to trade some of his privacy for convenience, and the government sneaking around, covertly monitoring law-abiding citizens' cellphone communications, giving the public no say in the matter at all.

If a public debate had been held to decide whether society is willing to trade its privacy for a sense of security that would be one thing. However, this practice has been going on for twenty years or more without a single piece of legislation enacted to limit the use of Stingrays or to provide oversight to prevent the abuse of this technology. Recently, the use of the Stingray was held to be a search within the meaning of the Fourth Amendment, and the Supreme Court has held that any search of a cellphone requires a warrant. The problem is that law enforcement officers have displayed their willingness to deceive judicial officials; therefore, it is difficult to believe that the practice will stop based on judicial holdings and policy documents alone. As Stephanie Pell eloquently said, "the communications of Americans will only be secured through the use of privacy enhancing technologies like encryption, not with regulations prohibiting the use or sale of intercepting technology."[190]

The FCC needs to act in order to ensure that cellular communications remain private, at least and until Congress decides to investigate and act on this issue. Defending the privacy of American citizens' communications against abuse by the use of secretive technology falls to the FCC. The abuses by law enforcement agencies are a symptom of a larger problem, which, if left unchecked, could lead to national security breaches, stolen trade secrets, espionage, or even terrorist activity, if it has not already. An insecure communications network is the Achilles heel of a strong nation, and while unchecked mass surveillance by law enforcement is profoundly disturbing, the thought that anyone with moderate technical knowledge and a few hundred dollars in their pocket can eavesdrop on 99% of our communications is terrifying. The FCC must take the steps necessary to secure the homeland against this very real and rapidly growing threat.

190. Stephanie Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore: The Vanishing Government Monopoly over Cellphone Surveillance and its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 6 (Fall 2014).