SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Law Review

Volume 68 | Issue 1

2017

From Historical Cell-Site Location Information to IMSI-Catchers: Why Triggerfish Devices Do Not Trigger Fourth Amendment Protection

Kristi Winner

FROM HISTORICAL CELL-SITE LOCATION INFORMATION TO IMSI-CATCHERS: WHY TRIGGERFISH DEVICES DO NOT TRIGGER FOURTH AMENDMENT PROTECTION

CONTENTS

INTRODUCTION

In 2011, major cell service providers in the United States received over 1.3 million requests from law enforcement officials for customer records.[1] Typically, these requests are made due to an ongoing

1. Will Oremus, *Law Enforcement Wants Your Private Cellphone Data. Wireless Carriers Will Hand it Over, for a Fee*, SLATE (July 9, 2012, 5:10 PM), http://www.slate.com/blogs/future_tense/2012/07/09/ed_markey_wireless_

criminal investigation in which the government seeks to prove that a suspect was near a certain location at a certain time based on cell-site location information ("CSLI") recorded by the service providers. In short, CSLI is a record of the cell towers to which the user's cell phone connects when the user places and ends a phone call. This, in turn, indicates an approximate location of the cell phone. Usually, law enforcement only needs a court order to make these requests.

Take, for example, *United States v. Carpenter*.[2] In 2011, Police arrested four men suspected of robbing various RadioShack and T-Mobile stores in the Detroit, Michigan area.[3] One of the men confessed that the group had robbed nine stores in Michigan and Ohio, and he also implicated fifteen other men.[4] The man provided the FBI with the phone numbers of some of the participants.[5] The FBI then obtained court orders to acquire "transactional records" from the particpants' cell service providers for sixteen phone lines.[6] The magistrate required a showing of "specific and articulable facts" that demonstrate "there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation" to issue the orders.[7] The records included cell-site location information that helped to prove that two of the suspects were within a half-mile to two miles of several robberies at the time that they occurred.[8] These two suspects, Timothy Carpenter and Timothy Sanders, were subsequently convicted of nine armed robberies in violation of the Hobbs Act.[9] The two men appealed their convictions and sentences to the United States Court of Appeals for the Sixth Circuit. They argued that their cell-site location information should have been suppressed because acquiring the records constituted a search under the Fourth Amendment, and therefore the police needed a warrant supported by probable cause.[10] The Sixth Circuit rejected this argument. The court held that the government's collection of business records containing

surveillance_report_law_enforcement_requests_private_cell_phone_data_1_3_million_times_a_year.html [https://perma.cc/5JNH-32G9].

2. 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

3. *Id.* at 884.

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.*

8. *Id.* at 885.

9. *Id.* at 884–85.

10. *Id.* at 885–86.

cell-site data was not a search under the Fourth Amendment because the user voluntarily relinquished the information to a third party, the service provider.[11] On June 5, 2017, the Supreme Court granted certiorari to hear *Carpenter* in its next term.[12]

Although the police regularly collect CSLI without a warrant, and no apparent circuit split exists that would require Supreme Court review, the issue is ripe for certiorari. Major cell providers' growing unwillingness to cooperate with law enforcement, even with court orders or warrants—likely due to public pressure and uncertainty in the law[13] —has caused law enforcement to engage in self-help to obtain the information themselves. United States law enforcement agencies also use devices capable of collecting CSLI in real-time. These devices are most often referred to as an IMSI-catcher, "StingRay," or "TriggerFish." Circuit courts disagree about whether cell phone users have a reasonable expecation of privacy in their CSLI if law enforcement collects the data rather than cell phone service providers. Whichever way the Supreme Court decides *Carpenter*, the Court's ruling—no matter how narrow—will affect how law enforcement must treat collection of CSLI.

Just as cell phones have become ubiquitous with modern day life, so has a certain relinquishment of privacy. This Comment argues that the Court's analysis of the Fourth Amendment's intersection with modern technology should distinguish between the communications' content and metadata such as CSLI because CSLI does not protect the user's reasonable expectation of privacy.

Part I explains the underlying technology that allows cell phones to interact with cell towers and discusses the differences between historical cell-site location information that cell service providers keep in the regular course of business and prospective cell-site location information. Part II then provides a brief history of United States law enforcement's use of IMSI-catchers and the technology that enables their use. Part III discusses the statutes under which law enforcement has authority to gather historical and prospective cell-site location information from cell service providers and to utilize their own IMSI-catchers. Part III explains state and federal laws that have been en-

11. *Id.* at 885–90.

12. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

13. *See, e.g.*, David Kravetz, *AT&T Demands Clarity: Are Warrants Needed for Customer Cell-Site Data?*, ARS TECHNCIA (Nov. 18, 2014, 9:10 AM), https://arstechnica.com/tech-policy/2014/11/att-demands-clarity-are-warrants-needed-for-customer-cell-site-data/ [https://perma.cc/F49M-EN3Z] (explaining AT&T's confusion and frustration regarding the requirements to release user's data to law enforcement).

acted specifically to address government use of IMSI-catchers. Part IV summarizes the Supreme Court's Fourth Amendment precedent relevant to cell-site tracking and illustrates how Circuit courts have applied it in the context of historical and prospective CSLI and the use of IMSI-Catchers. Finally, Part V analyzes the Fourth Amendment jurisprudence as applied to IMSI-Catchers and concludes that cell phone users do not possess a reasonable expectation of privacy in their cell-site location information.

I. THE BASICS OF CELLULAR TECHNOLOGY, CSLI, AND IMSI-CATCHERS.

Collection of CSLI can be separated into three categories: (1) historical CSLI, such as the stored information obtained from cell service providers in *Carpenter*; (2) prospective CSLI, that is, the collection of CSLI in real-time from a cell service provider; and (3) prospective CSLI obtained by use of an IMSI-catcher. To understand the privacy implications pertaining to each category, it is essential to understand cellular technology and how the information is obtained by service providers and law enforcement.

A. Historical Cell-Site Location Information.

Wireless cell phone service operates through radio signaling, in which the cell phone device communicates with antenna towers operated by a service provider.[14] Each cell phone service provider has its own infrastructure of radio base stations, also referred to as "cell sites," throughout its geographical coverage area.[15] These cell sites have antennas that detect radio signals from cellular phones to create a connection to the cellular network.[16] A cell site typically contains three antennas that point in opposite directions 120 degrees apart,[17] splitting the cell site into three pie-slice shaped "sectors." As long as the cellular telephone is powered on, it automatically searches for cell

14. ELEC. SURVEILLANCE UNIT, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL: PROCEDURES AND CASE LAW FORMS 178 n.41 (2005), https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf [https://perma.cc/EB6Z-MFEH] [hereinafter DOJ 2005 MANUAL].

15. *ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 20 (2010) [hereinafter *ECPA Judiciary Hearing 2010*] (statement of Professor Matt Blaze, University of Pennsylvania).

16. *Id.* at 13.

17. Judge Herbert B. Dixon Jr., *Scientific Fact or Junk Science? Tracking a Cell Phone Without GPS*, JUDGES' J., Winter 2014, at 37, 37–38.

towers to connect to by sending out signals or "pings" to identify itself to nearby cell sites.[18] The cellular phone typically connects to a sector facing the direction of the phone from the closest cell site with the strongest connection.[19] When the cell phone reaches a cell-site sector and identifies itself, the cell site receives the cell phone's mobile electronic serial number (ESN),[20] international mobile subscriber identity number (IMSI),[21] and international mobile station equipment identity number (IMEI).[22] This process is termed "registration."[23]

Cellular phones ping cell towers roughly every seven seconds.[24] A cellular device often receives a signal from more than one antenna[25] and, if needed, the cellular device can reconnect to one of the additional six sectors.[26] The pings identify which cell-site sector can provide the strongest connection for the device.[27] Although a cellular device may register with more than one cell-site sector, the cellular device "camps" on the sector providing the strongest signal.[28] This process is essential for a cell phone to make and receive calls. When a cell phone is idle and receives a page from another cell phone attempting to connect, it responds by paging whichever cell-site sector it is camped on, and the call is then placed upon that sector.[29]

Whenever the user places or receives a call, the cell phone provider receives this information from its network and records where

18. DOJ 2005 MANUAL, *supra* note 14, at 178 n.41.

19. Dixon, *supra* note 17, at 38.

20. An ESN is a unique identifier for each actual cellular telephone device. DOJ 2005 MANUAL, *supra* note 14, at 177 n.36.

21. An IMSI is a unique identifier for the SIM card inside of the cellular telephone device. *Id.* at 177 n.37.

22. *Id.* All SIM-card based cell phones contain an IMEI number that remains the same even if the SIM card is removed. *See* Mir Ubaid, *Can You Hear Me Now? How Police Track Your Cell Phone*, TOM'S GUIDE (Oct. 14, 2015, 9:38 AM), https://www.tomsguide.com/us/cellphone-tracker-stingray,news-21718.html [https://perma.cc/VF3K-SJU8].

23. Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426 (2007).

24. *Id.*

25. Dixon, *supra* note 17, at 38.

26. *See* Transcript of Record at 9, United States v. Sims, No. 2:07-cr-00298 (E.D. Pa. Nov. 13, 2007) (testimony of William Shute).

27. *Id.*

28. Heath Hardman, *The Brave New World of Cell-Site Simulators*, 8 ALB. GOV'T L. REV. 1, 18 (2015).

29. Transcript of Record, *supra* note 26, at 9.

the cell tower is located and which of the three sectors covered by that tower is serving the user's phone.[30] This information is known as historical CSLI. The type of information recorded includes: the personal telephone number, date, time the call was initiated, duration of the call, whether the call was inbound or outbound, and the cell site(s) and sector(s) to which the phone was connected when the call was initiated and terminated.[31] The cell-site sector in which a call is terminated is often not the same cell-site sector in which the call was made. This is because the cell device searches for the strongest connection while the user is on the phone, and it switches from one cell site to another without any interruption to the phone call or notice to either party on the call.[32] Service providers retain historical CSLI for various amounts of time, typically from one to two years.[33]

A particular cell-site sector to which a user is connected does not necessarily provide an accurate description of where the phone is located. Historical CSLI can be useful to locate a cell phone within a general area or, in particular, to reveal the direction someone is traveling over long distances as they repeatedly switch towers in a particular direction.[34] A cell device does not always connect to the closest cell tower relative to its location. Cell phone signals "are in a frequency range that travels in a straight line and has limited penetration capabilities."[35] Therefore, structures such as buildings and tunnels can prevent a cell phone from connecting to a nearby tower.[36] The size of the cell-site sector's geographical coverage also plays a role in how precisely CSLI can determine a cell phone's location.[37] In more heavily

30. *See ECPA Judiciary Hearing 2010, supra* note 15, at 13–14 (testimony of Professor Matt Blaze, University of Pennsylvania) (explaining how phone companies know where to route incoming phone calls).

31. Transcript of Record, *supra* note 26, at 15, 19.

32. *Id.* at 11.

33. *See* Patrick Siewert, *Cellular Provider Record Retention Periods*, FORENSIC FOCUS (April 18, 2017), https://articles.forensicfocus.com/2017/04/18/cellular-provider-record-retention-periods/ [https://perma.cc/R8NJ-9D3H].

34. Mike Masnick, *Turns Out Cell Phone Location Data Is Not Even Close to Accurate, but Everyone Falls for It*, TECHDIRT (Sept. 9, 2014, 7:56 AM) https://www.techdirt.com/articles/20140908/04435128452/turns-out-cell-phone-location-data-is-not-even-close-to-accurate-everyone-falls-it.shtml [https://perma.cc/WU9N-J84X].

35. Bert Markgraf, *How Far Can a Cell Tower Be For a Cell Phone to Pick Up the Signal?*, CHRON, http://smallbusiness.chron.com/far-can-cell-tower-cellphone-pick-up-signal-32124.html [https://perma.cc/5ZW3-G4QW] (last visited Sept. 19, 2017).

36. *Id.*; Dixon, *supra* note 17, at 38.

37. *ECPA Judiciary Hearing 2010*, *supra* note 15, at 23-24 (Statement of Professor Matt Blaze, University of Pennsylvania).

populated areas in which more cell coverage is needed, coverage typically extends a few blocks.[38] In rural areas, however, cell-site coverage can vary from a quarter of a mile to several miles.[39] Due to the growing popularity of cell phone use in recent years, the number of cell sites has increased, and the size of cell-site sectors has steadily decreased.[40] In turn, the accuracy of historical CSLI relative to the cellular phones actual location will increase as service providers provide better coverage.[41]

B. Prospective Cell-Site Location Information

Cell phone service providers can also actively collect user's CSLI in "real-time." This is known as prospective CSLI. In doing so, providers "ping" the cell phone and locate the nearest cell site to the cellular device at any time the phone is powered on.[42] Service providers can also obtain a much more accurate prediction of a cell phone's location by triangulation. Triangulation pinpoints the cell phone's location by:

> [C]omputing the distance between the cell device and three antennas based on the time delay of the signal between the device and each antenna, and drawing a circle around each tower, with each circle having a radius of the phone's distance from that tower. The circles will intersect to pinpoint the location of the phone.[43]

38. Tim De Chant, *Why Your Cell Phone Drops Calls in Dense Cities*, CITYLAB (Sept. 23, 2011) https://www.citylab.com/life/2011/09/cell-phones-anddensity/172/[https://perma.cc/DN8P-XBPY].

39. *See* Chris Silver Smith, *Cell Phone Triangulation Accuracy Is All Over the Map*, SEARCH ENGINE LAND (Sept. 22, 2008, 4:59 PM), http://searchengineland.com/cell-phone-triangulation-accuracy-is-all-over-the-map-14790 [https://perma.cc/DVC8-G5KY].

40. *ECPA Judiciary Hearing 2010, supra* note 15, at 24–25 (Statement of Professor Matt Blaze, University of Pennsylvania). *See also Wireless Snapshot 2017*, CTIA, https://www.ctia.org/docs/default-source/default-document-library/ctia-wireless-snapshot.pdf [https://perma.cc/35G4-VUQJ] (last visited Oct. 4, 2017) ("At the end of 2016, a record 308,334 cell sites were in operation, representing growth of over 57 percent in the last ten years.").

41. Dixon, *supra* note 17, at 39.

42. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 131 (2012).

43. *See* Dixon, *supra* note 17, at 38.

In other words, triangulation creates a Venn diagram of three cell sites to which the cell phone has connected, and the overlap of the diagram is the area the cellular device is likely located.

Triangulated cell-site data is generally only available prospectively because cell service providers typically do not routinely record the data.[44] However, cell service providers can utilize triangulation to locate the source of incoming 911 calls.[45] The Federal Communications Commission requires cell service providers to maintain the ability to locate, with certain accuracy, the location of any cell phone that makes a 911 call within their network.[46] Otherwise, cell service providers typically do not store triangulated data as historical CSLI.

II. IMSI-CATCHERS.

An IMSI-catcher is a device used by law enforcement that simulates the signals emitted by cell towers in order to enable a target cell phone to register with it.[47] The target cell phone is unable to distinguish the device from authentic cell service provider infrastructure.[48] This allows the device to "catch" the same type of data that a normal cell tower receives from cell phones upon registration.

The capabilities of IMSI-catchers and to what exent they are utilized in practice by law enforcement in the United States was once unclear. Government use of IMSI-catchers and other cell phone surveillance technology had been deliberatly concealed. In recent years, due to pressure from interested parties, the U.S. Department of Justice has announced its policy on the federal government's use of StingRay devices, and the overall transparency of IMSI-Catcher use has improved on the federal, state, and local levels.

---

44. *See* Pell & Soghoian, *supra* note 42, at 128.

45. *Id.*

46. *See* 47 C.F.R. § 20.18(h) (2014) (setting location accuracy and reliability standards for cell phone calls within certain areas).

47. *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183, 183, 185 (2014) ("Cell site simulators are an electronic surveillance device that mimics a cell tower causing all nearby cell phones to register their data and information with the cell site simulator. Law enforcement increasingly relies on these devices during the course of routine criminal investigations.").

48. *Id.* at 192. IMSI-catchers take advantage of cell phone devices operating on 2G connections because they do not require authentication of cell sites to register with them. Ubaid, *supra* note 22. IMSI-catchers are also capable of forcing 3G and 4G connections to temporarily downgrade to 2G to avoid authentication. *Id.* It is believed that newer models of IMSI-catchers can directly register with cell phones operating on a 4G network without downgrading the connection to 2G. *Id.*

A. Origins—The Birth of the StingRay.

The United States originally developed cellular surveillance technology for military surveillance purposes.[49] Law enforcement followed suit and began using the devices in the early 1990s.[50] Originally, U.S. agencies utilized the technology to test cellular phones.[51] But soon enough, cellular equipment manufacturers developed and sold cellular surveillance products specifically for government surveillance use.[52] By 1991, Harris Corporation, the leading manufacturer for cell phone surveillance technology in the United States, began marketing its products to the general law enforcement community.[53]

Today, United States federal law enforcement uses IMSI-catchers which are manufactured by Harris Corporation and marketed under the name "StingRay."[54] IMSI-catchers have become colloquially referred to as StingRay devices when referring to United States law enforcement's use of them. Other common names used to describe StingRay devices or IMSI-catchers include Kingfish, TriggerFish, Amberjack, or Hailstorm, among others.[55] However, these terms originate from different surveillance products manufactured by the Harris

49. John Kelly, *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY, http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsapolice/3902809/ [https://perma.cc/FU9X-SN8U] (last visited Sept. 27, 2017).

50. Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J.L. & TECH. 1, 14 (2014).

51. *Id.*

52. *Id.*

53. *See, e.g.*, Glen L. Roberts, *Who's on the Line? Cellular Phone Interception at Its Best*, http://gbppr.dyndns.org/~gbpprorg/2600/harris.txt [https://perma.cc/83QE-99GZ] (last visited Sept. 27, 2017) ("[T]he cellular phone monitoring equipment is sold only to the law enforcement market.").

54. *See* Ryan Gallagher, *Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 1:00 PM), https://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/2/ [https://perma.cc/K4DZ-5CVQ] (explaining that Harris Corporation manufactures StingRay devices and keeps a "code of silence" to attempt to deter others from creating similar devices and that records show exclusive dealings between Harris Corp. and government agencies).

55. *Id.*; United States v. Lambdis, 197 F. Supp. 3d 606, 609 (S.D.N.Y. 2016) ("A cell-site simulator" is "sometimes referred to as a 'StingRay,' 'Hailstorm,' or 'TriggerFish.'").

Corporation.[56] Although these devices may possess similar capabilities to that of an IMSI-catcher or StingRay, in the sense that they can track locations of cellular phones, the technology behind the devices is dissimilar.[57]

Although federal law enforcement once used Harris' TriggerFish device, the device no longer appears to be manufactured.[58] In 1995, FBI agents used a TriggerFish to locate infamous computer hacker, Kevin Mitnick.[59] The TriggerFish simulated a cell site in order to locate Mitnick's phone.[60] Although the TriggerFish device had the same capabilities as a StingRay device, the extent of the device's capabilities is unclear. The product was originally marketed in 1991 as a type of wireless wiretap device capable of eavesdropping on phone calls,[61] but it is unknown whether law enforcement used the device for this purpose. Nonetheless, this benchmark helps predict how long law enforcement has been utilizing this type of cell phone surveillance technology.

It is unclear when the StingRay device was introduced to the market, but the U.S. Trademark Office lists the device as registered in 2003.[62] The public learned of the government's use of StingRay devices for the first time in 2012 as a result of *United States v. Rigmaiden*,[63] the first case to question use of the device. In *Rigmaiden*, the defendant participated in a scheme to obtain fraudulent tax refunds.[64] Rigmaiden used an aircard under a false identity to perpetrate his fraudulent activity.[65] Law enforcement used a StingRay device to locate the aircard and, subsequently, Rigmaiden's

56. *See* Gallagher, *supra* note 54 (listing technology produced by Harris). I used TriggerFish in the title of this Comment solely for pun purposes; all the StingRay puns were taken. *See, e.g.*, Jason Norman, Note, *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*, 68 FED. COMM. L.J. 139 (2016).

57. *Id.*

58. *See id.* (noting that trademark records show that registration for the TriggerFish was filed in July 2001, but the trademark was cancelled in 2008 and Harris Corporation does not market the product).

59. Pell & Soghoian, *supra* note 50, at 14.

60. *Id.*

61. *See* Roberts, *supra* note 53; Gallagher, *supra* note 54.

62. STINGRAY, Registration No. 2,762,468.

63. 844 F. Supp. 2d 982 (D. Ariz. 2012).

64. *Id.* at 987.

65. *Id.*

location in an apartment.[66] This case attracted the public's and the media's attention because the government went to great lengths to conceal that they had used a StingRay and would not reveal how the technology worked.[67] This case led to the discovery that Harris Corporation and government agencies deliberately concealed the use of StingRay devices.[68] The level of secrecy surrounding government use of IMSI-catchers has understandibly increased judicial, legislative, and public scrutiny. As a result, pressure from privacy advocates, filing of Freedom of Information Act requests,[69] and action by influential Senate and House members[70] has caused the government to reveal details about StingRay use and specifications.

B. The Secrecy Behind the Use of IMSI-Catchers.

Both the Harris Corporation and the FBI have shielded the technology behind StingRay devices. Harris does not disclose details about StingRay devices on its website, and includes a warning with its marketing materials that they should only be distributed to the law

66. *See* Order at 4–5, United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (No. CR 08-814-PHX-DGC), 2013 WL 1932800, at *3. "Using the cell-tower information, a map, and various calculations, a government agent was able to narrow" the general location of a Rigmaiden's aircard. The government then obtained an order and a "warrant authorizing the use of a mobile tracking device to communicate with the aircard," which tracked the aircard to an apartment. *Id.*

67. Linda Lye, *In Court: Uncovering Stingrays, A Troubling New Location Tracking Device*, ACLU (Oct. 22, 2012, 12:45 PM), https://www.aclu.org/blog/court-uncovering-stingrays-troubling-new-location-tracking-device [https://perma.cc/WR5L-QXAH] ("[T]he government hid from the judge the facts that stingrays collect information about third parties, that they can pinpoint targets even within their homes, and that some models capture content, not just location.").

68. *Id.* ("[T]he papers the government submitted to get the so-called 'warrant' never told the judge that the government wanted to use a stingray (or IMSI catcher, or cell site emulator), what the device is, or how it works.").

69. *See, e.g.*, Nathan Freed Wessler, *ICE Using Powerful Stingray Surveillance Devices in Deportation Searches*, ACLU (May 23, 2017, 10:15 AM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/ice-using-powerful-stingray-surveillance-devices [https://perma.cc/3AY7-ML9E].

70. *See Stingrays: A New Frontier in Police Surveillance Panel 1*, CATO INSTITUTE (Feb. 15, 2017), https://www.cato.org/multimedia/events/stingrays-new-frontier-police-surveillance-panel-1 [https://perma.cc/7RJ4-JFCM] (discussing efforts by the House Committee on Oversight and Government Reform to introduce legislation limiting government use of cell phone surveillance technology).

enforcement and communications service providers authorized under 18 U.S.C. § 2512.[71]

The FBI and Harris Corporation are bound by a non-disclosure agreement that restricts discussion regarding StingRay technology.[72] Local law enforcement is bound by the same non-disclosure agreement if they wish to acquire a StingRay device. The FCC requires local law enforcement to coordinate with the FBI before acquiring a StingRay.[73] The FBI then requires the local agency to sign a non-disclosure agreement before acquiring a StingRay.[74] The FBI revealed an example of the non-disclosure agreement in a letter to the Baltimore Police Department.[75] The agreement restricts the Baltimore Police Department and the Office of the State's Attorney for Baltimore City from discussing the device or its capabilities in any court proceeding.[76] It also requires that the police notify the FBI immediately upon any court order requesting sensitive information pertaining to StingRay devices.[77]

These non-disclosure agreements have caused police departments to not only keep quiet about the capabilities of StingRays, but also to not disclose the use of the device at all.[78] This agreement forced the

71. Only law enforcement and communication service providers may lawfully manufacture, assemble, possess, distribute, and advertise wire, oral, or electronic communication intercepting devices. 18 U.S.C. § 2512 (2012); HARRIS ASSURED COMMC'NS, HARDWARE MANUAL 3 (2010), https://cryptome.org/2015/03/fcc-stingray-final.pdf [https://perma.cc/VH9K-4PU7].

72. *See, e.g.*, Letter from Ernest Reith, Acting Assistant Dir., FBI, to Frederick H. Bealefeld, III, Police Comm'r, Balt. Police Dep't & Gregg L. Bernstein, Esq., State's Attorney, Office of the State's Attorney for Balt. City (July 13, 2011), http://s3.documentcloud.org/documents/1808819/baltimore-police-stingray-non-disclosure-agreement.pdf [https://perma.cc/H7VW-7SGA] (specifying the non-disclosure requirements between the Baltimore Police Department, Office of the Baltimore State's Attorney, and the FBI regarding Harris Corporation tracking devices).

73. Tim Cushing, *FCC Denies It Requires Law Enforcement to Sign a Non-Disclosure Agreement with the FBI Before Deploying Stingray Devices*, TECHDIRT (Oct. 10, 2014, 1:33 PM), https://www.techdirt.com/articles/20141008/13471728772/fcc-denies-it-requireslaw-enforcement-to-sign-non-disclosure-agreement-with-fbi-before-deploying-stingraydevices.Shtml [https://perma.cc/64UN-C32J].

74. *See id.* (assuming that FBI requires local law enforcement to sign a non-disclosure agreement based on an FBI agent's comments).

75. *See* Letter from Ernest Reith to Frederick H. Bealefeld, III, and Gregg L. Bernstein, *supra* note 72.

76. *Id.*

77. *Id.*

78. *See, e.g.*, Kim Zetter, *Florida Cops' Secret Weapon: Warrantless Cell Phone Tracking*, WIRED (Mar. 3, 2014, 9:00 AM), http://www.wired.com/2014/

government's lack of transparency in the *Rigmaiden* case.[79] Fear of disclosure has also caused local and federal law enforcement to dismiss charges in lieu of revealing sensitive information that may violate the agreement.[80]

The federal government currently owns hundreds of StingRay devices and has spent over 100 million dollars on the devices.[81] The Department of Homeland Security has given $1.8 million in grants to local law enforcement agencies to purchase StingRay devices.[82] However, it is unknown exactly how many local law enforcement agencies own StingRay devices. According to the American Civil Liberties Union, "72 agencies in 24 states and the District of Columbia" own StingRay devices.[83] But this number dramatically underrepresents actual use among state and local law enforcement.[84]

C. Technology of IMSI-catchers.

IMSI-catchers contain "an antenna, a computer with mapping software, and a special device."[85] The device is about the size of a briefcase and can be set up virtually anywhere.[86] Although the range is unclear, the Department of Justice claims their IMSI-catchers are typically deployed within 1,000 feet of the subject phone.[87] Since cell

03/stingray/ [https://perma.cc/Z3PP-TH5L] (reporting on a Florida police department that did not disclose use of a StingRay to the court over two hundred times).

79. *See supra* Section II.A.

80. *See* Jason M. Weinstein et al., *Privacy vs. Public Safety: Prosecuting and Defending Criminal Cases in the Post-Snowden Era*, 52 AM. CRIM. L. REV. 729, 742 (2015) ("Local prosecutors have gone so far as to make favorable plea deals or even to dismiss cases altogether in order to avoid disclosing information about the use of this technique.").

81. *Stingrays: A New Frontier in Police Surveillance Panel 1*, *supra* note 70, at 7:00.

82. *Id.* at 17:45.

83. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them [https://perma.cc/5CP3-HZDP] (last visited Sept. 19, 2017).

84. *Id.*

85. Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, WALL ST. J. (Sept. 21, 2011, 10:33 PM), http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/ [https://perma.cc/23N3-R2KR].

86. *See, e.g.*, Gallagher, *supra* note 54.

87. *Examining Law Enforcement Use of Cell Phone Tracking Devices: Hearing Before the Subcomm. on the Info. Tech. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 12 (2015) (statement of Seth Stodder, Assistant

phones give preference to the cell site with the strongest signal, an IMSI-catcher only needs to emit the strongest signal in an area near the target cell phone to successfully register with the phone.[88] If law enforcement knows the unique hardware numbers attached to the phone, such as the IMSI number, they can travel with the IMSI-catcher until it registers with the correct cell phone.[89] Law enforcement also uses the device to find out which cell phones are located within a specific area.[90] In this case, law enforcement points the antenna in the target direction and will receive identifying information from all of the cell phones in the area that successfully register with the device.[91]

IMSI-catchers are also capable of identifying more precise locations of target cell phones once an initial connection is made.[92] Law enforcement can move to different locations around the target area, and the IMSI-catcher can measure the signal strength from each location to triangulate the location of the target cell phone more precisely.[93] This process is essentially the same as triangulation done by prospective CSLI collection directly from cell service providers, except that the device is portable and measures one data point at a time, rather than three or more at once.

There are two distinct aspects of StingRay capabilities that seem to garner the most misunderstanding. First, StingRay devices are *capable* of capturing the content of communications. However, it is important to realize that the StingRay devices used by law enforcement in the United States must be configured as pen registers—which do not capture the content of communications—because law enforcement acquires its authority to use the devices from the Pen/Trap statute.[94] Therefore, the StingRays are configured to not capture the content of any communication. In addition, StingRay devices are not capable of capturing subscriber information from the target cell phone regardless of the limitations of the Pen/Trap Statute.[95] Second, StingRay devices by their nature, attract all cell phones nearby to

Secretary, U.S. Department of Homeland Security) [hereinafter *Tracking Devices House Hearing 2015*].

88. Ubaid, *supra* note 22.

89. *See* Valentino-DeVries, *supra* note 85.

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.*

94. *See infra* Sections III.B–C.

95. *Tracking Devices House Hearing 2015*, *supra* note 87, at 12.

connect to them—not just the target cell phone. This creates the concern that StingRay devices collect information from innocent third-party bystanders. The Department of Justice has addressed this issue as well. In 2002, the Department of Justice issued a policy document titled "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."[96] Furthermore, in 2015, the Department of Justice specifically addressed overcollection concerns in its policy statement regarding use of StingRay devices.[97] The policy requires agencies to implement an auditing system to manage and dispose of data from third parties.[98]

III. THE LEGAL STANDARD NEEDED TO OBTAIN CSLI.

The government has derived statutory authority to obtain CSLI from the Pen/Trap Statute[99] and the Stored Communications Act ("SCA"),[100] both within the Electronic Communications Privacy Act of 1986 ("ECPA").[101] The ECPA has been frequently updated and amended to keep up with advancing technology,[102] and the Pen/Trap Statute is a prime example of that.

A. Statutory Authority for Historical CSLI.

Prosecutors have derived statutory authority to obtain historical CSLI from the SCA.[103] The SCA allows a governmental entity to "require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service."[104] The SCA grants the

96. Memorandum from Larry D. Thompson, U.S. Dep't of Justice, Office of the Deputy Att'y Gen., Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices (May 24, 2002), http://www.justice.gov/sites/default/files/dag/legacy/2007/10/09/memo-05242002.pdf [https://perma.cc/U5KY-KNWE].

97. U.S. DEP'T OF JUSTICE, DEPARTMENT OF JUSTICE POLICY GUIDANCE: USE OF CELL-SITE SIMULATOR TECHNOLOGY (Sept. 3, 2015), http://www.justice.gov/opa/file/767321/download [https://perma.cc/WN2R-E3RX] [hereinafter DOJ 2015 POLICY]; *see infra* Section III.C.

98. DOJ 2015 POLICY, *supra* note 97, at 6.

99. 18 U.S.C. § 3121–27 (2012).

100. *Id.* §§ 2701–12.

101. Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2510–22 (2012)).

102. McLaughlin, *supra* note 23, at 428.

103. 18 U.S.C. §§ 2703–12; *ECPA Judiciary Hearing 2010*, *supra* note 15, at 70 (written statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

104. § 2703(c).

government authority to obtain all records from a cell service provider other than those that contain contents of communications, which the SCA defines as "any information concerning the substance, purport, or meaning of [a] communication."[105] Location data is not categorized as the content of a communication, "rather it is ancillary data conveyed so that the wireless telephone can connect with the nearest cell tower."[106] Records requests pursuant to the SCA require proof of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[107]

Records requests under 18 U.S.C. § 2703(d) are a common occurrence.[108] The amount of record requests made under the SCA has increased dramatically in recent years.[109] Chief Judge Beryl A. Howell of the U.S. District Court for the Disctict of Colombia recently released summary data that revealed how often requests under 18 U.S.C. § 2703(d) have been made in criminal cases handled by the Justice Department or the U.S. Attorney's Office for the District of Columbia since 2008. The records showed that the requests have increased sevenfold since 2014 in the District of Colombia alone.[110]

B. Statutory Authority for Prospective CSLI

The statutory standard utilized to request prospective CSLI from cell service providers and to receive court authorization to utilize a StingRay device is much more controversial and complicated than requests for historical CSLI. The language of the SCA alone is not sufficient to enable the government to retrieve data in real time. In

105. *Id.* § 2510(8).

106. *ECPA Judiciary Hearing 2010*, *supra* note 15, at 70 (written statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

107. 18 U.S.C. § 2703(d).

108. *See, e.g.*, *Verizon's Transparency Report for the First Half of 2015*, VERIZON, https://www.verizon.com/about/portal/transparency-report/wp-content/uploads/2016/01/Verizon-Transparency-Report-2015-first-half.pdf [https://perma.cc/4CCS-LLMC] (stating that Verizon Wireless received 149,810 requests for customer data in the first half of 2015).

109. Spencer S. Hsu, *Court: Warrantless Requests to Track Cellphones, Internet Use Grew Sevenfold in D.C. in Three Years*, WASH. POST (July 18, 2017), https://www.washingtonpost.com/local/public-safety/court-warrantless-requests-to-track-cellphones-internet-use-grew-sevenfold-in-dc-in-three-years/2017/07/18/b284ac32-6b36-11e7-9c15-177740635e83_story.html?utm_term=.15cb8cb8959a [https://perma.cc/86Y7-6PJS].

110. *Id.* (noting that this number includes requests for an individuals' Internet connection records in addition to cell phone tower records).

2005, the Department of Justice created a type of "hybrid order" to establish legal authority to retreive prospective CSLI.[111] The order advised that the government should request prospective CSLI under both the Pen/Trap statute[112] and the section 2703(d) of the SCA.[113]

Congress enacted the Pen/Trap statute in response to the Supreme Court's holding in *Smith v. Maryland*[114] to establish procedural requirements for law enforcement's use of pen registers or trap and trace devices. The statute authorized law enforcement to install the devices with a court order. Fifteen years later, the USA PATRIOT Act[115] amended the definition of a pen register to include any device that collects "dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,"[116] and amended the definition of "trap and trace device" to include any device that collects "dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication."[117] Under the Pen/Trap statute, the applicants must only identity themselves and their agency[118] and certify that "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[119] If this relatively low burden is met, then the court is required to authorize the installation of the pen/trap device.[120] On its face, the Pen/Trap statute would seem to permit law enforcement to retrieve prospective CSLI from cell service providers.[121] However, the Communications Assistance for Law Enforcement Act ("CALEA"),[122] passed in 1994, includes a provision that limits the type of information that law enforcement can obtain pursuant to the Pen/Trap statute. It states that, "with regard to

111. Pell & Soghoian, *supra* note 42, at 135–136.

112. 18 U.S.C. § 3122 (2012).

113. *Id.* § 2703(d).

114. 442 U.S. 735 (1979).

115. Pub. L. No. 107–56, 115 Stat. 272 (2001) (codified as amended at 18 U.S.C. § 3127(3) (2012)).

116. 18 U.S.C. § 3127(3) (2012).

117. *Id.* § 3127(4).

118. *Id.* § 3122(b)(1).

119. *Id.* § 3122(b)(2).

120. *Id.* § 3123(a).

121. *ECPA Judiciary Hearing 2010*, *supra* note 15, at 71 (written statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

122. Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001–1010 (2012)).

information acquired solely pursuant to the authority of the pen registers and trap and trace devices . . . such call-identifying information shall not include any information that may disclose the physical location of the subscriber."[123] With this limitation, law enforcement would not have authority to request prospective CSLI because it may disclose the physical location.

The government has relied on the fact that CALEA states information that may disclose the physical location of the subscriber cannot be acquired *solely* by use of a Pen/Trap Statute.[124] This language suggests that another statute could be utilized to grant authority to the government to gather CSLI information. By combining the Pen/Trap Statute and § 2703 of the SCA, the Department of Justice effectively benefits from the language of the Pen/Trap Statute that states that the court *shall*[125] issue an ex parte order rather than the language in the SCA that states a court *may* issue an order.[126] At the same time, the Department of Justice overcomes the "solely" language in the statute by relying on section 2703(d) of the SCA that permits law enforcement to use a court order to obtain all non-content subscriber information.[127] The combination of the statutes also helps overcome arguments that suggest that cell phones are "tracking devices" under 18 U.S.C. § 3117(b) and therefore, not an "electronic communication" under the Pen/Trap statute, because the SCA does not exclude tracking devices from the types of information that may be provided, nor does it exclude location information.

C. IMSI-Catchers and the Law.

Law enforcement derives statutory authority to operate IMSI-catchers by utilizing the same "hybrid order" used for obtaining prospective CSLI. Although, the Department of Justice noted in 2005 that the prohibition in CALEA limiting the ability to disclose location information only applies to cell service providers because, "[b]y its very terms, this prohibition applies only to information collected by a pro-vider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate

123. 47 U.S.C. § 1002(a)(2).

124. *Id.*

125. 18 U.S.C. § 3123(a).

126. *Id.* § 2703(d).

127. Under this theory, the government must still meet the higher judicial showing under 18 U.S.C. § 2703(d). *ECPA Judiciary Hearing 2010, supra* note 15, at 72 (statement of Marc J. Zwillinger, Zwillinger Genetski, LLP).

targeted cell phones."[128] Therefore, the federal government's position was that the Pen/Trap Statute was the "safest method of allowing law enforcement to collect [CSLI] directly using its own devices."[129]

In 2015, the Department of Justice changed its policy for utilizing StingRay devices.[130] The change was due to challenges by media and nonprofit organizations,[131] as well as influence from legislative bodies.[132] The new policy requires a warrant pursuant to Rule 41 of the Federal Rules of Criminal Procedure—or the relevant state equilvalent—in addition to authorization from the Pen/Trap Statute to obtain authorization to utilize a cell-site simulator.[133] The policy also requires agencies to comply with certain training, auditing, and management controls.[134] The Department of Justice emphasized again that because cell-site simulators used by the Department must be configured like pen registers to obtain authorization from the statute, the devices do not collect the contents of any communication.[135] However, the policy only applies to federal agencies, leaving state and local law enforcement with discretion to enact their own policies.

At least nine states have enacted laws that regulate the use of cell-site simulators,[136] and at least five have required a warrant to use a cell-site simulator, including California,[137] Minnesota,[138] Utah,[139] Virginia,[140] and Washington.[141] Although the federal government no

128. DOJ 2005 MANUAL, *supra* note 14, at 48.

129. *Id.*

130. *See* DOJ 2015 POLICY, *supra* note 97.

131. Shawn Marie Boyne, *Stingray Technology, the Exclusionary Rule, and the Future of Privacy: A Cautionary Tale*, 119 W. VA. L. REV. 915, 928–29 (2017).

132. *See Stingrays: A New Frontier in Police Surveillance Panel 1*, *supra* note 70.

133. DOJ 2015 POLICY, *supra* note 97, at 3.

134. *Id.* at 2–3.

135. *Id.* at 2.

136. COLO. REV. STAT. § 16-3-303.5(2) (2017); 725 ILL. COMP. STAT. 168/10 (Supp. 2017); IND. CODE § 35-33-5-12(a) (2014); ME. STAT. tit. 16, § 648 (2017); MD. CODE ANN., CRIM. PROC. § 1-203.1(b)(1) (LexisNexis 2016); MINN. STAT. §§ 626A.28(3)(d), 626A.42(2)(a) (2017); MONT. CODE ANN. § 46-5-110(1)(a) (2017); TENN. CODE ANN. § 39-13-610(b) (2017); WIS. STAT. § 968.373(2) (2017).

137. CAL. PENAL CODE § 1546.1(b)(1) (2017).

138. MINN. STAT. § 626A.28 (2017).

139. UTAH CODE ANN. § 77-23c-102(1)(a) (LexisNexis 2017).

140. VA. CODE ANN. § 19.2-70.3 (2017).

141. WASH. REV. CODE §§ 9.73.260, 9.73.270 (2017).

longer utilizes hybrid orders or the Pen/Trap statute alone to obtain prospective CSLI, these statutes are still often utilized by the states to obtain CSLI and to authorize the use of StingRay devices.

IV. The Fourth Amendment

A. Evolution of the Fourth Amendment and Technology

The Fourth Amendment provides:

> [T]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[142]

To trigger protection under the Fourth Amendment, and thus require a warrant for a search, the search must be considered unreasonable.[143] Historically, for an action to constitute a search within the meaning of the Fourth Amendment, law enforcement must have physically trespassed.[144] In *Olmstead*, the Supreme Court held that a wiretap did not constitute a search under the Fourth Amendment because law enforcement secured the evidence by hearing only, without physical intrusion in to the defendant's house or office.[145] Nearly thirty years later, the Supreme Court deviated from the *Olmstead* trespass theory in a similar case.[146] *Katz* involved placement of a listening device on a telephone booth that enabled law enforcement to hear calls the defendant made from inside the booth.[147] The Supreme Court found that "[t]he Fourth Amendment protects people, not places," and that what someone "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[148] *Katz* became the seminal case to determine what constitutes a reasonable expectation of privacy in the context of Fourth Amendment

142. U.S. Const. amend. IV.

143. Carroll v. United States, 267 U.S. 132, 147 (1925).

144. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928).

145. *Id.* at 464.

146. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (explaining "that the underpinnings of Olmstead . . . have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling").

147. *Id.* at 348.

148. *Id.* at 351–52.

analysis. It established a two-prong test requiring: (1) that a person has an actual subjective expectation of privacy and (2) that the expectation is one that society is prepared to recognize as reasonable.[149]

The third-party doctrine effectively eliminates an individual's reasonable expectation of privacy—and thus, Fourth Amendment protection—in information voluntarily disclosed to a third party. The doctrine was first applied in cases involving government agents and undercover informants. In *Hoffa v. United States*,[150] the Supreme Court held that law enforcement's use of a government informant did not violate the Fourth Amendment when the defendant voluntarily invited the informant into his hotel room, even though the defendant did not know he was a government informant.[151] The Court based its reasoning on the fact that Hoffa voluntarily assumed the risk that the third party might disclose the information he shared with the government.[152] The Court also held, in *Lopez v. United States*,[153] that recorded statements made to an Internal Revenue Service Agent were not a search under the Fourth Amendment.[154]

The Supreme Court later extended the third-party doctrine to include business records in *United States v. Miller*.[155] In *Miller*, the government subpoenaed Miller's banking records from his banking institution.[156] The Supreme Court held that Miller did not have an expectation of privacy in his bank records.[157] The Court reasoned that he could not claim ownership or possession of the records because they belong to the bank,[158] and the documents "contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[159] Three years later, in *Smith v. Maryland*,[160] the Supreme Court applied the third-party doctrine to a pen register.[161] The Court determined that the installation

149. *Id.* at 361 (Harlan, J., concurring).

150. 385 U.S. 293 (1966).

151. *Id.* at 302–03.

152. *Id.* (quoting Lopez v. United States, 373 U.S. 427, 465 (1963)).

153. 373 U.S. 427 (1963).

154. *Id.* at 439–40.

155. 425 U.S. 435 (1976).

156. *Id.* at 437–38.

157. *Id.* at 442.

158. *Id.* at 440.

159. *Id.* at 442.

160. 442 U.S. 735 (1979).

161. *Id.* at 736.

of a pen register by a telephone company at the request of law enforcement was not a search because telephone users voluntarily convey the phone numbers they dial to phone companies.[162] The Court emphasized that it was of no consequence that "most people may be oblivious to a pen register's esoteric functions" because telephone users typically know that the information must be conveyed to telephone companies to facilitate the call and the company records the information for a variety of legitimate business purposes.[163] The holding in *Smith* also distinguished content and non-content information, noting that a pen register only collects information collected as a means of establishing communication, not the actual communication between the caller and the recipient of the call.[164]

The Supreme Court first addressed surveillance in the context of the Fourth Amendment in companion cases, *United States v. Knotts*[165] and *United States v. Karo*[166]—two cases involving the use of an electronic beeper to track an individual's movements. In *Knotts*, law enforcement placed a beeper inside a container of chloroform and tracked Knotts's movements as he transported the jar.[167] The Court held that Knotts did not have a reasonable expectation of privacy in his movements out in public in plain view.[168] Although the beeper enhanced law enforcement's surveillance capabilities, normal visual surveillance could have achieved the same result.[169] The Court in *Karo*, however, did not reach the same conclusion. In *Karo*, police also installed a beeper in a can of ether and tracked Karo's movements as he transported the can into his home and to two other homes.[170] The Court held that the tracking of the beeper was an unreasonable search because the government obtained "information that it could not have obtained from outside the curtilage of the house."[171]

In *Kyllo v. United States*,[172] the Court again addressed individuals' expectation of privacy within the home as it pertains to sense-

162. *Id.* at 742.

163. *Id.* at 742–43.

164. *Id.* at 741.

165. 460 U.S. 276 (1983).

166. 468 U.S. 705 (1984).

167. *Knotts*, 460 U.S. at 278.

168. *Id.* at 281.

169. *Id.* at 285 (Brennan, J., concurring).

170. *Karo*, 468 U.S. at 708.

171. *Id.* at 706.

172. 533 U.S. 27 (2001).

enhancing technology.[173] Law enforcement used a thermal imaging device from a street corner to detect high levels of heat emanating from the home.[174] The police relied on this information in order to obtain a search warrant and subsequently found marijuana in the home.[175] The Court held that use of a device not in general public use was an unreasonable search because it revealed information about the interior of the home that could not otherwise have been obtained without physical intrusion into the home.[176]

Most recently, in *United States v. Jones*,[177] the Court addressed the use of a GPS tracking device.[178] In *Jones*, police placed a GPS device on the defendant's car to track his movements for twenty-eight days.[179] The Court unanimously held that the use of the GPS device was a search under the Fourth Amendment, but decided it on different grounds than previous tracking cases. The majority relied on the trespass theory set out in *Olmstead*, focusing on the physical intrusion on Jones's car to find the search unreasonable.[180] Justice Scalia, writing for the majority, declined to apply the *Katz* test because "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation."[181] He reminded the Court that the *Katz* test did not narrow the scope of the Fourth Amendment.[182] In other words, placement of the beeper on Jones's car was enough to constitute an unreasonable search under the trespass theory without any need to address reasonable expectation of privacy in Jones's movements. Justice Scalia recognized that if Jones had been tracked by electronic means, without an incidental trespass, that the outcome of the decision may have been different, but declined to address that issue.[183]

Justices Sotomayor and Alito, however, did apply the *Katz* analysis in their concurrences. Justice Sotomayor urged the Court to consider potential technological advances in surveillance technologies.[184] Justice Sotomayor argued that the unique attributes of

173. *Id.* at 34–37.

174. *Id.* at 29–30.

175. *Id.* at 30.

176. *Id.* at 34.

177. 565 U.S. 400 (2012).

178. *Id.* at 402.

179. *Id.* at 403.

180. *Id.* at 404–06.

181. *Id.* at 406.

182. *Id.* at 406–07.

183. *Id.* at 412.

184. *Id.* at 416 (Sotomayor, J., concurring).

surveillance technology, such as GPS monitoring, should be taken into account when analyzing reasonable expectation of privacy, stating, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[185] Justice Sotomayor added that application of the third-party doctrine is ill suited to the digital age.[186] Justice Alito rejected the use of the trespass test altogether and argued that individuals have a reasonable expectation of privacy in long-term monitoring.[187]

B. How Courts Have Applied the Fourth Amendment to CSLI.

The Sixth Circuit held, in *United States v. Carpenter*,[188] that cell phone users did not have a reasonable expectation of privacy in their cell phone records conveyed to cell service providers.[189] The court analogized Carpenter's situation to the Supreme Court's finding in *Smith* to confirm the conclusion.[190] The Fourth,[191] Fifth,[192] and Eleventh[193] Circuits have come to similar conclusions.

185. *Id.*

186. *Id.* at 417.

187. *Id.* at 424–25 (Alito, J., concurring).

188. 819 F.3d 880 (6th Cir. 2016).

189. *Id.* at 883–84 (finding that the government's collection of phone records showing defendants' geographical locations did not constitute a warrantless search violating the Fourth Amendment).

190. *Id.* at 887–88 (holding that, just as Smith did not have an expectation of privacy in the *phone numbers* collected by the government, Carpenter similarly did not have an expectation of privacy in the *location* data collected by the government through phone records).

191. United States v. Graham, 824 F.3d 421, 424, 427 (4th Cir. 2016) (en banc) (holding that, under the third-party doctrine, the government did not violate the Fourth Amendment because the defendant did not have a reasonable expectation of privacy in the historical CSLI collected by the defendant's cell phone provider).

192. *In re* Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (finding that orders to obtain cell-site information for a specific phone placing and terminating calls are not "categorically unconstitutional," as the Fourth Amendments protects only reasonable expectations of privacy).

193. United States v. Davis, 785 F.3d 498, 518 (11th Cir. 2015) (finding that the defendant had a diminished expectation of privacy in records created and kept by his cellular phone company, and the disclosure of the records did not constitute an unconstitutional invasion of privacy).

In *United States v. Graham*,[194] the Fourth Circuit specifically addressed Justice Alito's concerns of twenty-four hour "dragnet" surveillance that he expressed in his concurring opinion in *Jones*.[195] In *Graham*, law enforcement acquired CSLI that spanned over 200 days.[196] The District Court held that the defendant did not have a reasonable expectation of privacy in his cell-site records, relying on the third-party doctrine established in *Smith*, and that the amount of CSLI obtained from law enforcement did not change this expectation of privacy.[197] The decision was later affirmed—but criticized—by the Fourth Circuit in 2015, when the court held that the defendant did have an expectation of privacy in his CSLI, but admitted the evidence because law enforcement relied in good faith on court orders issued in accordance with the SCA.[198] In 2016, the Fourth Circuit reheard its 2015 decision in *Graham* and reverted back to the district court's original holding—that cell phone users do not enjoy a reasonable expectation of privacy in historical CSLI.[199] This decision eliminated the "circuit split" among courts, and seemingly closed the door to possible Supreme Court review.[200]

Although the issue of whether the third-party doctrine squarely applies to historical CSLI obtained from a cell service provider appears to have been resolved, the issue of voluntariness is often challenged.[201] It seems critics find that since the signals cellular phones

194. 796 F.3d 332 (4th Cir. 2015), *aff'd on reh'g en banc on other grounds*, 824 F.3d 421 (4th Cir. 2016).

195. *Id.* at 347.

196. United States v. Graham, 846 F. Supp. 2d 384, 387 (D. Md. 2012), *aff'd on other grounds*, 796 F.3d 332 (4th Cir. 2015), *aff'd on reh'g en banc*, 824 F.3d 421 (4th Cir. 2016).

197. *Id.* at 387–90.

198. *Graham*, 796 F.3d at 338.

199. *Graham*, 824 F.3d at 427. *See also* Robinson Meyer, *No One Will Save You From Cellphone Tracking Unless the Supreme Court Acts*, ATLANTIC (June 2, 2016), https://www.theatlantic.com/technology/archive/2016/06/fourth-circuit-csli-cellphone-location-tracking-legal/485225/ [https://perma.cc/D9R2-VPBS] (discussing the Fourth Circuit's en banc reversal of its previous decision as a result of the "third-party doctrine," limiting a defendant's reasonable expectation of privacy).

200. *Meyer*, *supra* note 199. However, on June 5, 2017, the Supreme Court granted certiori to review the descision in *Carpenter*. United States v. Carpenter, 819 F.3d 880, 883–84 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (June 5, 2017) (No. 16-402).

201. *See, e.g.*, Brief for the Center for Democracy & Technology as Amicus Curiae Supporting Petitioner at 20–22, Carpenter v. United States, 137 S. Ct. 2211 (No. 16-402) (arguing that the voluntariness requirement should not be considered in expectation of privacy analysis); Brief for United States Justice

emit are automatic and continuous, the user cannot voluntary share CSLI information in any meaningful way. Only one circuit court has addressed whether cell phone users have a reasonable expectation of privacy in CSLI captured prospectively by cell service providers at law enforcement's request. In *United States v. Skinner*,[202] the Sixth Circuit, applying *Knotts*, held that Skinner did not have a reasonable expectation of privacy in his CSLI while traveling along public roadways.[203] However, the court did not address whether Skinner would maintain this expectation of privacy if he had traveled within the constitutionally protected area of his home.

In 2012*, United States v. Rigmaiden*[204] was the first case in a federal court to address the issue of StingRay use. In an order denying the defendant's motion to suppress, the court held that Rigmaiden did not have a reasonable expectation of privacy in his CSLI. The court relied on the fact that Rigmaiden fraudulently obtained both the aircard that law enforcement tracked and the apartment where he was located.[205] Therefore, akin to the reasoning in *Rakas v. Illinois*,[206] he did not have a reasonable expectation of privacy in his wrongful presence within the apartment.

The U.S. District Court for the Southern Disrtict of New York, in *United States v. Lambis,*[207] was the first federal court to uphold suppression of evidence obtained from a StingRay. In *Lambis*, the Drug Enforcement Administration utilized a StingRay to locate Lambis in his home.[208] Analogizing to *Kyllo*, the court held that use of a StingRay device to locate Lambis in his home was an unreasonable search because "the 'pings' from [his] cellphone to the nearest cell site were not readily available 'to anyone who wanted to look' . . . ."[209]

Foundation, et al. as Amicus Curiae Supporting Petitioner at 33–34, Carpenter v. United States, 137 S. Ct. 2211 (No. 16-402) (arguing that CSLI is not voluntarily conveyed to cell service providers, but is mandated by government).

202. 690 F.3d 772 (6th Cir. 2012).

203. *Id.* at 781, 777–78.

204. 844 F. Supp. 2d 982 (D. Ariz. 2012).

205. United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at *6 (D. Ariz. May 8, 2013).

206. 439 U.S. 128 (1978).

207. 197 F. Supp. 3d 606 (S.D.N.Y. 2016).

208. *Id.* at 609.

209. *Id.* at 609–10 (quoting United States v. Knotts, 460 U.S. 276, 281 (1983)).

V. IMSI-Catchers and the Fourth Amendment.

A. The Third-Party Doctrine

Although collection of historical and prospective CSLI fits more squarely within the third-party doctrine when obtained through a cell service provider, a law enforcement officer's use of an IMSI-catcher does not. Even though a cell phone may simultaneously convey the same location information to a StingRay device and a cell site operated by the carrier, StingRay devices obtain the information directly from the cellular phone. A StingRay never retrieves the cell-site information from the cellular service provider, therefore it effectively circumvents the third party. However, the third-party doctrine is not necessary to find a lack of a reasonable expectation of privacy in CSLI.

B. Surveillance in Constitutionally Protected Areas.

As recognized in *Karo*, law enforcement's surveillance of individuals within a home presents higher privacy concerns.[210] The Court reasoned that "[i]f a DEA agent had entered the house in question without a warrant to verify that the ether was in the house, he would have engaged in an unreasonable search . . . ."[211] However, the same could have been said for the situation in *Knotts,* in which law enforcement tracked the location of the chloroform to the inside of the defendant's home.[212] The Court noted that there was no evidence that "the beeper was used after the location in the area of the cabin had been initially determined."[213] The reasoning that apparently distinguishes *Knotts* from *Karo* is that "[e]ven if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises."[214] But the Court did not recognize that law enforcement could have discovered the ether inside the home through regular visual surveillance as well. If a DEA agent had physically followed Karo as he traveled with the can of ether, he would have also observed—without any need to enter the premises—Karo entering the home with the ether, and he also would have subsequently observed Karo leaving with the ether and traveling to other private homes. With regular

210. United States v. Karo, 468 U.S. 705, 714–15 (1984).

211. *Id.* at 706.

212. *Knotts*, 460 U.S. at 278–79.

213. *Id.*

214. *Karo*, 468 U.S. at 715.

surveillance from outside of the home, law enforcement could confirm that the ether remained in the home by the simple fact that it had not been taken out yet.

It could also be argued that continuous tracking of an object within a home reveals movements throughout the home that could not be discovered through regular visual surveillance. However, a StingRay, *at its best,* can decipher the location of a cell phone within a couple meters.[215] Law enforcement cannot tell the difference if your phone is in your bathroom or ten feet away in your bedroom, because the technology is simply not capable of such precise tracking.

Regardless of the adverse holdings in *Karo* and *Knotts*, there is one important distinction between use of a government-installed beeper and the government's use of a StingRay device. In *Karo*, law enforcement placed the GPS tracker inside of a can without Karo's knowledge, but StingRay devices capture information that the user of a cell phone knows is broadcasted outside of the home. As stated in the seminal case establishing the test for a reasonable expectation of privacy, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[216] Cell phone users are aware that their cell phones automatically search for cell towers when powered on, and entrance into the home does not change this expectation. It is of no consequence whether the cell phone user is aware that the government is capturing the information that the cell phone is sending rather than the cell service provider, because as the Court held in *Hoffa*, the Fourth Amendment does not apply to information disclosed to an undercover government actor. StingRays are essentially undercover cell towers, and it does not make a difference whether a cell phone user knows that the particular cell tower it has connected to is owned by a government actor.

215. *The "Stingray", Government's New Tracking and Surveillance Tool*, EXPERIENCED CRIM. LAW. (Oct. 29, 2012), http://www.experiencedcriminallawyers.com/stingray-government-tracking-and-surveillance-tool/ [https://perma.cc/2EJX-8EBM].

216. Katz v. United States, 389 U.S. 347, 351 (1967). *See also* Lewis v. United States, 385 U.S. 206, 210 (1966) (discussing the lack of a Fourth Amendment violation when the petitioner invited an undercover agent into his home for the purpose of selling the agent narcotics); United States v. Lee, 274 U.S. 559, 563 (1927) (finding that the use of a searchlight that revealed cases of illegal liquor on a ship's deck prior to the boarding of the ship by Coast Guard officials did not violate the Fourth Amendment).

Of course, one could counter this argument by quoting Scalia's opinion in *Kyllo*, in which he conditioned the fact that the use of thermal-imaging technology was a search because it was not "in general public use."[217] But, as explained by Orin Kerr, "no case has taken *Kyllo* beyond the facts of the case itself, and no court has viewed *Kyllo* as a symbolic endorsement of broad privacy rights in new technologies."[218] This result is largely due to the difficulty in deciphering what exactly defines general public use. The thermal-imaging device used in *Kyllo*—decided only sixteen years before this Comment was written—is arguably in general public use today given the fact that these types of devices are available for purchase at your local Home Depot for installation on your phone.[219] Application of Scalia's "general public use" doctrine becomes moot as soon as technology advances. Putting aside the general public use argument, use of a StingRay device to locate a phone is distinct from use of a thermal-imaging device to detect heat emanating from a home in one key respect: StingRay devices are used to decipher the location of an object and a thermal-imaging device, as used in *Kyllo*, was used to reveal a fact about the home that could not have been deciphered through regular visual surveillance. Although the thermal-imaging device was used with the intention of locating marijuana, in order to locate the marijuana law enforcement had to first discover the temperature of the home.

C. Reasonable Expectation of Privacy in Content Versus Non-Content Data

The expectation of privacy in CSLI should be analyzed in the same way as other forms of technology in which users trasmit non-content data or communications. The United States Courts of Appeals for the Third,[220] Ninth,[221] and Tenth[222] Circuits have rejected

217. Kyllo v. United States, 533 U.S. 27, 34 (2001).

218. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 837 (2004).

219. *See, e.g.*, *FLIR ONE-Thermal Imaging Camera for Android*, HOME DEPOT, http://www.homedepot.com/p/FLIR-ONE-Thermal-Imaging-Camera-for-Android-757928/206480277 [https://perma.cc/QBJ9-SB9E] (last visited Sept. 17, 2017).

220. United States v. Christie, 624 F.3d 558, 573–74 (3d Cir. 2010) (finding that there is not a reasonable expectation of privacy in an IP address because it is voluntarily conveyed to third parties).

221. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (explaining that Internet users have no expectation of privacy in their IP information, because the information is provided to Internet providers "for the specific purpose of directing the routing of information").

the idea that there is a reasonable expectation of privacy in non-content-transmittal data such as email addresses or IP addresses.

In *Forrester*, the Ninth Circuit reasoned that "[t]he government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail."[223] During an investigation of an Ecstasy-manufacturing operation, the government utilized various surveillance techniques to monitor the defendant's e-mail and Internet activity.[224] The government installed a pen register known as a "mirror port" on the defendant's account and acquired not only the e-mail addresses he communicated with but the IP addresses of the websites he had visited and the total volume of information sent from his account.[225] The court cited to *Ex parte Jackson*,[226] in which the Supreme Court held "[l]etters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles."[227]

StingRay devices, as used by the United States government, operate in the same way as the mirror port in *Forrester*. Both devices acquire information as it is transmitted to a third party or parties. This is not the same as the third-party doctrine, because the information does not reach the third-party recipient before transmission to the government. As stated in *Carpenter*, "[a]lthough the content of personal communications is private, the information necessary to get those communications from point A to point B is not."[228] For these reasons, a cell phone user's reasonable expectation of privacy in their CSLI when obtained by government-operated IMSI-catchers, such as the StingRay, should be analyzed in the context of content versus

222. United States v. Perrine, 518 F.3d 1196, 1205 (10th Cir. 2008) (discussing that the use of peer-to-peer software, allowing others to access a computer, could expose information to the public and thus reduced any expectation of privacy in a computer's contents).

223. *Forrester*, 512 F.3d at 511.

224. *Id.* at 505.

225. *Id.*

226. 96 U.S. 727 (1877).

227. *Forrester*, 512 F.3d at 511 (quoting *Jackson*, 96 U.S. at 733). *See also* United States v. Hernandez, 313 F.3d 1206, 1209–10 (9th Cir. 2002) (holding that although a person has legitimate privacy interest in that a mailed package will not be opened and searched, there can be no reasonable expectation that postal service employees will not handle the package or that they will not view its exterior).

228. United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016), *cert. granted*, 137 S. Ct. 2211 (2017).

non-content data. This distinction makes the most sense in the context of contemporary Fourth Amendment jurisprudence. Because regulation of StingRays in the United States limits the type of data that may be obtained to non-content data, users do not have a reasonable expectation of privacy in the CSLI collected by government-operated IMSI-catchers.

CONCLUSION

Privacy interests must balance the interests of the individual and the interests of law enforcement; sacrificing one for the other does not benefit society as a whole. Cell phone users do not have a reasonable expectation of privacy in the information their phones disseminate to third parties. Differentiating non-content information from content information strikes a necessary balance between individual privacy and effective law enforcement.

Supreme Court precedent on the Fourth Amendment and technology as it stands today—as applied to government acquisition of CSLI—results in the conclusion that it is not a search. Although the Supreme Court will likely limit its ruling in *Carpenter* to historical CSLI without guidance as to government use of StingRay devices, the decision may motivate Congress to address the issue. If the Supreme Court analyzes an individual's reasonable expectation of privacy in data disseminated through technology by differentiating between content and non-content data, Congress can effectively enact legislation that reflects that concept. In addition, Congress is in the best position to address Justice Alito's concerns regarding long-term monitoring as expressed in *Jones*.[229] Other concerns regarding collection of CSLI and the use of StingRay devices are based on misconceptions of how the technology is actually utilized by law enforcement. Greater transparency by government about the use of StingRay devices and effective legislation would eliminate these concerns.

Although the idea of law enforcement tracking cell phones may give some cell phone users a sense of unease, this capability essentially comes with the territory of technology. As Justice Alito stated in *Jones*, "[n]ew technology may provide increased convenience or security at the expense of privacy . . . . [E]ven if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[230] Of course, the Supreme Court may decide to establish a new way of analyzing reasonable expectations of privacy as applied to

229. United States v. Jones, 565 U.S. 400, 424–27 (Alito, J., concurring).

230. *Id.* at 427.

technology in *Carpenter*, and thus hold that acquisition of CSLI by law enforcement is an unreasonable search. But until then, we may just have to shut our phones off.

Kristi Winner[†]

† J.D. Candidate, 2018, Case Western Reserve University School of Law. I would like to thank Lorain County Assistant Prosecuting Attorney, Matt Kern, for introducing me to StingRays and for his helpful guidance during my initial research; the Law Review staff for all of their hard work; and most importantly, my mother, Gail, and my sister, Amanda, for their endless love and support throughout my academic journey.