Touro Law Review

Volume 33 | Number 3 Article 18

2017

Stingrays, Triggerfish, and Hailstroms, Oh My: The Fourth Amendment Implications of the Increasing Government Use of Cell-Site Simulators

Jenna Jonassen

STINGRAYS, TRIGGERFISH, AND HAILSTORMS, OH MY! THE FOURTH AMENDMENT IMPLICATIONS OF THE INCREASING GOVERNMENT USE OF CELL-SITE SIMULATORS

Jenna Jonassen[*]

I. INTRODUCTION

Since as early as its interpretation in *Katz v. United States*,[1] the Fourth Amendment has protected the privacy rights of individuals in situations where a reasonable expectation of privacy exists.[2] This finding was based on a narrow reading of the Fourth Amendment's own language, which provides:

> The 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.[3]

However, emerging technology has undoubtedly called into question what was assumed to be an almost indelible protection of an

[*]Touro College Jacob D. Fuchsberg Law Center, J.D. Candidate 2018; Siena College, B.A., in English, minor in Writing and Communications, 2009. I would like to give a special thanks to my advisor, the Honorable Mark Cohen, for his inspiration, insight, and overwhelming confidence in my abilities throughout this process. I also owe gratitude to my parents, brother, and sister for their never-ending patience and encouragement while I work to achieve all of my law school aspirations. Thank you to all of my friends for their support in this endeavor, especially my lifelong friend, Kristin Sheridan, who provides nothing but endless love and laughs. Last, but certainly not least, I would like to thank my note editor, Jessica Vogele, for her guidance every step of the way—I could not have had a better role model.

[1] Katz v. United States, 389 U.S. 347 (1967).

[2] Christopher D. Browne, *Ill-Suited to the Digital Age: Problems with Emerging Judicial Perspectives on Warrantless Searches of Cell Site Location Information*, 4 NW. INTERDISCIPLINARY L. REV. 57, 83-84 (2013).

[3] U.S. CONST. amend. VI (emphasis added).

individual's privacy interests. In 2001, the United States Supreme Court recognized in *Kyllo v. United States*[4] that "[i]t would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology."[5] Yet, since *Kyllo* was decided, the amount of available technology has only grown, with the technology information business expected to become a $547 billion industry in 2017.[6] Consistent with the findings of the Supreme Court in *Kyllo*,[7] and particularly the late Justice Anton Scalia,[8] it is clear that this quickly-advancing technology has made it increasingly difficult for the Court to keep up with its potential constitutional implications. Now with the emergence of advanced surveillance equipment, it has become judicially and statutorily unclear as to what degree this technology either eliminates or reduces such expectations of privacy, especially with respect to cellular telephone devices.[9]

Today, cellular and mobile devices have become the primary platform for communication,[10] financial transactions,[11] political

---

[4] Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

[5] *Id.* at 34.

[6] *2017 Technology, Media, and Telecommunications Predictions Infographics*, DELOITTE GLOBAL, https://www2.deloitte.com/content/dam/Deloitte/global/Documents/Technology-Media-Telecommunications/gx-deloitte-2017-tmt-predictions-infographics.pdf (last visited Mar. 18, 2017).

[7] *Kyllo*, 533 U.S. at 34.

[8] United States v. Jones, 565 U.S. 400, 427 (2012) (Scalia, J., concurring) ("[T]he Katz test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

[9] This is based on the unanswered question as to whether an individual whose use of a device which knowingly transmits information through third-party wireless carriers actually has a reasonable expectation that the transmissions will remain private.

[10] *See Facts and Infographics Archive*, CTIA, http://www.ctia.org/resource-library/facts-and-infographics/archive/infographic-smartphones-comprise-77-percent-of-traffic-on-wireless-networks (last visited Mar. 18, 2017) (indicating that 56.6% of device connections in North America come from smartphones); Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CENTER (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/ (indicating that 67% of smartphone users use their phones to share pictures, videos, or commentary about community events).

[11] *See Facts and Infographics Archive*, CTIA, http://www.ctia.org/industry-data/facts-and-infographics-details/fact-and-infographics/98-percent-of-visit-growth-in-e-commerce-from-smartphones (last visited Mar. 18, 2017) (indicating that "[s]martphones account for 98% of

information,[12] content streaming,[13] and location services.[14] Since cellular technology has become a ubiquitous force in the function of today's society, it is of no surprise that local police and federal agencies have also attempted to take advantage of society's reliance on these devices by using them as an investigatory assistance tool to help establish the location of victims, fugitives, criminals, and terrorists.[15] With the development of military-type technology, federal and state police agencies have spent hundreds of thousands of dollars on cell-site simulator equipment that can be used to manipulate radio-frequency transmissions from cellular phone towers to give police an identified target's cellular location.[16] The most technologically-advanced versions of these simulators, devices known primarily as a StingRays, Triggerfish, or Hailstorms, have been used by numerous local and federal government agencies to obtain information from all

---

the growth in digital commerce site visits worldwide"); *Facts and Infographic Archives*, CTIA, http://www.ctia.org/industry-data/facts-and-infographics-details/fact-and-infographics/more-than-one-quarter-of-millennials-prefer-shopping-via-smartphone (last visited Mar. 18, 2017) (indicating that 28% of millennials in the United States alone "prefer shopping on their smartphones than on their computers"); Smith, *supra* note 10 (indicating that 57% of wireless users use their phones for wireless banking).

[12] *See Facts and Infographics Archive*, CTIA, http://www.ctia.org/resource-library/facts-and-infographics/archive/infographic-voters-increasingly-use-smartphones-for-political-info (last visited Mar. 18, 2017) (indicating that in 2014, approximately 28% of voters used their cellular smart devices for political information, more than double the amount in 2010); Smith, *supra* note 10 (indicating that 40% of cellular uses use their devices to look up government services or information).

[13] *See Facts and Infographics Archive*, CTIA, http://www.ctia.org/industry-data/facts-and-infographics-details/fact-and-infographics/young-adults-spend-more-than-11-hours-per-week-streaming-via-smartphones (last visited Mar. 18, 2017) (indicating that those between the ages of 18-24 spend more than 11 hours per week streaming content from their mobile phones); *Facts and Infographics Archive*, CTIA, http://www.ctia.org/resource-library/facts-and-infographics/archive/infographic-more-than-half-of-digital-video-views-will-be-on-mobile-next-year (last visited Mar. 18, 2017) (indicating that over 52% of all digital worldwide video views in 2016 will be from mobile devices).

[14] *See Facts and Infographics Archive*, CTIA, http://www.ctia.org/industry-data/facts-and-infographics-details/fact-and-infographics/73-percent-of-millennials-use-smartphone-when-lost (last visited Mar. 18, 2017) (indicating that 73% of millennials first turn to their cellular telephones when getting lost as opposed to utilizing other means); Smith, *supra* note 10 (indicating that 67% of smartphone users use their phone for "turn-by-turn navigation while driving," with 25% using their phone to obtain public transit information, and 11% using their phones "at least occasionally to reserve a car or taxi service.").

[15] *See, e.g.*, In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 451-52 (S.D.N.Y. 2006).

[16] *In Support of a Warrant Requirement for the Use of StingRays*, N.Y. CIV. LIBERTIES UNION, https://www.nyclu.org/en/legislation/support-warrant-requirement-use-stingrays (last visited Mar. 18, 2017).

surrounding cellular devices in order to locate their targets.[17] Once the target is discovered, the police are able to surveil with real-time tracking, leading them to the target's almost precise location without wasting valuable police time and resources.[18]

However, many have recognized that the ability of state and local governments to freely use such technology to their advantage does not come without potential Fourth Amendment implications.[19] In fact, few statutory and common law principles currently stand in the way of the government's ability to use and therefore potentially abuse these devices.[20] Similarly, minimal, if any, court approval is needed to authorize their use.[21]

Though initial use of this technology had previously evaded court intervention for quite some time,[22] jurisdictions are currently split as to how the benefits of this technology can still be used without violation of an individual's privacy rights.[23] Some authorities have required that agencies establish the minimal criteria needed for a pen-register/trap-trace warrant[24] before cell-site location data can be obtained through the use of a cell-site simulator.[25] Contrarily, some courts have placed a much heavier burden on the proponent, requiring that they establish sufficient probable cause[26] prior to its legal use.[27]

---

[17] *See id.*

[18] *Id.*

[19] *See, e.g.*, Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L. J. 183 (2014); 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. L. J. OF TECH. 1 (2014).

[20] Browne, *supra* note 2, at 57.

[21] Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE L.J. & TECH. 134, 142 (2013).

[22] Browne, *supra* note 2, at 57.

[23] Christopher Izant, Note, *Stingray Surveillance: Legal Rules by Statute or Subsumption*?, HARV. L. SCH. NAT'L SEC. J. (July 15, 2016 at 10:32 PM), http://harvardnsj.org/2016/07/stingray-surveillance-legal-rules-by-statute-or-subsumption/.

[24] 18 U.S.C. § 3122(b) (2012) (indicating what the contents of an application for a pen/register warrant must include).

[25] Izant, *supra* note 23.

[26] As a primarily judicial construct, "probable cause" has no statutory definition; however, the United States Supreme Court has indicated that it requires belief that the condition precedent to the execution of a search warrant will occur and that, once it has, "there is a fair probability that the contraband or evidence of a crime will be found in a specified place." U.S. v. Grubbs, 547 U.S. 90, 95 (2006) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

[27] Izant, *supra* note 23.

However, without any governing standard upon which to rely, the potential ongoing violation of individual privacy rights remains high with the continuing use of this technology.

Accordingly, this Note attempts to provide an accurate road map of the various types of information concerning cell-site simulator use and how its implications on Fourth Amendment rights call for the establishment of a sufficient probable cause warrant prior to its use. Section II will outline the basic technology behind the functionality of cellular telephones. This information is vital to the understanding of the concepts discussed in Section III, the basic functionality of cell-site simulator devices, more commonly known as StingRays, Triggerfish, or Hailstorms. Section III will also delve into the developments, costs, and frequency of use of such devices on a national spectrum.

Section IV will discuss the changes in the interpretation of the Fourth Amendment to the Constitution over time and how this "right to be left alone" has transformed with the progressions in new technology. Relatedly, Section V will address Congress's past and present attempts at providing guidance for the advancements in electronic surveillance equipment. As examined therein, it was not until a few years ago that the legality of cell-site simulators was even discussed, despite reports indicating their use by government agencies for several years prior.[28] While Section V will discuss the inadequacies of the law in regulating cell-site simulators, Section VI will document the strongest argument against the need for even minimal regulation of these devices—the third-party disclosure doctrine. This doctrine relies upon an individual's voluntary relinquishment of his privacy rights to third parties, which proponents argue occurs upon the signing of a cellular contract.[29] Section VII will analyze how the lower courts have interpreted the impact of the use of cell-site simulators on Fourth Amendment rights and therefore will provide a brief discussion of the current common law on this subject.

Finally, Section VIII will provide an overall analysis on this subject and how a Supreme Court decision on the quantum of proof necessary for the authorization of use of a cell-site simulator is desperately needed to provide the lower courts with reliable precedent. Nonetheless, because most cases and agency procedure guidelines

---

[28] Pell & Soghoian, *supra* note 21, at 143.

[29] Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

discussed herein seem to reflect the conclusion that cell-site simulators have a strong tendency to implicate an individual's Fourth Amendment rights, often inadvertently by the very nature of their functionality, it seems likely that the Supreme Court would resolve the jurisdictional splits by requiring that any potential user establish probable cause to justify such an intrusive invasion into an individual's private life.

II. BASIC CELLULAR PHONE FUNCTIONALITY

At the most basic level, a cellular phone is best described as a "short-range radio transmitter"[30] that has the capability of making and receiving calls through the transmission of radio frequencies to "cellular base stations" or "cell sites"[31] on cellular network towers[32] ("cell towers") generally located within three to 15 miles[33] from the cellular device. Upon receipt of these transmissions, the cell tower then transmits or "pings" this signal to other cell towers within the service provider's network until it becomes in range of the recipient of the call.[34] Therefore, in order for the radio frequency to transmit to the intended recipient, it must weave a path between the caller and the recipient by bouncing back and forth between the network's cell towers.[35] To ensure the strongest signal between the caller and the intended recipient, cell phones are able to locate the closest cell towers

---

[30] Browne, *supra* note 2, at 61.

[31] Owsley, *supra* note 19, at 187-88 (indicating that cell sites are usually placed "atop towers, but the equipment can also be placed on trees, roofs, flagpoles, and buildings.").

[32] *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006) (indicating that individual cellular towers within a network can be anywhere from miles apart (more common in less populated rural areas) to several hundred feet apart (more common in more highly populated areas)).

[33] Browne, *supra* note 2, at 61-62.

[34] Browne, *supra* note 2, at 62.

[35] The path which cell phone signals take is best exemplified by the following:

> When a caller dials a number on a cellular telephone, a transceiver sends signals over the air on a radiofrequency to a cell site. From there the signal travels over phone lines or a microwave to a computerized mobile telephone switching office ("MTSO") or station. The MTSO automatically and inaudibly switches the conversation from one base station and one frequency to another as the portable telephone moves from cell to cell.

Owsley, *supra* note 19, at 188.

by sending automatic signals in a procedure known as "registration."[36] This process finds the strongest signal by forcing the cellular phone to "identif[y] the closest tower, and ensure[] that calls sent to and received by the phone will be routed through that tower . . . ."[37]

This registration process occurs repeatedly every seven seconds as long as the cellular device is turned on[38] and cannot be controlled at the discretion of the cellular user.[39] It also permits the cellular device to be identified through a series of identification numbers[40] and allows the service providers "to create and maintain a record of every cell tower with which each phone on their networks has registered, and when each of those registrations happened."[41] This collected data stored by the cellular service provider is more commonly known as cell-site location information ("CLSI").[42] Through the collection of CLSI, the cellular service provider has the means to identify the location of a cellular user at any given time through monitoring of the registration process.[43] While cellular

---

[36] Owsley, *supra* note 19, at 188; Pell & Soghoian, *supra* note 21, at 144. The United States Department of Justice, via an Electronic Surveillance Manual, describes the registration procedure as follows:

> Cellular telephones that are powered on will automatically register or re-register with a cellular tower as the phone travels within the provider's service area. The registration process is the technical means by which the network identifies the subscriber, validates the account and determines where to route call traffic. This exchange occurs on a dedicated control channel that is clearly separate from that used for call content (i.e. audio) — which occurs on a separate dedicated channel.

Electronic Surveillance Manual: Procedures and Case Law Forms, U.S. DEP'T OF JUST., 178-79 n.41 (rev. June 2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.

[37] Browne, *supra* note 2, at 62.

[38] Browne, *supra* note 2, at 62.

[39] *Electronic Surveillance Manual*, *supra* note 36, at 40.

[40] *In re* Application of the U.S. for an Order Auth. the Use of a Pen Register and a Trap and Trace Device and Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005) ("[T]hese codes include an Electronic Serial Number (a unique 32-bit number programmed into the phone by the manufacturer), and a Mobile Identification Number, a 10-digit number derived from the phone's number.").

[41] Browne, *supra* note 2, at 62-63. The Department of Justice's Electronic Service Manual indicates that the collection of this data is necessary to "provide service to cellular telephones." *Electronic Surveillance Manual*, *supra* note 36, at 42.

[42] Browne, *supra* note 2, at 63.

[43] Browne, *supra* note 2, at 63 (indicating that the registration process allows a network carrier "to pinpoint the location of a cell phone by cross-referencing the location of the cell tower with which the phone registered, at the time at which the registration occurred. Using this information, a cell phone service provider can determine the location of a cell phone, and by implication its user, at virtually any point in time . . . ."). *See also* In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Telephone,

carriers claim that the collection of such data is primarily used by network service providers for billing purposes,[44] use of this information leaves the carrier able to identify a cellular device within an isolated range of the nearest cell tower,[45] the accuracy of which increases with the growing use of smart phone technology and the installation of more cell towers by service providers.[46]

III. CELL-SITE SIMULATORS: DEVELOPMENTS, COSTS, AND USAGE

Cell-site simulators, otherwise known as International Mobile Subscriber Identity ("IMSI") catchers, are the government's most widely used "spy" tools to track cellular phone activity.[47] The concept was first invented by a German manufacturing company known as Rohde & Schwarz in 1996 when it created a machine that forced cellular devices within range to identify their own serial numbers for surveillance purposes.[48] However, the technology behind this concept quickly advanced as the United States government, military agencies, and intelligence agencies helped in making these devices more refined.[49] In just a few years, the Harris Corporation, a Florida-based

460 F. Supp. 2d 448, 451 (S.D.N.Y. 2006) ("Knowledge of the locations of multiple towers receiving signals from a particular telephone at a given moment permits the determination, by simple mathematics, of the location of the telephone with a fair degree of precision through the long established process known as triangulation."); Pell & Soghoian, *supra* note 19, at 12-13 (indicating that the service provider is not only able to pinpoint the phone's location, but also numbers recently called and other personal data).

[44] *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Telephone*, 460 F. Supp. 2d at 451 (indicating that this information is generally used to determine whether roaming charges apply or to track call volume to determine the need for more cell towers).

[45] *Id.* at 450-51 (stating that in some cases the closest tower receiving the signal from a cellular device can pinpoint not only the range of the device from the tower, but also "in which of the three 120-degree arcs of the 360-degree circle surrounding the tower the particular phone is located."); Browne, *supra* note 2, at 64 (indicating that this degree of accuracy can be up to a 200-foot range, which is enough to determine a cell phone user's location in "a building or other residence").

[46] Browne, *supra* note 2, at 64.

[47] *See generally Electronic Surveillance Manual*, *supra* note 36; Pell & Soghoian, *supra* note 21.

[48] Pell & Soghoian, *supra* note 19, at 13-14 (citing Dirk Fox, *IMSI-Catcher*, 21 DATENSCHUTZ UND DATENSICHERHEIT 539, 539 (1997)).

[49] Pell & Soghoian, *supra* note 19, at 14.

manufacturer,[50] exclusively developed, and continues to develop,[51] more sophisticated cell-simulator devices, including Triggerfish, and the most commonly-known and technologically advanced version, the StingRay machine.[52]

Still, little is known about the specifics behind the development of these highly technical machines outside of what is minimally provided by patent and trademark registration information[53] and Freedom of Information Law ("FOIL") requests made by advocates against the use of cell-site devices to numerous police departments and the Federal Bureau of Investigation ("FBI").[54] For example, purchase orders released in response to these FOIL requests fail to indicate anything more than the fact that these machines were purchased from the Harris Corporation at relatively high prices.[55] However, what is

---

[50] According to the Harris Corporation's website, it specializes in the manufacture of "tactical communications, geospatial systems and services, air traffic management, environmental solutions, avionics and electronic warfare, and space and intelligence." *About Harris*, HARRIS TECHNOLOGY, https://www.harris.com/about (last visited Mar. 18, 2017).

[51] Ryan Gallagher, *Law & Disorder: Meet the Machines that Steal Your Phone's Data*, ARS TECHNICA (Sept. 25, 2013, 1:00 PM), http://arstechnica.com/tech-policy/2013/09/meet-the-machines-that-steal-your-phones-data/.

[52] *See* W. Scott Kim, Note, *The Fourth Amendment Implications on the Real-Time Tracking of Cell Phones Through the Use of "Stingrays,"* 26 FORDHAM INTELL. PROP., MEDIA & ENT. L. J. 995, 1001 (2016) (indicating that the Patent and Trademark Office reveals that the name StingRay was registered as a trademark in 2003 by the Harris Corporation); Pell & Soghoian, *supra* note 19, at 14-15; Gallagher, *supra* note 51 (indicating that trademark information for the first StingRay machine was filed by Harris Corporation in August 2001); *Stingrays*, N.Y. CIV. LIBERTIES UNION, http://www.nyclu.org/stingrays (last visited Mar. 18, 2017).

[53] Gallagher, *supra* note 51. In fact, the Harris Corporation website itself does not indicate to the public that it manufactures such equipment. Kim, *supra* note 52, at 1000.

[54] *See Stingrays*, *supra* note 52 (discussing FOIL requests made to the Erie County Sheriff's Office, Rochester Sheriff's Department, and the New York State Police in 2015).

[55] The New York Civil Liberties Union website indicates that in May 2014, the New York State Police released purchase orders which revealed that they had paid $197,100 to obtain a StingRay device in 2005, as well as a total of $263,230 to maintain and upgrade equipment and provide training for StingRay machines in 2012, which increased in 2013 by $181,174. This revealed that the New York State Police had spent at least $651,504 on this StingRay machine. Also, in May 2016, the Rochester Police Department produced information that they purchased a StingRay machine known as "KingFish" from the Harris Corporation in June of 2015. The information further provides that KingFish is able to be attached to department vehicles to identify and track cellular devices and costs the Rochester New York Police Department approximately $200,600 for hardware, software, and training on use of the device. The website also suggests that such hardware would likely cost the Rochester Police Department additional thousands of dollars to be used for yearly maintenance fees with the Harris Corporation in order to keep the cell-site simulator operational. In particular, one record revealed that the Harris Corporation informed the Rochester Police Department that it had to upgrade its KingFish unit to the Hailstorm unit to keep its technology operational for a cost of $388,000. *See Stingrays*, *supra* note 52.

known is that the Harris Corporation has earned approximately $40 million from technology contracts with local city and state police authorities in providing cell-site simulator equipment.[56] Based on the availability of procurement records, federal authorities alone have been noted to spend over $30 million on cell-site simulator equipment since 2004.[57] However, most authorities show that the funding for such machines comes from the federal government through anti-terror grants.[58]

StingRay machines have been described as "box-shaped portable device[s]," which function by impersonating cellular base stations[59] and deceiving any nearby cellular devices into thinking that they are connecting to a cellular tower.[60] The portability of the device is important to its function, as it can be set up anywhere, even in moving vehicles.[61] Accordingly, these devices can be easily moved to more accurately pinpoint the location of a cellular device user in real time.[62]

Though police agencies admit that use of these devices is an essential investigatory tool that provides "important crime-fighting and surveillance techniques"[63] that can "help solve crimes, track fugitives or abducted children or even foil a terror attack,"[64] the information obtained from a StingRay is not narrowly limited to the subject of the agency's search.[65] Contrarily, StingRay devices are known to force *all* cell phones in the area of the cell tower to send their

---

[56] Gallagher, *supra* note 51.

[57] Gallagher, *supra* note 51.

[58] 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-nsa-police/3902809/ (last visited Mar. 18, 2017).

[59] Gallagher, *supra* note 51.

[60] Pell & Soghoian, *supra* note 19, at 11; Gallagher, *supra* note 51.

[61] Gallagher, *supra* note 51.

[62] Ryan Gallagher, *FBI Accused of Dragging Feet on Release of Info About "Stingray" Surveillance Technology*, SLATE: FUTURE TENSE (Oct. 19, 2012, 4:00 PM), http://www.slate.com/blogs/future_tense/2012/10/19/stingray_imsi_fbi_accused_by_epic_of_dragging_feet_on_releasing_documents.html.

[63] Kelly, *supra* note 58.

[64] Kelly, *supra* note 58.

[65] Proposed Brief Amicus Curiae in Support of Daniel Rigmaiden's Motion to Suppress at 1, 3, United States v. Rigmaiden, No. CR 08-814-PHX-DGC, 2013 WL 1932800 (No. 904-3), https://www.aclu.org/files/assets/rigmaiden_amicus.pdf (referring to such a search as a "dragnet sweep" and indicating that in "locat[ing] a suspect's cell phone, [S]ting[R]ays obtain information from *all* devices on the same network in a given area and send signals into the homes, bags, or pockets of the suspect and third parties alike."). Kim, *supra* note 52, at 997.

identification information to the device.[66] Since the machine is only able to detect a particular cellular phone's identification once it registers with a network, the device must search and collect information from *every* in-range cellular device before it can actually pinpoint the targeted user.[67] Some upgrades to the StingRay machines make their functionality even more intrusive—software upgrade "FishHawk" allows users to listen to conversations without the cellular user's knowledge, while the "Porpoise" upgrade can be installed to provide dual-functionality for surveillance of both location and incoming and outgoing text messages.[68]

As reported by the American Civil Liberties Union ("ACLU"), at least 68 agencies in 23 different states have admitted to owning at least one cell-site simulator.[69] The New York Police Department, the biggest municipal police department in the nation, is claimed to have used cell-phone tracking devices at least 1,000 times since 2008, or as frequently as 200 times per year, all the while avoiding any judicial guidance as to the constitutionality of its use due to the lack of requirements.[70] In Erie County, New York, reports reveal that the Sheriff's Office had utilized cell-site simulator technology approximately 47 times during investigations over the last four years, while only once obtaining a minimum degree of judicial approval before using the equipment.[71] On a federal level, agencies known to use cell-site simulation technology include the Federal Bureau of Investigation ("FBI"); the Drug Enforcement Administration ("DEA"); the United States Secret Service; the Immigration and Customs Enforcement; the United States Marshals Service; the Bureau

---

[66] Proposed Brief Amicus Curiae, *supra* note 65, at 8, 10.

[67] Izant, *supra* note 23.

[68] Gallagher, *supra* note 51.

[69] Such states are noted to include Alaska, Arizona, California, District of Columbia, Delaware, Florida, Georgia, Illinois, Indiana, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Missouri, New York, North Carolina, Oklahoma, Pennsylvania, Tennessee, Texas, Virginia, Washington, and Wisconsin. Other states continue to conceal whether they use cell-site simulator technology for investigative purposes and whether there is any judicial approval prior to their use of the machines. *Stingray Tracking Devices: Who's Got Them?*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last visited Mar. 18, 2017).

[70] Joseph Goldstein, *New York Police Are Using Covert Cellphone Trackers, Civil Liberties Group Says*, N.Y. TIMES (Feb. 11, 2016), http://www.nytimes.com/2016/02/12/nyregion/new-york-police-dept-cellphone-tracking-stingrays.html.

[71] *NYPD Has Used Stingrays More Than 1,000 Times Since 2008*, N.Y. CIV. LIBERTIES UNION (Feb. 11, 2016), http://www.nyclu.org/news/nypd-has-used-stingrays-more-1000-times-2008.

of Alcohol, Tobacco, Firearms, and Explosives; the Internal Revenue Service; the United States Army; the United States Navy; the United States Marine Corps; the United States National Guard; the United States Special Operations Command; and the National Security Agency.[72]

IV. THE FOURTH AMENDMENT: THE RIGHT TO BE LEFT ALONE

A. Early Interpretations of the Fourth Amendment

While the Fourth Amendment explicitly states that "[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,"[73] this seemingly simple and unequivocal statement of rights has triggered "[o]ver a century of jurisprudential uncertainty."[74] Though the scope and application of the Fourth Amendment has changed considerably over time, with this uncertainty being such a significant part of the history of the Fourth Amendment, it is no surprise that the modern advancements in technology continue to frustrate the application of the Fourth Amendment.[75]

Initially, the Supreme Court had interpreted the context of the Fourth Amendment to be a mere extension of an individual's property rights, based on the concept that, sans technology, both physical trespass and intrusion had to occur for a government agent to actually conduct a search.[76] As a result, the Supreme Court held that Fourth Amendment rights were only implicated during *actual* physical intrusion of an individual's private property.[77] However, the Supreme Court shifted its application after deciding *United States v. Katz*, in

---

[72] *Stingray Tracking Devices: Who's Got Them?*, *supra* note 70.

[73] U.S. CONST. amend. VI.

[74] Will Stancil, Note, *Warrantless Search Cases Are Really All the Same*, 97 MINN. L. R. 337, 339 (2012).

[75] *Id.* ("Over a century of jurisprudential uncertainty has stemmed from warring interpretations of those twenty-four words.").

[76] *Id.* at 340-41.

[77] *See* Olmstead v. United States, 277 U.S. 438 (1928) (as the seminal case to initially determine that Fourth Amendment protection stemmed from property interests). Further, *compare* Goldman v. United States, 316 U.S. 129, 135-36 (1942) (holding that a monitoring device placed *against* the wall of a private residence was not unlawful) *with* Silverman v. United States, 365 U.S. 505, 511-12 (1961) (holding that police surveillance violated Fourth Amendment rights of the defendant when evidence was obtained upon use of a device that was *physically driven into the wall*).

which it found that the Fourth Amendment did not protect property or places but instead protected people.[78] Therefore, any person who had a "justifiable, reasonable, or legitimate" expectation of privacy which was annexed by government action would have standing to claim a Fourth Amendment violation.[79] Under *Katz*, physical trespass of property was no longer the only means under which one could claim a Fourth Amendment violation,[80] forcing the Court to subsequently define the circumstances that would prompt a "reasonable expectation of privacy" in order to comply with the *Katz* test. While cases were determined on a fact-specific basis, it was generally held that reasonable expectations of privacy did *not* exist in situations where someone had voluntarily made otherwise private details available for public knowledge,[81] or in areas where little, if any, intimate activities took place.[82] However, while this is easily applied to the aforementioned situations, the courts struggled with the introduction of modern technology and how it complied with the *Katz* test.

B. The Fourth Amendment as Applied to New Technology

Of all of the Court's cases which confronted the use of new technology, *Kyllo v. United States*[83] is certainly one of the most influential, since its holding broadly applied Fourth Amendment protections to emerging surveillance equipment.[84] Evaluating whether or not the use of a thermal imaging device to read heatwaves from the interior of defendant's home constituted an unreasonable search in

---

[78] United States v. Katz, 389 U.S. 347, 351 (1967).

[79] *Id.* at 352 (indicating that a person who enters a telephone booth, though within public view, is still a person protected by the Fourth Amendment so long as he has an objective reasonable belief and assumption "that the words he utters into the mouthpiece will not be broadcast to the world.").

[80] *Id.* at 352-53.

[81] *See, e.g.*, Florida v. Riley, 488 U.S. 445 (1989) (holding that an individual had no reasonable expectation of privacy in performing illegal activities in an area that was commonly and easily visible from the air); California v. Greenwood, 486 U.S. 35 (1988) (holding that a police search of garbage left on the street was not in violation of an individual's Fourth Amendment rights).

[82] Oliver v. United States, 466 U.S. 170, 179 (1984) (holding that an open field was not intended to be protected from government intrusion under the Fourth Amendment because it does "not provide the setting for . . . intimate activities . . .").

[83] Kyllo v. United States, 533 U.S. 27 (2001).

[84] *Id.*

violation of the Fourth Amendment,[85] the Court held that an individual has an indelible, and therefore reasonable, expectation of privacy within the four walls of the home, and the information that was obtained by the use of the thermal imaging device, though not obtained by *physical* means, still constituted an unreasonable intrusion because the information could not have been obtained otherwise.[86] Justice Scalia, writing for the majority, indicated that the Fourth Amendment was not constricted by technological advancements, especially when these advancements intruded into the most protected area of private property— the four walls of the home.[87] However, Justice Stevens, joined by Justice O'Connor and Justice Kennedy, wrote in the dissent that the only actual intrusion into the home was heat, and given that heat could be just as easily sensed by any member of the public from outside the home as it could from a thermal imaging device, an individual would have no reasonable expectation of privacy against it.[88] Had the Court utilized the overly simplistic rationale of the dissent, arguably any use of modern surveillance technology would pose no reasonable threat against an individual's perception of privacy because anyone from the general public could technically observe one's location.

The Court subsequently addressed a technological advancement similar to cell-site simulators in *United States v. Knotts*.[89] In *Knotts*, the Court set out to determine whether the use of location technology constrained the protections provided by the Fourth Amendment.[90] The Court held that police reliance on a beeper's signal to track the final destination of defendant's vehicle did *not* violate the defendant's reasonable expectation of privacy,[91] relying on the concept that an individual "traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one

---

[85] *Id.* at 29.

[86] *Id.* at 35-39, 40.

[87] *Id.* at 33-34.

[88] *Kyllo*, 533 U.S. at 42-44 (Stevens, J., dissenting) ("Any member of the public might notice that one part of a house is warmer than another part or a nearby building if, for example, rainwater evaporates or snow melts at different rates across its surfaces. Such use of the senses would not convert into an unreasonable search if, instead, an adjoining neighbor allowed an officer onto her property to verify her perceptions with a sensitive thermometer.").

[89] United States v. Knotts, 460 U.S. 276 (1983).

[90] *Id.* at 277.

[91] *Id.* at 284-85.

place to another."[92] The Court reasoned that such information was not private and could have easily been gathered by simple observation.[93] Due to the obvious lack of intrusion involved in obtaining information made public versus that obtained from the interior of a home, the most private and protected of locations, it is clear why the Court ruled differently in *Knotts* than it did in *Kyllo*.

Contrarily, in deciding *United States v. Karo*,[94] the Court held that location surveillance equipment placed into a can of chemicals to monitor the movement of the container in connection with potential drug trafficking *did* pose a Fourth Amendment violation.[95] In this case, the DEA learned that the defendant had ordered 50 gallons of ether from a government informant to extract cocaine from clothing that had been trafficked into the United States.[96] In response, the DEA planted a location-tracking device in one of the cans of ether that it delivered to the defendant.[97] Using the tracking device to follow the location of the ether, the DEA traced the signal to many locations, one of which was the defendant's own residence.[98] In contrast to the facts of *Knotts*, the government's device in *Karo* was able to track the defendant's movements *inside* the walls of his own home which could not have been obtained through simple visual observance.[99] As a result, the Court ruled that this was an unreasonable intrusion.[100]

With the development of more precise location technology, the Supreme Court was once again forced to address technology's impact on Fourth Amendment rights in *United States v. Jones*.[101] Here, the Court addressed the government's placement of a global-positioning ("GPS") tracking device to the undercarriage of the defendant's vehicle.[102] Using this device, the government was able to monitor the defendant's whereabouts for a total of 28 days on suspicion of drug

---

92 *Id.* at 276.

93 *Id.*

94 United States v. Karo, 468 U.S. 705 (1984).

95 *Id.* at 706.

96 *Id.* at 708.

97 *Id.*

98 *Id.* at 709.

99 *Karo*, 468 U.S. at 715 (contrasting this case with *United States v. Knotts* in that the information obtained here was not something that could have been "visually verified").

100 *Id.* at 718.

101 United States v. Jones, 565 U.S. 400 (2012).

102 *Id.* at 402.

trafficking.[103] In holding that this GPS tracking constituted an unreasonable search under the Fourth Amendment,[104] the Court asserted that the *Katz* reasonable expectation of privacy test did not *substitute* the Fourth Amendment rights for common law trespass, but merely *added* to them.[105] More simply put, although the Court had previously indicated that physical intrusion and trespass of property were required for a search to have actually occurred,[106] the decision in *Jones* broadened the list of activities which constituted a search within the context of the Fourth Amendment.[107] In light of this, the concurrence found that the defendant *did* have a reasonable expectation of privacy in his public whereabouts when under long-term monitoring by the government.[108] Specifically, Justice Sotomayor conceded that the concept of location tracking in general threatened an individual's reasonable expectations of privacy:

> GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . .
>
> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may alter the relationship between citizen and government in a way that it is inimical to democratic society.

---

[103] *Id.* at 402-03.

[104] *Id.* at 404, 413.

[105] *Id.* at 409.

[106] Olmstead v. United States, 277 U.S. 438, 466 (1928).

[107] *Jones*, 565 U.S. at 404 (holding that the installation of a GPS device on a vehicle with the purpose of monitoring the whereabouts of the vehicle constituted a search under the Fourth Amendment).

[108] *Id.* at 413-14 (Sotomayor, J., concurring).

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. 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.[109]

Justice Sotomayor's concurrence, especially when considered in conjunction with the majority opinion, suggested that modern technological advancements do not limit an individual's rights pertaining to unreasonable search and seizures as provided under the Fourth Amendment.

It has been argued that the placement of advanced technology in the hands of the public can leave those individuals with no true expectation of privacy, as people who are aware of the capabilities of technology should have no expectation to be safe from it.[110] Nonetheless, the Court has consistently held steadfast to the belief that Fourth Amendment rights are fixed and not amorphous.[111] While the Court has placed great emphasis on the expectation of privacy found within the four walls of the home, an overall analysis of the aforementioned Supreme Court cases reveal that one has a reasonable expectation of privacy in *any* act that is not knowingly made public or ordinarily observed.

V. DEVELOPMENT OF THE LAW AS APPLIED TO CELL-SITE SIMULATION DEVICES

With little case law discussing the limitations of law enforcement in utilizing cell-site simulation devices, there is a

---

[109] *Id.* at 415-16 (Sotomayor, J., concurring).

[110] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580 (2009).

[111] *See, e.g.*, *Jones*, 565 U.S. at 404, 413 (affirming the decision of the United States Court of Appeals for the District of Columbia Circuit and holding that an individual's privacy rights were not minimized by the government's warrantless placement of GPS technology on the individual's vehicle); Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the government's use of a thermal imaging device to expose intimate and private details about the petitioner was unconstitutional); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that the government's use of an electronic recording device positioned outside of a telephone booth in order to listen to the petitioner's words violated his reasonable expectation of privacy).

concomitant lack of agency guidance concerning use of this technology, especially when compared with other devices used by the government.[112] What little is known about the regulation of cell-site simulators is comprised in a few acts and magistrate opinions which fail to account for both the frequency and recommended use of cell-site simulators.[113] Only when carefully pieced together can such scarce guidelines actually assist in determining the restraints that the government must take in using such intrusive technology. Although they are few and far between, there are some acts, common law, and Department of Justice guidelines that have impacted the law concerning the collection of cell-site information.[114] Below is a brief history of some of the most relevant acts and orders that have shaped the law surrounding the collection of cell-site data as known today.

A. The Electronic Communications Privacy Act of 1968 and Pen/Trap Orders

The Electronic Communications Privacy Act of 1968 ("ECPA") was, and still is, well-known for affixing some of the primary restrictions on surveillance technology.[115] While the ECPA included three titles,[116] Title II and Title III of the Act are the most relevant to the types of electronic communication discussed herein.

Title III of the ECPA contains provisions for the issuance of Pen Registers and Trap/Trace devices and is otherwise known as the "Pen/Trap Statute."[117] Under the ECPA, a "pen register" is a tool that records outgoing numbers dialed from the targeted device, while a "trap/trace device" is a tool that captures incoming numbers from the targeted device.[118] Authorization for the use of such devices requires only two pieces of information: 1) the identity of the government agent making the application, and 2) the government agent's certification that the information to be obtained is relevant to the pending criminal

---

[112] Pell & Soghoian, *supra* note 19, at 20.

[113] Pell & Soghoian, *supra* note 19, at 20.

[114] *See* Pell & Soghoian, *supra* note 19, at 20-34.

[115] *In re* Application of the U.S. for an Order Auth. the Use of a Pen Register and a Trap and Trace Device and Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005).

[116] *Id.*

[117] *Id.* at 752.

[118] *Id.*

case.[119] Once such certification is made, the reviewing judge is forced to issue an *ex parte* order, even if there is doubt as to the facts and circumstances surrounding the certification.[120]

Based on this Act, the United States Department of Justice issued a 2005 Electronic Surveillance Manual and took the position that Pen/Trap orders "must be obtained by the government before it can use its own device to capture [codes unique to] a cellular telephone," including location information.[121] However, that very same manual also indicates that Pen/Trap devices do *not* include those that "identify that telephone to the network" or "receive[s] radio signals, emitted from a wireless cellular telephone."[122] Given that cell-site simulators both identify telephones on a network *and* receive signals emitted from other wireless cellular telephones, it is clear that the Department of Justice purposefully excluded these devices from the list of those that require even the minimal requirements of a Pen/Trap Order.[123] While a subsequent 2013 Department of Justice document indicated that a Pen/Trap Order is necessary when the government is trying to obtain codes unique to a target phone, it failed to address what type of court authorization, if any, is required to obtain cellular location data.[124] Furthermore, even though the Pen/Trap provision under this Act was amended in 2001 to include any device that also captures "signaling information," the type of court authorization required for location information continues to be unclear.[125]

---

[119] *Id.* at 753 (citing 18 U.S.C. § 3122(b) (2012)).

[120] *In re Application of the U.S. for an Order Auth. the Use of a Pen Register and a Trap and Trace*, 396 F. Supp. 2d at 753.

[121] Linda Lye, *Stingrays: The Most Common Surveillance Tool the Government Won't Tell You About*, AM. CIV. LIBERTIES UNION OF N. CAL. 1, 5 (June 27, 2014), https://www.aclunc.org/sites/default/files/StingRays_The_Most_Common_Surveillance_Tool_the_Govt_Won%27t_Tell_You_About_0.pdf.

[122] *Id.*

[123] *Id.* (indicating that despite the fact that cell-site simulators are excluded from the Pen/Trap Order requirements, court authorization is recommended "out of an abundance of caution").

[124] *Id.*

[125] *Id.*

B. The Stored Communications Act

In response to the Supreme Court's decision in *Olmstead v. United States*,[126] Congress enacted the Stored Communications Act ("SCA"), barring service providers from willingly disclosing customer communication information to any outside source, including the government, absent a qualifying exception.[127] If such information is required, however, the SCA provides the necessary procedure that the government must follow in order to obtain a telecommunication customer's information.[128]

Despite the fact that the SCA frustrates the practices of many federal agencies that rely on their unfettered ability to obtain electronic communications,[129] the SCA is also drastically inconsistent and provides little guidance as to what is required for authorized disclosure:

> For example, the SCA contained multiple provisions allowing for the disclosure of the same stored communications. Under subsection (c)(1)(A), the SCA allows disclosure of communication information upon the issuance of a warrant based on probable cause. However, subsection (c)(1)(B) refers the reader to subsection (d) of the same provision, which states that a court "shall issue" an order directing a cell-service provider to disclose electronic communications only if the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the … records or other information sought[] are relevant and material to an ongoing criminal investigation." The standard of proof of subsection (c)(1)(A), probable cause, and that of subsection (c)(1)(B), relevance to an ongoing criminal investigation, are clearly different.[130]

---

[126] Olmstead v. United States, 277 U.S. 438 (1928).

[127] Jeremy H. D'Amico, Note, *Cellphones, Stingrays, and Searches! An Inquiry into the Legality of Cellular Location Information*, 70 U. MIAMI L. REV. 1252, 1269, 1273 (2016); Richard M. Thompson II & Jared P. Cole, *Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA)*, CONGRESSIONAL RESEARCH SERVICE 1, 3 (May 19, 2015), https://fas.org/sgp/crs/misc/R44036.pdf.

[128] Thompson II & Cole, *supra* note 127.

[129] Thompson II & Cole, *supra* note 127, at 1.

[130] D'Amico, *supra* note 127, at 1272.

The SCA appears to allow courts to authorize obtainment of cell-site data both by a necessary showing of probable cause, a relatively high burden for the government to meet, *while at the same time* authorizing the obtainment of cell-site data under a much lower burden of proof of reasonable materiality to an ongoing investigation.[131] As previously indicated by critics of the SCA: "Why would law enforcement seek to satisfy the probable cause standard under subsection (c)(1)(A) if it can obtain the same stored communications under a relevance standard of subsection (c)(1)(B)?"[132]

The SCA also does not explicitly indicate whether cell-site data is a "stored communication" that is even covered under the SCA.[133] For example, the SCA's definition of "electronic communications" fails to include that which comes from a "tracking device,"[134] seeming to indicate that cell-site information could still be obtained regardless of the SCA's limitations. With the amorphous technology of cell-site simulators, the SCA provides little restriction on the government's use.

C. Communications Assistance for Law Enforcement Act

In October 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") in order to require telecommunication carriers to obtain the technology and equipment necessary to provide cellular data information to the government upon its request.[135] The government enacted CALEA due to "concerns that emerging technologies such as digital and wireless communications were making it increasingly difficult for law enforcement agencies to execute authorized surveillance."[136] In 2006, Congress expanded the reach of CALEA to include broadband Internet access providers in the statute's definition of "telecommunication carriers."[137]

---

131 D'Amico, *supra* note 127, at 1272-73.

132 D'Amico, *supra* note 127, at 1273.

133 D'Amico, *supra* note 127, at 1273-74.

134 D'Amico, *supra* note 127, at 1274.

135 Lye, *supra* note 121, at 6.

136 *Introduction*, *Communications Assistance for Law Enforcement Act*, FEDERAL COMMUNICATIONS COMMISSION, https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance#introduction (last updated Feb. 9, 2017).

137 *Id*.

While CALEA prohibits the government's use of a Pen/Trap Order when trying to obtain an individual's location information,[138] the Department of Justice's 2005 Electronic Surveillance Manual has indicated that the government can still use cell-site simulators and other IMSI catchers to obtain location information.[139] This is mostly due to a nuanced interpretation of CALEA, as it only applies to "information collected by a provider and not information collected directly by law enforcement authorities."[140] Therefore, interpreting when it is safe to use a cell-site simulator, in what capacity, and upon what authorization remains unclear.

D. The 2001 U.S.A. Patriot Act

As technology rapidly advanced at the beginning of the twenty-first century, the government's need for easy access to a vast array of electronic data also reached an all-time high. After the September 11, 2001 terrorist attacks, Congress enacted the Patriot Act, which was characterized as a "'sweeping antiterrorism law that gave the government vast new powers to conduct electronic surveillance. . . ."[141] Though enacted to increase the government's role in the private lives of citizens for protection purposes, the Patriot Act actually increased the privacy of many individuals when it came to cell-site information[142]—something that had yet to be definitively done before.

Under the Patriot Act, the term "pen register" was expanded to include any "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"[143] and it required definitive court authorization, by way of a Pen/Trap Order,[144] before it could be obtained by the

---

138 Lye, *supra* note 121, at 6.

139 Lye, *supra* note 121, at 6.

140 Lye, *supra* note 121, at 6.

141 Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 607 (2003).

142 Pell & Soghoian, *supra* note 19, at 26.

143 Pell & Soghoian, *supra* note 19, at 26 n.130.

144 As a reminder, a Pen/Trap Order requires *only* that the government agent making the application identify himself or herself and certify that the information to be obtained is relevant to a pending criminal investigation. 18 U.S.C. § 3122(b) (2012).

government.[145] Given that cell-site simulators work by obtaining information from the signals emitted by a cellular device, the Patriot Act suggested that the government's use of cell-site simulators had to be preceded by a Pen/Register Order authorized by the court.[146] Although the proof necessary to obtain a Pen/Register Order is not a particularly difficult burden for the government to meet,[147] the Patriot Act at least prevents the government from using cell-site simulation technology without *any* authorization by the court, as was likely previously allowable under the SCA and CALEA due to their conflicting provisions.

E. The 2012 StingRay Magistrate Opinion

Despite the government's long-term use of cell-site simulators, it was not until 2012 that federal judges began to address the capacities of cell-site simulators and their impact on individual's Fourth Amendment search and seizure rights. In 2012, a Texas federal magistrate judge issued one of the first orders denying the use of a StingRay machine, a portable device that would allow the government to capture radio signals from the target's cellular telephone, analyze the target's registration data, and use the collected information to determine his location.[148] In this particular case, the DEA was conducting a criminal investigation of the defendant, a suspected narcotics trafficker.[149] Having knowledge that the defendant had been using his cell phone to initiate trafficking operations, the DEA applied to the court for authorization to install and use "a pen register trap and trace device for a period of sixty (60) days to detect radio signals emitted from wireless cellular telephones in the vicinity of the [defendant]. . . ."[150] The DEA further notified the court that it intended to obtain this information through the use of a StingRay machine.[151]

---

145 Pell & Soghoian, *supra* note 19, at 27.

146 Pell & Soghoian, *supra* note 19, at 27.

147 *See supra* note 144.

148 In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012).

149 *Id.* at 748.

150 *Id.*

151 *Id.*

While the court noted that Pen/Register Orders had typically been used to obtain cellular data,[152] it also indicated that the method that the DEA proposed to use to obtain the data in this case would virtually transform the defendant's cellular phone into a government tracking device.[153] As the burden of proof for a Pen/Register Order would only require the identity of the government agent making the application and his certification that the information to be obtained is relevant to a pending criminal case,[154] the court determined that the DEA's use of a StingRay machine to track the defendant required a higher burden of proof than a typical Pen/Trap Order.[155] Due to the wide array of information that could be obtained with the StingRay device, as well as the DEA's lack of proof as to why the StingRay machine would be sufficiently allowable for use under only a Pen/Register Order, the court denied the DEA's application for its use.[156] The court was concerned that the DEA was unable to explain the StingRay technology and how it could be limited to obtaining only the defendant's information.[157] Clearly, the high likelihood of infringement, even inadvertently, on an individual's constitutional rights had finally become apparent.

F. The September 2015 U.S. Department of Justice Order of Public Affairs re: Enhanced Policy for Use of Cell-Site Simulators

On September 3, 2015, the Department of Justice issued a directive specifically related to the government's use of cell-site simulators during investigations, requiring "increased privacy protections and higher legal standards."[158] The directive promised to

---

[152] *Id.* at 748-49; *see also* In the Matter of an Application of the United States of America For an Order Authorizing the Use of a Two Pen Register and Trap and Trace Devices, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008) (granting the government's application for the obtainment of cell-site information because it was based on "specific and articulable facts showing reasonable grounds to believe that the information sought is relevant and material to an ongoing criminal investigation").

[153] *In the Matter of the Application of the United States of America*, 890 F. Supp. 2d at 752.

[154] 18 U.S.C. § 3122(b) (2012).

[155] *In the Matter of the Application of the United States of America*, 890 F. Supp. 2d at 752.

[156] *Id.*

[157] *Id.* at 749.

[158] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, U.S. DEP'T OF JUST. (Sep. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators (referring to *The DOJ Cell-Site Simulator Policy*, U.S. DEP'T OF JUSTICE (Sep. 3, 2015), https://www.justice.gov/opa/file/767321/download).

increase accountability, "improve training and supervision," and create a more "consistent legal standard" for its use,[159] and was applicable to federal law enforcement agencies administered by the Department of Justice.[160]

With this policy, the Department of Justice desired to protect the privacy rights of individuals through careful auditing to ensure that insufficient data obtained through the use of cell-site simulators was appropriately deleted, including the content of text messages, emails, contact lists and pictures."[161] It also indicated that the new policy clarified "that cell-site simulators may not be used to collect the contents of any communication in the course of criminal investigations."[162] Despite the above, the Department of Justice still recommended that government users of cell-site technology obtain a search warrant supported by probable cause before attempting to use the technology.[163] This unequivocal assertion suggests that even the Department of Justice was aware of the potential infringement of individual constitutional rights that could occur with the use of cell-site simulation devices. However, these recommendations concerning the use of cell-site simulators have yet to be addressed by either the Supreme Court or the New York Court of Appeals.

VI. THE THIRD-PARTY DISCLOSURE DOCTRINE

A. History

With the Supreme Court narrowing the Fourth Amendment's focus and protections on whether an individual has a "legitimate expectation of privacy" in the activity in question,[164] the third-party disclosure doctrine has been a significant obstacle in a proponent's argument that cell-site information falls into a constitutionally protected category.

The most well-known case addressing the third-party disclosure doctrine for search and seizure purposes is *Lee v. United*

---

159 *Id.*

160 *Id.*

161 *Id.*

162 *Id.*

163 *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158.

164 Katz v. United States, 389 U.S. 347 (1967).

States.[165] Here, the defendant was convicted for the sale of opium based on incriminating statements that he unknowingly made to an undercover agent working for the Bureau of Narcotics.[166] While the defendant argued that evidence of his statements should be suppressed in violation of the Fourth Amendment, the Supreme Court nevertheless affirmed the defendant's conviction, holding that information given with consent and made freely available to the public was not a violation of an individual's Fourth Amendment rights.[167]

Later courts began broadening *Lee's* holding to include not only public conversations but also any combination of acts that were purposefully made public.[168] These cases stood for the proposition that "when a person reveals some information to a third party, they assume the risk that the third party may disclose it to the Government."[169] Therefore, no individual could validly allege a violation of his Fourth Amendment rights in the government's obtainment of any information that he willingly made public.

However, the concept of assuming all risk during voluntary relinquishment of information became, and remains, cloudier when considering intangible information, such as cell-site data. Any cell-phone user can recall signing a rather lengthy carrier contract when initiating service, often filled with legal jargon and endless terms, representations, and warranties; however, few, if any, can remember the terms to which they signed.[170] Instead, one usually only recalls that the provided terms must be agreed to before the carrier provides the

---

[165] Lee v. United States, 343 U.S. 747 (1952).

[166] *Id.* at 749.

[167] *Id.* at 750-52 (indicating that the information obtained from the defendant was given freely with his consent).

[168] Browne, *supra* note 2, at 86 (indicating that voluntary relinquishment of an expectation of privacy is exemplified in many daily activities made purposefully public, including "numbers dialed on a telephone, deposit slips handed to a bank teller, information written on the exterior of a package sent through the mail, statements made to undercover police officers, personal documents handed over to government officials, trash left for pickup by municipal employees, or academic papers turned over to professors").

[169] In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d 113, 120 (E.D.N.Y. 2011) (citing Smith v. Maryland, 442 U.S. 735, 742-46 (1979)).

[170] United States v. Graham, 796 F.3d 332, 345 (4th Cir. 2015) (indicating that "studies have shown that users of electronic communication services often do not read or understand their providers' privacy policies.").

user with service.[171] Few really ever consider what "providing the user with service" truly means.[172] While it does mean that the user has accessibility to his address book, his social calendar, and the worldwide web at the push of a button, it also means that the user is allowing the carrier to be the third-party receiver for all incoming and outgoing cellular data.[173]

Therefore, by using the cellular phone and agreeing to the carrier's terms, a user is voluntarily conveying his cellular information, including location, to the carrier for processing.[174] As the agreement to convey this information is usually done in a willing and purposeful manner, does the cellular user now assume all risk that his information and location may fall into the hands of the government? There has yet to be clear judicial insight as to whether the third-party disclosure doctrine would provide valid reasoning to infer than an individual's signing of a cellular phone contract causes him to voluntarily forfeit his expectation of privacy under the Fourth Amendment in instances involving cell-site simulators.

B. The Third-Party Disclosure Doctrine and Cellular Information as Interpreted by the Courts

The most notable case involving cellular information and the third-party doctrine arose from the Supreme Court's decision in *Smith v Maryland*.[175] Here, after Patricia McDonough was robbed, she began receiving threatening phone calls and visits from a man who claimed to be the robber.[176] When the police ran the license plate provided by McDonough after one of the visits, the police found out that the car belonged to defendant, Michael Lee Smith.[177] Thereafter, the police obtained a Pen/Register Order which allowed the telephone company

---

[171] Liane Cassavoy, *Before You Sign a Cell Phone Contract: What You Need to Know*, LIFEWIRE, https://www.lifewire.com/before-signing-cell-phone-contract-579606 (last updated Oct. 17, 2016).

[172] *Id.*

[173] Browne, *supra* note 2, at 65-66.

[174] *In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d at 121 (indicating that when one turns his phone on and utilizes calling and texting features, he is "voluntarily" conveying his cellular data to the third-party service carrier).

[175] Smith v. Maryland, 442 U.S. 735 (1979).

[176] *Id.* at 737.

[177] *Id.*

to record the numbers dialed from the defendant's home telephone.[178] The Register eventually revealed that calls were placed from the defendant's phone to McDonough's home.[179] Based on these findings, the police obtained a search warrant for the defendant's home, where they found a phone book flagged with McDonough's number.[180] The defendant was arrested, identified by McDonough, and indicted for robbery.[181]

The defendant submitted a pre-trial motion seeking to suppress all evidence obtained from the Pen/Register Order, claiming that the police's failure to secure a probable cause warrant violated his Fourth Amendment rights against unreasonable searches and seizures.[182] The trial court denied the defendant's motion and the appellate court affirmed the defendant's conviction.[183] Thereafter, the Supreme Court held that people had no "actual expectation of privacy" in the phone numbers they dial since all users were forced to submit the numbers to the telephone carrier in order for the calls to be completed.[184] Citing *United States v. Miller*,[185] the Court determined that the defendant "assumed the risk of disclosure" and therefore it was unreasonable for him to expect the phone numbers that he dialed to remain private.[186]

---

[178] *Id*.

[179] *Id*.

[180] *Smith*, 442 U.S. at 737.

[181] *Id*.

[182] *Id*.

[183] *Id*. at 737-38.

[184] *Id*. at 735. The court further held that:

> All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies "for the purposes of checking billing operations, detecting fraud and preventing violations of law." *United States v. New York Tel. Co.*, 434 U.S., at 174–175, 98 S.Ct., at 373. Electronic equipment is used not only to keep billing records of toll calls, but also "to keep a record of all calls dialed from a telephone which is subject to a special rate structure." *Hodge v. Mountain States Tel. & Tel. Co.*, 555 F.2d 254, 266 (CA9 1977) (concurring opinion).

Smith, 442 U.S. at 742.

[185] United States v. Miller, 425 U.S. 435 (1976).

[186] *Smith*, 442 U.S. at 744 ("This analysis dictates that petitioner can claim no legitimate expectation of privacy here. When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and "exposed" that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed. The switching equipment that

Though not specifically discussing location tracking, the Court's ruling expanded the concept of the third-party disclosure doctrine to telephone devices.[187]

In *State v. Andrews*,[188] the Court of Special Appeals in Maryland was asked to decide whether a cell phone could be turned into a "real-time tracking device by the government without a warrant" in light of the State's argument that the third-party doctrine prevented the defendant from proclaiming a Fourth Amendment violation.[189] Here, the Baltimore City Police Department picked up the defendant, Kerron Andrews, through the warrantless use of a cell-site simulator.[190] Specifically, the Baltimore City Police ascertained the defendant's location by using Hailstorm, a brand of cell-site simulator, which tricked the defendant's phone into providing signals that the police used to narrow his location to a specific residence in Baltimore City.[191] The Hailstorm was authorized for police use through the obtainment of a Pen/Register-Trap/Trace Order, which allowed for collection of GPS data from the defendant's cellular device.[192] The government obtained the defendant's precise location with the assistance of the defendant's cellular carrier and through the defendant's use of the email application on his phone.[193]

The Baltimore City Police Department obtained an arrest warrant and went to the defendant's residence, finding him on the couch with the targeted cell phone in his pants pocket.[194] At trial, the defendant argued that the Baltimore City Police Department's use of the cell-site simulator without a probable cause warrant constituted an unreasonable search and seizure under the Fourth Amendment, to which the Circuit Court agreed and suppressed all evidence as "fruit of the poisonous tree."[195] The State appealed to the Court of Special Appeals of Maryland,[196] which held that the use of the cell-site

processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber.").

187 *Id.* at 744-45.

188 State v. Andrews, 227 Md. App. 350 (2016).

189 *Id.* at 354, 395.

190 *Id.* at 354.

191 *Id.* at 359.

192 *Id.* at 356-57.

193 *Andrews*, 227 Md. App. at 359.

194 *Id.*

195 *Id.* at 354.

196 *Id.* at 354-55.

simulator *did* constitute an illegal search and seizure despite arguments that the defendant chose to voluntarily provide his cellular data to the public through the mere activation of his cellular phone.[197] The court further identified the government's use of cell-site simulation technology as the beginning of an "age of no privacy."[198]

Despite the State's argument that the cell-site simulator merely obtained cellular data "regularly transmitted by activated cell phones as part of their ordinary use,"[199] the court distinguished the cell-site simulator from a typical cellular phone tower in that a StingRay device *tricks* the cellular phones into transmitting data rather than just collecting data already being transmitted.[200] Accordingly, the court determined that cell phone users do not voluntarily convey this information "simply by choosing to activate and use their cell phones and to carry the devices on their person."[201] Relying on *Katz*'s holding that the Fourth Amendment applies to people and *not* places, the court concluded that people *do* have a legitimate expectation in real-time cell data, including location information.[202] As such, the court held that the Baltimore City Police Department's use of a cell-site simulator without a valid search warrant based on probable cause was a violation of the defendant's Fourth Amendment rights to be free from illegal searches and seizures.[203]

VII. THE LAW AS IT STANDS TODAY: THE FOURTH AMENDMENT AS APPLIED TO CELL-SITE SIMULATION DEVICES

A. *United States v. Rigmaiden*

In 2013, the United States Court of Appeals for the Ninth Circuit decided a case involving a cell-site simulator in *United States v. Rigmaiden*.[204] Here, the government alleged that the defendant had been using the identities of individuals (some deceased) to file

---

197 *Id.* at 392-93.

198 *Andrews*, 227 Md. App. 350 at 371-72.

199 *Id.* at 377-78.

200 *Id.* at 379.

201 *Id.* at 392 (indicating that cellular phone users do not *actively* submit their location information to their service provider).

202 *Id.* at 355.

203 *Andrews*, 227 Md. App. at 355-56.

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

fraudulent tax returns through the Internal Revenue Service ("IRS") website, enabling him to claim more than $3,000,000 in tax refunds.[205] In moving to suppress evidence against him, the defendant claimed that the process used by the IRS in obtaining his identification and location violated his Fourth Amendment rights against unreasonable search and seizure.[206]

Specifically, in 2007, the IRS subpoenaed subscriber information for the internet addresses that the defendant used to file the allegedly fraudulent returns, discovering that the address was associated with a Verizon wireless Internet card owned by someone named Travis Rupard.[207] In 2008, the IRS Fraud Detention Center identified a large number of potentially fraudulent tax filings that required refunds to be sent to different debit cards all associated with the same bank account.[208] After doing further research, the IRS Fraud Detention Center found that the accounts were maintained by the same Travis Rupard, though it suspected that this was a false identity as the address and driver's license number associated with the account belonged to a female by a different name.[209]

The IRS pursued further investigations of this individual, eventually coming across an e-mail exchange between Rupard and a co-conspirator wherein Rupard had requested that the co-conspirator establish a bank account for his fraudulent tax filings.[210] The government also obtained transaction logs from Verizon in connection with the use of the defendant's wireless Internet card.[211] Combining this information with the email correspondence, the IRS was able to identify that the defendant, using the alias "Travis Rupard," was the actual owner of the wireless card.[212] The IRS was thus able to synthesize these facts to determine that the location of the wireless card would lead them right to the defendant.[213] The police obtained cell-site records from the network carrier connected with the Internet card, Verizon Wireless, and discovered that the Internet card was being used

---

[205] *Id.* at *1.
[206] *Id.* at *4.
[207] *Id.* at *1.
[208] *Id.*
[209] *Rigmaiden*, 2013 WL 1932800 at ***1**.
[210] *Id.* at *2.
[211] *Id.*
[212] *Id.*
[213] *Id.*

regularly between the same towers around Santa Clara, California.[214] Wanting the defendant's location, the police manipulated cell towers until they were able to determine a point within an area of just one-quarter mile of his location.[215]

Thereafter, the police obtained an order from the court that authorized the installation of a cell-site tracking device via a Pen/Register and Trap/Trace Order.[216] Upon further use of this device, the police tracked the use of the Internet card directly to the specific apartment where the defendant lived.[217] The police then verified that the apartment belonged to the defendant and obtained a search warrant of the apartment, leading to the defendant's arrest.[218] The defendant was indicted on 74 counts of mail and wire fraud, after which he made a motion to suppress any information obtained by the police through the use of the cell-site simulator, arguing that the collected information was outside the scope of the warrant obtained by the police.[219]

The Ninth Circuit ultimately found that the defendant did *not* have a reasonable expectation of privacy in either the Internet card, his laptop, or his apartment.[220] As the defendant had obtained the Internet card and laptop fraudulently and used the Internet card and laptop solely for fraudulent purposes, the Ninth Circuit held that the defendant could not have a reasonable expectation of privacy in such use.[221] Although the defendant may have had a "thoroughly justified subjective expectation of privacy" in his use of the equipment, the court determined that it was "not one which the law recognizes as legitimate."[222] Further, the court determined that the defendant's presence in the apartment was also wrongful because it was fraudulently registered under the name of a deceased individual.[223] Therefore, the court determined that the defendant also had no legitimate expectation of privacy in the apartment.[224]

---

214 *Rigmaiden*, 2013 WL 1932800 at *3.

215 *Id.*

216 *Id.*

217 *Id.*

218 *Id.*

219 *Rigmaiden*, 2013 WL 1932800 at *1.

220 *Id.* at *5.

221 *Id.*

222 *Id.* at *6 (relying on *Rakas v. Illinois*, 429 U.S. 128, 143 n.12 (1978)).

223 *Id.*

224 *Rigmaiden*, 2013 WL 1932800 at *6 ("One who so thoroughly immerses himself in layers of false identities should not later be heard to argue that society must recognize as legitimate his expectation of privacy in the location and implements of his fraud.").

In sum, the Ninth Circuit held that given the "totality of the unique circumstances," the defendant lacked an "objectively reasonable expectation of privacy" and that "[a]s a result, no Fourth Amendment violation occurred when the government searched for and located the [Internet card] in his apartment."[225] Nonetheless, since the defendant had no legitimate expectation of privacy in this case, the court never addressed whether the cell-site simulation device was properly used and authorized.

In 2016, the United States District Court for the Southern District of New York decided a similar issue in *United States v. Lambis*.[226] Here, the DEA was authorized, under a Pen/Register warrant, to obtain cell-site data to determine the defendant's location on suspicion that he was part of an international drug-trafficking scheme.[227] Through the use of pen register technology, the DEA was able to narrow the defendant's location to "the Washington Heights area by 177th and Broadway" but was unable to identify an apartment building or apartment number.[228] Therefore, the DEA arranged for an agent to physically carry a portable StingRay device, which simulated nearby cell towers and forced surrounding cellular phones to transmit location information, around the identified Washington Heights area.[229] By using the StingRay machine, the agent was able to identify the apartment building where the defendant was located, and was further able to locate the defendant's specific apartment number after walking up and down the halls with the device until he found the location where "the signal was strongest."[230]

After identifying that the apartment belonged to the defendant, the DEA obtained consent to search the defendant's bedroom and recovered evidence that led to his arrest.[231] The defendant moved to suppress all evidence found in his apartment on the basis, similar to the holding in *Kyllo v. United States*,[232] that the use of the cell-site simulator constituted an unreasonable search of the interior of his

---

225 *Id.* at *9.

226 United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016).

227 *Id.* at 608.

228 *Id.* at 609.

229 *Id.*

230 *Id.*

231 *Lambis*, 297 F. Supp. 3d at 609.

232 Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that it was a Fourth Amendment violation to reveal "details of the home that would previously have been unknowable without physical intrusion").

home and surveilled activities that were not purposefully made public.[233] Contrarily, the government argued that its use of the StingRay machine was authorized under the original Pen/Register warrant and therefore did not constitute a violation of the defendant's constitutional rights.[234]

The Southern District of New York ultimately held that the use of the StingRay technology to determine the defendant's precise location was not contemplated in the approval of the original warrant application and was therefore outside of its scope.[235] Even though the government argued that it had sufficient probable cause at the time that the StingRay machine was used, the court determined that the government's belief was not sufficient because it was required under the Fourth Amendment to obtain such a warrant from a magistrate *prior* to conducting the search, not *after*.[236] The court supported its determination with evidence that internal policies issued by the Department of Justice required the government to obtain a valid search warrant prior to the use of cell-site simulation technology.[237] Given the court's emphasis on the inherent intrusiveness of the StingRay devices,[238] as well as the indication that the minimal requirements needed to establish a Pen/Register warrant were insufficient in this case,[239] *Lambis* suggests that probable cause must be established in order to authorize use of these highly-intrusive cell-site simulation devices.[240]

VIII. ANALYSIS: PROBABLE CAUSE IS THE APPROPRIATE STANDARD FOR THE USE OF CELL-SITE SIMULATION TECHNOLOGY

With no definitive consensus as to whether the government's use of StingRay machines and other types of cell-site simulators violates an individual's Fourth Amendment rights against unreasonable searches and seizures without a probable cause warrant,

---

233 *Lambis*, 297 F. Supp. 3d at 610.

234 *Id.* at 611.

235 *Id.*

236 *Id.*

237 *Id.*

238 The court finds a cell-site simulation search to be much more "intrusive than a canine sniff," for example. *Lambis*, 297 F. Supp. 3d at 610.

239 *Id.* at 611.

240 *Id.*

the current state of the law has allowed the government to use these highly-intrusive devices with minimal boundaries.[241] However, given that the courts have previously expressed concern over a privacy-less society,[242] and the fact that individuals have an expectation and belief that the government is not going to track their location and cellular data without their consent,[243] it is likely that the Supreme Court would hold that the government is not authorized to utilize these highly invasive and machines without a showing of probable cause.

The Department of Justice has already recommended that the use of cell-site technology, including cell-site simulators, be authorized only with sufficient probable cause.[244] As discussed *supra* in Section V, the Department of Justice, concerned by the Fourth Amendment implications of cell-site simulators,[245] has stated that the government's application for the use of a cell-site simulator should include the specifics of the technology to be used, the possibility that the retrieval of information from a target phone could disrupt other cellular devices in the area, and how that specific government agency plans to ensure that the data collected will no longer be accessible during future uses of the technology.[246] As such, the proverbial red flag has clearly been waived. For the Department of Justice to issue a department-wide policy concerning the use of cell-site simulation technology, its reservations concerning the potential constitutional infringement that such technology can cause must be relatively strong.[247] Following suit, the Supreme Court is also likely to see how threatening this technology can be to the Fourth Amendment protections.

---

[241] Pell & Soghoian, *supra* note 19, at 35 (indicating that there is a "dearth of judicial analysis" on the topic of cell-site simulators and the collection of cell-site data by the government despite the use of "cellular surveillance devices for more than twenty years").

[242] *See, e.g.*, United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring).

[243] D'Amico, *supra* note 127, at 1279-80.

[244] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158.

[245] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158.

[246] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158.

[247] *See* United States v. Lambis, 197 F. Supp. 3d 606, 611 (S.D.N.Y. 2016) (indicating that the Department of Justice's enhanced policy was based on its own recognition that it "may not turn a citizen's cell phone into a tracking device").

Since StingRay machines and other cell-site simulators have a unique ability and inadvertent likelihood that they will penetrate the area at the very core of the Fourth Amendment, the four walls of the home, common law precedent requires that a probable cause warrant be issued prior to its use.[248] For example, in *Andrews*, the police, after tracing the defendant's phone, found the defendant sitting on his couch with his cellular phone in his pocket.[249] Clearly, the use of the StingRay machine in that case penetrated the interior of the home and should, according to *Kyllo*, automatically constitute an unreasonable search under the Fourth Amendment.[250] However, even when cell-site simulators do not track an individual's precise location to an area within the four walls of his home, the Court in *Jones* has suggested that the use of cell-site simulators without a sufficient probable cause warrant can still classify as an unreasonable intrusion into the private life of an individual because lengthy surveillance monitoring can provide intimate details about a person's "familial, political, professional, religious, and sexual associations . . . ."[251]

One of the most important functions of the cell-site simulator is also its biggest problem. Cell-site simulators obtain not only location and registration information from the targeted cellular phone user, but also incidental information from third-party devices using the same cell network and towers.[252] Even the Department of Justice acknowledged this flaw as recently as 2015, when it promised to audit the type and amount of information collected when utilizing cell-site

---

[248] *See generally In Support of a Warrant Requirement for the Use of StingRays*, *supra* note 16.

[249] State v. Andrews, 227 Md. App. 350, 359 (2016).

[250] Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that obtaining "details of the home that would previously have been unknowable without physical intrusion" constitutes a search under the Fourth Amendment that requires a probable cause warrant).

[251] United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring); *see also* People v. Weaver, 12 N.Y.3d 433, 441-42 (2009) (indicating that location monitoring could reveals acts of "indisputably private nature" such as "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDs treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, [and] the gay bar").

[252] *Memorandum: Warrant Requirement for the Use of Stingrays in New York*, N.Y. CIV. LIBERTIES UNION 5 (Aug. 2015), https://www.nyclu.org/sites/default/files/memo_stingrayuse_NY_201508_final.pdf (indicating that reports show that even when personal information is not obtained from unintended users through the use of a cell-site simulator, use of the machine can still interfere with others' cell phone service, downgrading their service connectivity from 3G or 4G to 2G).

simulators department-wide.[253] However, while promises may be made, there is no actual way to prevent the collection of this extraneous data, considering that the cell-site simulators force the targeted phone and surrounding phones to disclose such information.[254] The mere fact that such an overbreadth of information can be received and reviewed by the government without the knowledge of the cellular user is certainly an infringement on that individual's constitutional rights because few, if any, individuals actively submit this information for public use.[255] Therefore, to allow such information to be obtained without at least a demonstration of probable cause would be unconstitutional because it would not adequately safeguard an individual's Fourth Amendment rights.[256]

With regard to how the third-party doctrine applies to the use of cell-site simulators, *Andrews* and *Lambis* provide the most logical explanations. Cell-site simulators do not simply intercept data being conveyed through a cellular device to a corresponding carrier's cell tower; instead, they *force* the phone to send communications that it may not otherwise emit for the sole purpose of intercepting those communications, interpreting the data, and pinpointing the exact location of the user.[257] Though many individuals today understand that their cellular data can be incidentally intercepted by virtue of the unique way in which cellular devices function, they most certainly do not have an expectation that the government may hack their phones to determine their almost precise location.[258] Generally, third-party carriers are able to provide some "push-back" to any government

---

[253] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158.

[254] Browne, *supra* note 2, at 86 (indicating that "[n]o affirmative action is required for cell phone users to convey their CSLI to a cell phone service provider").

[255] United States v. Lambis, 197 F. Supp. 3d 606, 615 (S.D.N.Y. 2016) (indicating that cell-site data being transmitted to cell-site simulators has a "layer of involuntariness" as they are "not transmitted in the normal course of the phone's operation" but are forced by the cell-site technology to "transmit their unique identifying electronic serial numbers"); Browne, *supra* note 2, at 86.

[256] Browne, *supra* note 2, at 71-72 ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."). Interestingly, this source has failed to identify what "withdrawing from public view" entails and whether or not an affirmative act is required for "withdrawal" from public view to take place.

[257] Proposed Brief Amicus Curiae, *supra* note 65, at 8, 10.

[258] *Memorandum: Warrant Requirement for the Use of Stingrays in New York*, *supra* note 252, at 2 (indicating that cell phone owners do not ever believe that their phone is "connecting with . . . a law enforcement device").

attempts at invalid intrusions; however, given that Stingrays and other cell-site devices are able to bypass third-party authorizations and still obtain location information without leaving behind any virtual footprints,[259] it can be argued that this is not a right that anyone could unequivocally forfeit absent knowledge about basic cell-site simulator functionality.

Furthermore, as cell-site simulators respond to the basic functionality of cellular devices in obtaining their information,[260] the individual never affirmatively acts to convey the information to the carrier.[261] This contrasts greatly with the cases in which the courts have determined the third-party disclosure doctrine to be a bar against privacy expectations in information purposefully made public.[262] Unless the potential risks of government interference are clearly explained to an individual prior to his or her agreement to use a cellular device, it is unclear whether that individual voluntarily and knowingly waived his right to privacy under the third-party disclosure doctrine.[263] Understanding such, it is clear that individuals *do* have an expectation of privacy in their cellular location, and since the Constitution prohibits such unreasonable and intrusive searches under the Fourth Amendment, the most likely outcome is that the Supreme Court will require that probable cause be established before the government can utilize a cell-site simulator. Given that probable cause requires at least a fair probability that a search will be successful in obtaining the

---

[259] Pell & Soghoian, *supra* note 21, at 147.

[260] As documented *supra*, cell-site simulators obtain their information from the registration processes performed by cellular devices every seven seconds. *Electronic Surveillance Manual*, *supra* note 36, at 178-79 n.41.

[261] Browne, *supra* note 2, at 86.

[262] *See* Browne, *supra* note 2, at 86 (indicating that voluntary relinquishment of an expectation of privacy was exemplified in many daily activities made purposefully public, including "numbers dialed on a telephone, deposit slips handed to a bank teller, information written on the exterior of a package sent through the mail, statements made to undercover police officers, personal documents handed over to government officials, trash left for pickup by municipal employees, or academic papers turned over to professors").

[263] Browne, *supra* note 2, at 86-87 ("Oblique mention in a statement of terms and conditions or user agreement for cell phone service that the service provider might share certain information with the government when required to do so does not change this result. Every rational presumption is indulged against waiver of fundamental constitutional rights; unless a cell phone user receives a clear, explicit, and conspicuous explanation that use of their phone result in their location and movements being warrantlessly monitored, he should not be presumed to waive his Fourth Amendment rights when his cell phone is turned on. Warnings of similar prominence have been required in agreements that purport to waive other constitutional and contractual rights.").

information that it seeks,[264] rather than a finding that the search is merely relevant to the investigation,[265] the probable cause standard provides the greatest guarantee of protection for individuals that the Fourth Amendment sought to preserve.

While the government may put forth arguments of the invaluable services that cell-site simulators provide, including assistance in locating wanted, and often quite dangerous, criminals,[266] it should be noted that the need for a higher quantum of proof for the authorization of cell-site simulators does not seek to demote the invaluable assistance that these devices could provide if properly authorized. Cell-site simulators can still provide instrumental information to federal agencies and local police departments to assist in their obtainment of justice; however, the ability to use this highly technical equipment should not be based on the mere certification of a government agent that the information to be obtained is relevant.[267] Instead, the sheer invasiveness of cell-site simulation technology into the private lives of its subjects should require an establishment of sufficient probable cause for its use.[268] Moreover, while some agencies, such as the Securities Exchange Commission, may rely on the minimum burden of proof that they need to demonstrate in order to obtain cellular and other electronic data,[269] the fact "that this is the way it had always been done" is simply not a justifiable argument when it comes to the infringement of an individual's constitutional rights.

Moreover, while some agencies may fear that a required showing of probable cause *prior* to the use of cell-site simulation technology can obstruct justice,[270] this requirement is not exempt from

---

[264] U.S. v. Grubbs, 547 U.S. 90, 95 (2006) (quoting Illinois v. Gates, 462 U.S. 213, 238 (1983)).

[265] *See* 18 U.S.C. § 3122(b) (2012) (listing the criteria for application of a Pen/Register Order).

[266] *In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Telephone, 460 F. Supp. 2d 448, 451-52 (S.D.N.Y. 2006).

[267] *See* 18 U.S.C. § 3122(b) (2012) (listing the criteria for application of a Pen/Register Order).

[268] Browne, *supra* note 2, at 84-85.

[269] Thompson II & Cole, *supra* note 127, at 1.

[270] StingRay technology has been described by federal officials as the way it "track[s] dangerous criminals . . . find[s] killers . . . find[s] kidnappers . . . find[s] drug dealers . . . [and] find[s] missing children . . . ." Brad Heath, *Police Secretly Track Cellphones to Solve Routine Crimes*, USA TODAY (Aug. 23, 2015), http://www.usatoday.com/story/news/2015/08/23/baltimore-police-stingray-cell-surveillance/31994181/.

certain exigencies which demand prompt attention.[271] This would not only account for the many critical situations in which time is of the essence for criminal investigations but would also allow the government to utilize this high-grade technology for assistance in obtaining necessary information during state-wide or country-wide emergencies. The waiver of the probable cause requirement in exigent circumstances could diminish the government's fear of an overall lack of control but also contemporaneously help individuals maintain their civil liberties guaranteed under the Constitution.

IX. CONCLUSION

Since its creation, the Fourth Amendment has protected an individual against unreasonable searches and seizures.[272] This protection was initially based on common-law principles of trespass, as determined in *Olmstead v. United States*, which required actual physical intrusion on private property before standing for a valid Fourth Amendment violation was found.[273] In these situations, private property was inherently determined to be an area in which one reasonably expected his activities to remain private.[274] However, with the emergence of new technology, the Supreme Court was forced to address many situations in which an individual's Fourth Amendment rights could be implicated without the occurrence of physical trespass.[275] This caused the Court to shift its reliance from places to people when determining Fourth Amendment claims.[276] The Court has since broadened Fourth Amendment protections in all situations where there exists a reasonable expectation of privacy.[277]

Yet, with the development of advanced surveillance technology, individuals' specific expectations of privacy have been

---

[271] Coolidge v. New Hampshire, 403 U.S. 443, 454-55 (1971) (indicating that there are a "few specifically established and well delineated exceptions" to the probable cause requirement that would justify the government's failure to obtain the probable cause warrant before conducting a search).

[272] U.S. CONST. amend. VI.

[273] Olmstead v. United States, 277 U.S. 438 (1928).

[274] *Id.* at 474-75.

[275] *See, e.g.*, United States v. Jones, 565 U.S. 400 (2012); Kyllo v. United States, 533 U.S. 27 (2001); Katz v. United States, 389 U.S. 347 (1967).

[276] *See Katz*, 389 U.S. at 351.

[277] *See generally Katz*, 389 U.S. at 350-51, 359.

further called into question.[278] While the Court had previously found that no expectation of privacy could possibly exist in situations where individuals made seemingly private details public,[279] the creation of cell-site simulation technology currently used by the United States government, military agencies, and intelligence agencies[280] has turned previously private information inadvertently into public knowledge.[281] This is of particular importance when it comes to cellular telephones and similar electronic devices for the reasons discussed in this Note.

Cellular telephones function through the outward emission of radio transmission waves.[282] These waves are automatically transmitted by the electronic device, regardless of the user's knowledge and intent, as long as the cellular device remains turned on.[283] While this technology allows the user to quickly and easily make and receive telephone calls, this process also makes these radio transmissions highly susceptible to third-party interference.[284] Though this interference is generally harmless, typically coming from outside carriers that assist in providing a strong signal to the cellular user,[285] data emitted by the cellular telephone is also subject to collection by the government through the use of a cell-site simulator.[286] Like cell towers, these simulators accept incoming radio transmissions; however, they do so only by tricking nearby cellular devices into thinking that they are cellular towers.[287] Contrary to regular cell towers, these cell-site simulators are portable, box-shaped devices that the government often uses to obtain a target's precise identification information.[288] Even if an individual is not the target of the

[278] *Kyllo*, 533 U.S. at 33-34 (wherein the Court determined that technology clearly affected the application of the Fourth Amendment and a vital question within this context concerned "what limits there are upon this power of technology to shrink the realm of guaranteed privacy").

[279] *See, e.g.*, Florida v. Riley, 488 U.S. 445, 445 (1989); California v. Greenwood, 486 U.S. 35, 35 (1988); Oliver v. United States, 466 U.S. 170, 171 (1984).

[280] *Stingray Tracking Devices: Who's Got Them?*, *supra* note 69.

[281] Kerr, *supra* note 110, at 580 (indicating that "new technologies can bring " 'intimate occurrences of the home out in the open' ").

[282] Browne, *supra* note 2, at 61-62.

[283] Browne, *supra* note 2, at 62.

[284] This is based on the concept that relay signals from cell phones effectively bounce back and forth between a network of cell towers until they reach their intended destination. Browne, *supra* note 2, at 62.

[285] Browne, *supra* note 2, at 62.

[286] Pell & Soghoian, *supra* note 19, at 16-17.

[287] Owsley, *supra* note 19, at 192.

[288] Gallagher, *supra* note 51.

government's investigation, that individual's cellular location may still be collected if he or she is within range of the cell-site simulator.[289]

Despite the obvious privacy concerns that come with the functionality of cell-site simulators, the government's use of these devices has managed to evade court discretion for years.[290] While there have been some attempts to control the government's use of surveillance technology of this type, the lack of knowledge concerning the capabilities of these devices has led to inconsistent and virtually unhelpful attempts at regulation.[291] For example, the enactment of the Electronic Communications Privacy Act and the Stored Communications Act has only led to further confusion over what type of information, if any, the government should supply to the courts for authorization of the use of cell-site simulation technology. While the very provisions of these acts are inconsistent, they have been interpreted to only require certification by a government agent that the information to be obtained is relevant to a criminal investigation,[292] consistent with the requirements of a Pen/Register Order.[293] However, this rather low burden of proof fails to account for the significant impact this technology has on an individual's reasonable expectation of privacy.

The invasiveness of surveillance technology has been well-documented by the court in *Jones*, where it was found that real-time tracking of individuals inevitably leads to the publication of private details about their personal lives which may not have ever been meant to be made public.[294] Accordingly, there is a need for a higher burden of proof before such devices can be utilized by the government in order to protect the private lives of citizens. A probable cause requirement, to be decided by a neutral and detached magistrate, *prior* to the government's use of cell-site simulators is warranted for the following reasons: (1) the inherently intrusive nature of the cell-site simulator devices;[295] (2) the overbreadth of information that can be inadvertently collected by StingRay machines and other cell-site simulators;[296] (3)

---

[289] Owsley, *supra* note 19, at 185-86 (indicating that these devices obtain data from all cellular users who happen to be in the area, regardless of the government's intention).

[290] Browne, *supra* note 2, at 57.

[291] Pell & Soghoian, *supra* note 19, at 20.

[292] D'Amico, *supra* note 127, at 1272-73; Lye, *supra* note 121, at 5.

[293] 18 U.S.C. § 3122(b) (2012).

[294] United States v. Jones, 565 U.S. 400, 415-16 (2012) (Sotomayor, J., concurring).

[295] *Id*.

[296] Owsley, *supra* note 19, at 185-86.

the lack of guarantee that such information will be properly discarded after their use;[297] (4) the cellular user's lack of knowledge that such information is being transmitted and collected;[298] and (5) the inability of the user to know whether cell-site simulation technology will be used to track an individual's location within the most protected area under the Fourth Amendment—the four walls of the home.[299] The need for a well-established probable cause burden prior to the use of cell-simulation technology is supported by the Department of Justice's own internal policy enhancements,[300] and is the only way to ensure a minimum level of protection of individual privacy rights that the Fourth Amendment serves to guarantee.

---

[297] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158 (indicating the Department of Justice's own concern that data handling and destruction were a concern with the use of cell-site simulators).

[298] *See* Browne, *supra* note 2, at 86-87 (contrasting the transmission of cell-site data from a cellular telephone to a cell-site simulator with the affirmative action required to purposefully make information available to the public, such as with "information written on the exterior of a package sent through the mail" or "statements made to undercover police officers").

[299] Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

[300] *Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators*, *supra* note 158.