YOU CAN RUN, BUT YOU CAN'T HIDE: LAW ENFORCEMENT'S USE OF "STINGRAY" CELL PHONE TRACKERS AND THE FOURTH AMENDMENT*

Cody Benway**

---

* Best Student Note (2017), Southern Illinois University Law Journal.

** Cody Benway is a third-year law student at Southern Illinois University School of Law, expecting his Juris Doctor in May of 2018. He would like to thank his faculty advisor, Professor Edward Dawson, for his continued guidance and feedback throughout the writing process. He would also like to thank his friends and family for their substantial support and encouragement.

I. INTRODUCTION

Today, it is almost impossible to imagine what it would be like without cell phones being in the pocket of almost every American citizen. Cell phones have developed from a novelty, to a luxury, to a convenience, to finally being an integral and necessary part of everyday life. No longer do cell phones operate only as a phone; cell phones also operate as a computer, a calculator, a camera, a dictionary, a phone book, a vault, a map, a gaming arcade, as well as an instant source of connection to almost any other piece of information available worldwide. It is difficult to remember how life was before having an entire world available in your pocket at any moment. As the technology continues to grow and become even more fantastic, American citizens continue to place more of themselves and their personal information into these cell phones.

While people continue to put more faith and information into their cell phones, they do not always realize that with these benefits come some risks. In this digital age, a cell phone opens a person up to not only their contact list, but also to the entire world. The advance of technology has greatly expanded the government's ability to conduct surveillance outside of the public's generally watchful eyes and directly into the public's private storage of information inside their cell phones.[1]

Law enforcement officials have begun to use the connection of cell phones as a major tool in their investigations and subsequent apprehension of criminal suspects.[2] One such tool officials are using is a cell-site simulator, otherwise known as a "Stingray." This device is currently being

1. Stephanie 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 J.L. & TECH. 134, 142 (2013).
2. Howard W. Cox, *Stingray Technology and Reasonable Expectations of Privacy in the Internet of Everything*, 17 FED. SOC'Y REV. 29 (Mar. 31, 2016), http://www.fed-soc.org/publications/detail/stingray-technology-and-reasonable-expectations-of-privacy-in-the-internet-of-everything.

used by law enforcement to identify and track cell phones of criminal suspects in criminal investigations.[3] These devices, posing as cell towers, capture information relayed from a suspect's cell phone and can be used by law enforcement to track and locate the cell phone being used by the suspect.[4] As cell phones have become such a central part of citizens' lives, most individuals consistently carry and use them during most hours of the day. From this constant connection between citizen and cell phone, law enforcement's ability to track the cell phone essentially allows law enforcement to track the person attached to that cell phone.

Stingrays have raised multiple Fourth Amendment concerns about law enforcement's improper intrusion into citizens' privacy, but the courts and Congress have not yet definitively responded.[5] As cell phones continue to improve and connect to more private information in citizens' lives, it becomes necessary to create a uniform legal standard which, in the words of Justice Lewis Powell, will allow "a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment."[6] This note sets out to propose such an accommodation through the creation of a statutory standard which will govern the use of Stingrays through search warrants and exclusionary rules.

Part II of this note provides an introduction to Stingrays, their use and application by law enforcement, and the continued attempts to keep the technology as secret as possible in order to protect the techniques used by law enforcement from criminal suspects. It also provides a brief history of the Fourth Amendment and its application in modern jurisprudence and statutory law as courts enter a new era of applying constitutional protections in the digital era. It is followed by a concise summarization of current academic literature related to Stingrays and the Fourth Amendment. Finally, a detailed overview of current statutory law related to electronic surveillance as passed by Congress is presented. Part III analyzes whether the use of Stingrays conflicts with Fourth Amendment protections of privacy and how courts have attempted to balance the interests of private citizens against the investigative goals of law enforcement. Part IV offers a statutory solution that will advance the protection of citizens' electronic privacy in the form of creating a new Chapter to Title 18 that would include language related to Stingrays and require a probable cause warrant for their use under Rule 41 of the Federal Rules of Criminal Procedure. The proposed chapter is written so that it will both satisfy current Supreme Court precedent interpreting the language of the Fourth Amendment and protect law enforcement investigative goals and evidentiary collection.

---

3. *Id.* at 29.
4. *Id.* at 29–30.
5. *Id.* at 30–31.
6. Oliver v. United States, 466 U.S. 170, 181 (1984).

II. BACKGROUND

Since at least 1995, law enforcement officials at the local, state, and federal level have been using Stingray cell phone trackers as part of their criminal investigations to locate, track, and apprehend criminal suspects.[7] However, law enforcement has taken great steps to ensure that these devices remain as secret as possible.[8] Because of this secrecy, Congress and the courts have been unable to fully understand and appreciate these devices and how they might infringe on American citizens' protections against unreasonable searches and seizures under the Fourth Amendment.[9] Even in the past few years, courts have shown difficulty in understanding these devices and have not been able to apply a consistent legal standard to their application for use in the field or as evidence in subsequent criminal proceedings.[10] As the Supreme Court continues to wrestle with advancing technology and its use by law enforcement, at least one Justice has suggested Congress may be in a better position to confront these challenges first.[11] In order to advance that position, it becomes necessary to not only understand what Stingrays actually are, but how history and current studies and rules can provide an effective starting point for a new regulatory scheme related to Stingrays.

This Part will first outline Stingrays and their operation, as currently known by the public. It will be followed by an overview of applicable Fourth Amendment law and how the Supreme Court's interpretation of the Fourth Amendment to protect American citizens from unreasonable searches and seizures. Next, it will survey the current academic literature analyzing Stingrays under the Fourth Amendment. Finally, it will review current statutory law related to electronic surveillance as provided by Congress.

---

7. LINDA LYE, AM. CIV. L. UNION, STINGRAYS: THE MOST COMMON SURVEILLANCE TOOL THE GOVERNMENT WON'T TELL YOU ABOUT 1 (2014), https://www.aclunc.org/publications/stingrays-most-common-surveillance-tool-government-wont-tell-you-about.
8. Cox, *supra* note 2, at 29.
9. *Id.*
10. *See generally* United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012) (relying primarily on information presented during an *ex parte* hearing with law enforcement officials about the involved Stingray without citing any additional sources to support the technical information relayed during the hearing); *In re* Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 U.S. Dist. LEXIS 151811 at *2, *10 (N.D. Ill. 2015) (expressing displeasure at both the lack of both available information on Stingrays and the lack of judicially-manageable standards to apply towards a Stingray warrant).
11. Kyllo v. United States, 533 U.S. 27, 51 (2001) (Stevens, J., dissenting) ("It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints.).

A. Stingrays: What They Are and How They Work

A Stingray, at its most basic definition, is a cell-site simulator that operates as a "mock" cell tower by intercepting cell phone signals and collecting certain information from the cell phones that are intercepted.[12] Stingrays are generally about the size of a suitcase and can be used by law enforcement agents to track a suspect's cell phone to a precise location.[13] Since cell phones continuously connect to cell towers, even when not being used, Stingrays can constantly collect information from cell phones within their range.[14]

By acting as a cell tower, Stingrays can "trick" all cell phones within range into connecting to the device, which will allow investigators to gather certain information and data related to the connecting cell phones.[15] These devices also do not allow a cell phone within range to opt-out of transmitting to the Stingray.[16] All cell phones within range are forced into connecting to the device since it operates as a cell tower with the strongest signal that is closest to the cell phone.[17] The data collected can include the unique serial numbers of the cell phones; the unique phone number associated with the phones; any information related to calls placed or received, including date, time, and duration of the calls; and location information.[18] When configured this way, a Stingray works most similarly to a pen register[19] or a trap and trace device.[20]

The Stingray manufacturer's price list revealed Stingrays can be configured to also intercept the actual content of calls, real-time text

12. Cox, *supra* note 2, at 29–30.
13. Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, WIRED (Oct. 28, 2015, 3:00 PM), https://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/; LYE, *supra* note 7, at 3 (describing testimony by Florida police officers that they used "portable equipment" and went to "every door and every window" in a large apartment complex in order to locate the suspect).
14. Zetter, *supra* note 13.
15. *See* Pell & Soghoian, *supra* note 1, at 145.
16. *See* LYE, *supra* note 7, at 3–4.
17. *See id.*
18. *See* Cox, *supra* note 2; Pell & Soghoian, *supra* note 1, at 146.
19. 18 U.S.C. § 3127(3) (2012) (defining "pen register"); *See also* United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n. 1 (1977); *Pen Register*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/pen_register (last visited Oct. 16, 2016) ("A device or process that traces outgoing signals from a specific phone or computer to their destination. Often used by law enforcement as the advanced counterpart of an outgoing call log. A pen register produces a list of the phone numbers or Internet addresses contacted, but does not include substantive information transmitted by the signals").
20. 18 U.S.C. § 3127(4) (defining "trap and trace" device); *See also Trap and Trace Device*, LEGAL INFO. INST., https://www.law.cornell.edu/wex/trap_and_trace_device (last visited Oct. 16, 2016) ("A device or process that records the sources of incoming signals to a specific phone or computer. Often used by law enforcement as the advanced counterpart of Caller ID. A trap and trace device identifies the phone numbers or Internet addresses of incoming signals, but does not include substantive information transmitted by those signals").

messaging, and Internet web pages visited through the intercepted cell phones.[21] All interceptions are done in a way that would make the Stingray operate as if it were being used under a Title III wiretap operation.[22] However, law enforcement agencies have said their Stingrays are not configured to operate in that manner and do not collect actual telephone conversations or text messages.[23]

Through the collection of data from the intercepted cell phones, law enforcement can use the data to locate and target a suspect's specific cell phone and use that information to locate and track the cell phone.[24] Stingrays are able to produce extremely accurate location information about the target's cell phone.[25] For example, in one case where the police were tracking a suspect's cell phone, a subsequent police report indicated the suspect was found only two meters away from where the Stingray indicated the suspect would be.[26] Law enforcement agencies have noted in other cases that Stingrays were used to find suspects in specific apartments within multi-unit buildings.[27]

Stingrays are currently owned and operated by law enforcement agencies at the local, state, and federal levels.[28] There are seventy-two agencies in states and the District of Columbia that possess Stingrays,[29] as well as other foreign countries, including Canada.[30] Federal agencies using them include the Federal Bureau of Investigation; Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms, and Explosives; Immigration and Customs Enforcement; Internal Revenue Service; National Security Agency; Secret Service; US Marshals Service; and most branches of the US military.[31] There are also multiple local and state law enforcement agencies that currently have access to this technology.[32] However, because of the attempts by law enforcement to conceal the use and operation of Stingrays, it is unknown whether even more agencies actually have them at their disposal.[33]

---

21. Pell & Soghoian, *supra* note 1 at 146.
22. *See* 18 U.S.C. § 2518.
23. *See* Zetter, *supra* note 13.
24. *Id.*
25. *See* LYE, *supra* note 7, at 3.
26. *Id.*
27. *Id.*
28. *Stingray Tracking Devices: Who's Got Them?*, ACLU, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them#agencies (last visited Oct. 15, 2016).
29. *Id.*
30. Shane Dingman, *Tracking Our Phones: How StingRay Devices are Being Used by Police*, THE GLOBE AND MAIL (Mar. 21, 2016), http://www.theglobeandmail.com/technology/tracking-our-phones-how-stingray-devices-are-being-used-by-police/article29322747/.
31. ACLU, *supra* note 28.
32. *Id.*
33. *Id.*

Indeed, even with all the information presented about what Stingrays are and what they can do, there is still a great amount of information unknown by the general public about these devices because of law enforcement's attempts to conceal this technology.[34] The FBI has imposed strict regulations and rules about the disclosure of Stingrays in applications for warrants or for use during court proceedings.[35]

Agencies are even required to sign non-disclosure forms with the FBI and the Harris Corporation, the company that makes Stingrays, that forbid agencies from discussing the device, the operation of the device, or any associated documents or forms related to the device in any court proceeding, legal memorandum, discovery request, or other related documents without prior approval from the FBI.[36] The forms even go so far as to allow the FBI to request a reduction or dismissal of any pending charges if the court were to require that information about Stingrays be disclosed.[37] Apart from secrecy in court proceedings, law enforcement agencies are also barred from disclosing materials pursuant to any FOIA requests or judicial inquiries.[38]

B. Supreme Court Precedent: The Fourth Amendment and Electronic Surveillance

1. Fundamental Fourth Amendment Doctrine

The Fourth Amendment of the United States Constitution protects citizens from unreasonable governmental searches and seizures.[39] The full text of the Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,

---

34. *See* Cox, *supra* note 2, at 31–32.
35. *Id.* at 31.
36. *Id.*
37. *See id.* at 31–32; Mike Opelka, *At Least 23 States Now Employ 'Stingray' Technology Allowing Police to Grab Your Cell Phone Data, Text Messages and More Without a Warrant*, THE BLAZE (Feb. 25, 2016, 12:42 PM), http://www.theblaze.com/stories/2016/02/25/at-least-23-states-now-employ-stingray-technology-allowing-police-to-grab-your-cell-phone-data-text-messages-and-more-without-a-warrant/.
38. Abby Simmons, *BCA Agreed to FBI Terms on Secret Cellphone Tracking*, STAR TRIB. (Dec. 5, 2014, 11:02 PM), http://www.startribune.com/bca-agreed-to-fbi-terms-on-secret-cellphone-tracking/284945781/. (The FBI required in the non-disclosure form that "[a]ny court orders directing the BCA to reveal information about Harris Corp. 'will immediately be provided to the FBI in order to allow sufficient time for the FBI to intervene to protect the equipment/technology and information from disclosure and potential compromise.'")
39. U.S. CONST. amend. IV.; *What Does the Fourth Amendment Mean?*, U.S. COURTS, http://www.uscourts.gov/about-federal-courts/educational-resources/about-educational-outreach/activity-resources/what-does-0 (last visited Oct. 16, 2016).

> 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.[40]

Courts analyze the right to protection from unreasonable governmental searches and seizures as a balancing test of two competing interests: the necessity of intrusion for legitimate government interests versus the necessary protections of a person's reasonable expectation of privacy and from unreasonable searches and seizures.[41]

Over the years, the Supreme Court has shifted the way it analyzes the Fourth Amendment. As the following sections will discuss, what the Court once found to be a singular common law property-based test[42] has now shifted to include both the common law property-based test and a "reasonable expectation of privacy" test.[43] In the electronic surveillance age, the Supreme Court has been forced to apply pre-digital era legal tests and standards to cases that may not necessarily fit within those narrow bounds. However, as at least one Justice has noticed, these pre-digital legal tests do not fit with the advancement of modern technology.[44]

2. 20th Century Electronic Surveillance and Fourth Amendment Precedent

In the beginning of the electronic surveillance cases, the Supreme Court followed its long-held approach of analysis under a common-law property based test to determine when evidence collection constituted a search.[45] When the facts showed a physical trespass, the Court concluded that a search under the Fourth Amendment occurred when "unauthorized physical penetration into the premises occupied" by individuals resulted in the monitoring of their private conversations.[46]

However, throughout the 20th century, the Court began to move away from the singular common-law property based test. Beginning with *Katz v. United States*, the Court began to move away from the singular common-law property based test towards the "reasonable expectation of privacy" test.[47]

---

40. U.S. CONST. amend. IV.
41. U.S. COURTS, *supra* note 39.
42. Kyllo v. United States, 533 U.S. 27, 31 (2001).
43. United States v. Jones, 565 U.S. 400, 404–07 (2012).
44. *Kyllo*, 533 U.S. at 51 (Stevens, J., dissenting).
45. *Jones*, 565 U.S. at 421 (Alito, J., concurring).
46. Silverman v. United States, 365 U.S. 505, 509 (1961).
47. Katz v. United States, 389 U.S. 347 (1967).

a. The *Olmstead*, *Silverman*, and *Goldman* Era

In *Silverman v. United States*, the facts showed police officers listened to conversations between the defendants through a "spike mike" that had been attached to a heating duct that ran through the wall of the house.[48] The Court held this constituted a search because the "spike mike" had made contact with the heating duct, which was part of the physical premises of the house and thus constituted a physical trespass on the house by law enforcement officials.[49]

The analysis did not change when law enforcement gathered evidence without having a physical trespass onto private property, but the overall result was the exact opposite; the Court found no search had occurred.[50] In *Olmstead v. United States*, police officers gathered evidence of conversations between the defendants by intercepting messages from house lines that were on nearby street.[51] No physical trespass of the defendants' house occurred when the messages were intercepted.[52] The Court held that because no physical trespass occurred when law enforcement intercepted the conversations, the Fourth Amendment did not apply and afforded no protections.[53] The Court reached a similar conclusion in *Goldman v. United States*.[54] In *Goldman*, law enforcement agents overheard a conversation by placing a "detectaphone" on the outer wall of an office in order to hear inside.[55] Again, the Court found that since no physical trespass had occurred, there was no violation of the Fourth Amendment.[56]

The trespass and common law property-based rule was deeply criticized in the above cases.[57] Both concurring and dissenting Justices found in each of the above cases that it should not matter whether a physical trespass had occurred, but only that private conversations had been picked up by unreasonable intrusion by law enforcement officials.[58] Picking up on these

48. *Id.* at 506.
49. *Id.* at 511.
50. *Jones*, 565 U.S. at 421 (Alito, J., concurring).
51. Olmstead v. United States, 277 U.S. 438, 456–57 (1928).
52. *Id.* at 457.
53. *Id.* at 466. ("The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment. Here those who intercepted the projected voices were not in the house of either party to the conversation.").
54. Goldman v. United States, 316 U.S. 129 (1942).
55. *Id.* at 131–32.
56. *Id.* at 135.
57. United States v. Jones, 565 U.S. 400, 422 (2012) (Alito, J., concurring).
58. *See Olmstead*, 277 U.S. at 479 (Brandeis, J., dissenting) ("It is, of course, immaterial where the physical connection with the telephone wires leading into the defendants' premises was made. And it is also immaterial that the intrusion was in aid of law enforcement. Experience should teach us to be most on our guard to protect liberty when the Government's purposes are beneficent. Men

cues, not long after the Court heard and decided the *Silverman* case, a new case would emerge that would entirely change the face of the Fourth Amendment, its application to law enforcement, and the way the Court conducted its Fourth Amendment analysis.

b. *Katz v. United States*

Katz is a monumental case that did away with the single trespass-based analysis of the Fourth Amendment and introduced the new standard of a "reasonable expectation of privacy".[59] In *Katz*, police officers attached an electronic listening device to the outside of a telephone booth where the defendant was making calls to transfer illegal wagering information.[60] In writing for the majority, Justice Stewart noted that while *Olmstead* and *Goldman* had previously held the Fourth Amendment would not apply in the absence of penetration into a private residence, "the premise that property interests control the right of the Government to search and seize has been discredited"[61] and that "…the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[62] The Court ultimately found that law enforcement had violated the defendant's expectation of privacy within the telephone booth because they had failed to secure a warrant within the guidelines proscribed by the Fourth Amendment, and therefore reversed the judgment of the lower court that found the defendant guilty.[63]

While Justice Stewart's opinion creates the "reasonable expectation of privacy" test for whether governmental intrusion goes beyond the scope of the Court's previous trespass-based decisions, it is Justice Harlan's concurring opinion that creates the two-prong test that is most often quoted by courts. The two-prong test requires (1) "a person have exhibited an actual

---

born to freedom are naturally alert to repel invasion of their liberty by evil-minded rulers. The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding"); *see also*, Silverman v. United States, 365 U.S. 505, 513 (Douglas, J., concurring) ("The concept of 'an unauthorized physical penetration into the premises,' on which the present decision rests, seems to me to be beside the point. Was not the wrong . . . done when the intimacies of the home were tapped, recorded, or revealed? The depth of the penetration of the electronic device—even the degree of its remoteness from the inside of the house—is not the measure of the injury"); *Goldman*, 316 U.S. at 139 (Murphy, J., dissenting) ("But the search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment. Surely the spirit motivating the framers of that Amendment would abhor these new devices no less. Physical entry may be wholly immaterial").

59. Katz v. United States, 389 U.S. 347 (1967).
60. *Id.* at 348.
61. *Id.* at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)).
62. *Id.* at 353.
63. *Id.* at 359.

(subjective) expectation of privacy," and (2) "that the expectation be one that society is prepared to recognize as 'reasonable.'"[64] If both elements are met, it appears Justice Harlan would argue the person would be afforded the protections under the Fourth Amendment from unreasonable searches and seizures, i.e. without a warrant.[65]

Additionally, Justice Harlan acknowledged that in a situation where a reasonable expectation of privacy may exist, the ability to search is not removed, but only the expectation of privacy can be superseded by a warrant or a warrant exception when there is a legitimate need for law enforcement intrusion.[66]

c. *Smith v. Maryland*

While Justice Harlan initially developed the two-prong privacy test in his concurrence in *Katz*, the Court fully adopted it a little over ten years later in *Smith v. Maryland*.[67] In *Smith*, law enforcement installed a pen register to record phone numbers dialed from the telephone of a robbery suspect's phone in order to determine whether he suspect was the individual that subsequently called the victim's phone number to threaten and harass her.[68] The police did not secure a warrant or court order before having the pen register installed.[69] The pen register confirmed it was the suspect that had been calling the victim, which lead to the suspect's eventual arrest and conviction.[70]

In holding that the Fourth Amendment applies only if a person's "reasonable expectation of privacy" was violated by government intrusion, the Court turned directly to the analysis conducted in the *Katz* decision.[71] The Court found the Fourth Amendment's application depends on whether a person "can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[72] That analysis turned on whether he use and installation of a pen register would violate the "legitimate expectation of privacy."[73] The Court noted a pen register is not the same as the listening device used in *Katz* because a pen register does not record the actual contents of the communication.[74] The Court went on to

64. *Id.* at 361 (Harlan, J., concurring).
65. *Id.*
66. *Id.* at 362.
67. Smith v. Maryland, 442 U.S. 735 (1979).
68. *Id.* at 737.
69. *Id.*
70. *Id.* at 737–38.
71. *Id.* at 739.
72. *Id.* at 740.
73. *Id.* at 741.
74. *Id.*; *see also* United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977) (describing that a pen register does not record sound or conversations. Pen registers "disclose only the telephone numbers that have been dialed").

reject the idea that a pen register's use constitutes a search under the Fourth Amendment because it does not violate a legitimate expectation of privacy because of the pen register's limited capabilities.[75]

To reach this conclusion, the Court applied the two-prong test described by Justice Harlan in the *Katz* decision.[76] First, the Court found there could be no subjective expectation of privacy because of a "doubt that people in general entertain any actual expectation of privacy in the numbers they dial,"[77] and that telephone users know that the phone numbers they dial must go through the telephone company's switchboard in order to complete the call.[78] Second, the Court refused to find that the expectation of privacy argued by the defendant was an expectation that society would find to be reasonable.[79] The Court found a person cannot have an expectation of privacy when they voluntarily submit their information to a third party, including the telephone company.[80] Further, when the defendant used his phone, he voluntarily turned over his information to the telephone company, which "exposed" his information in order to complete any calls, and defeated the argument about the defendant's legitimate expectation of privacy.[81] Based on its conclusion that there was no reasonable expectation of privacy in numbers dialed, and therefore no need to get a warrant to acquire that information, the Court affirmed the lower courts' judgment in favor of the State.[82]

3. The 21st Century and the Digital Age

As technology advances into the 21st century, it appears the Court has recognized technology can advance at a faster pace than the law, which has forced the Court to apply traditional Fourth Amendment principles and earlier decisions to the new and emerging technologies. The Court has also analyzed how law enforcement can intercept and search digital information contained in the new technologies, including cell phones, and how basic Fourth Amendment principles still protect citizens' right to privacy.

a. *Kyllo v. United States*

The Court confronted such a situation in *Kyllo v. United States*. In *Kyllo*, law enforcement used a thermal imaging scanner to scan the

75. *Smith*, 442 U.S. at 742.
76. *Id.*
77. *Id.*
78. *Id.*
79. *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).
80. *Id.* at 743–44.
81. *Id.* at 744.
82. *Id.* at 745–46.

defendant's residence in order to determine if there was marijuana being grown inside.[83] This scan was conducted without a probable cause warrant.[84] The defendant unsuccessfully moved to suppress the evidence seized after a subsequent search warrant was signed and carried out by agents.[85] After the District Court determined the thermal imaging was non-intrusive and did not violate the Fourth Amendment, the Court of Appeals affirmed the guilty plea after conducting the two-prong *Katz* test.[86] The Supreme Court granted certiorari.[87]

In writing for the majority, Justice Antonin Scalia noted technology impacts the privacy rights of citizens.[88] The central question the Court confronted in *Kyllo* was "what limits there are upon this power of technology to shrink the realm of guaranteed privacy."[89] In this case, the central focus was upon a search of the home, and the Court found that when dealing with the privacy of a person's home, there is a "minimum expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."[90] The Court noted the precedent of guaranteeing privacy for a person's home ran deep within Fourth Amendment jurisprudence and that it must be protected.[91]

Following that analysis, the Court found the intrusion by thermal imaging into the home, without first obtaining a warrant, was in violation of the Fourth Amendment.[92] However, the Court also found the *Katz* court was correct in rejecting the trespass-based doctrine of the past because of the impeding threat of new technology.[93]

In his dissenting opinion, Justice Stevens made a noteworthy argument to support his belief that no "search" occurred in this case. He noted that while a homeowner has an expectation of privacy for what occurs inside his home, there is no expectation of privacy when what occurs within the home is opened to the public,[94] and anything inside the home which leaves the four

---

83. Kyllo v. United States, 533 U.S. 27, 29–30 (2001).
84. *Id.* at 30.
85. *Id.*
86. *Id.* at 30–31.
87. *Id.*
88. *Id.* at 33–34. ("It 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").
89. *Id.* at 34.
90. *Id.* at 34 (emphasis in original).
91. *Id.* at 34 ("To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment").
92. *Id.* at 40.
93. *Id.* at 35–36 ("Reversing that approach would leave the homeowner at the mercy of advancing technology. . . . [T]he rule we adopt must take account of more sophisticated systems that are already in use or in development").
94. *Id.* at 44 (Stevens, J., dissenting) ("But the equipment in this case did not penetrate the walls of petitioner's home, and while it did pick up 'details of the home' that were exposed to the public, it did not obtain 'any information regarding the *interior* of the home") (internal citations omitted) (emphasis in original).

corners of the home and can be viewed from the public realm has no reasonable expectation of privacy, including heat emissions in this case.[95] He argued because technology continues to advance, the threat to privacy will continue to grow as the new technology becomes more available to the general public.[96]

Finally, Justice Stevens observed the Court is not in the best position to create such rules under the Constitution, as technology advances faster than the Court can hear the cases concerning it.[97] He argued it would be a much better alternative to give Congress the opportunity to face these challenges in a far more timely manner and with freedom from restrictive judicial decisions.[98]

b. *United States v. Jones*

The Court faced another recent test of electronic surveillance under the Fourth Amendment with *United States v. Jones*, a case about Fourth Amendment restrictions on GPS tracking. Law enforcement placed a GPS tracking device on the undercarriage of the defendant's wife's car and tracked the movement over a period of 28 days.[99] While the police secured a warrant ahead of time, they placed the GPS tracker outside of the authorized date and location stated in the warrant.[100] The District Court only partially suppressed the data when the defendant filed a motion to suppress, but the defendant was still convicted.[101] The Court of Appeals held the admission of the warrantless GPS evidence violated the Fourth Amendment and the Supreme Court granted certiorari.[102]

The majority opinion, again written by Justice Scalia, affirmed the decision of the Court of Appeals holding the warrantless use of the GPS tracker violated the Fourth Amendment.[103] The Court first noted the *Katz* privacy test was an addition to the common-law trespass test.[104] The Court then applied the common-law trespass test and concluded that law enforcement had intruded on the defendant's Fourth Amendment rights because officers physically attached the GPS device to the defendant's vehicle.[105]

---

95. *Id.* at 43–44.
96. *Id.* at 47.
97. *Id.* at 51.
98. *Id.* ("It would be far wiser to give legislators an unimpeded opportunity to grapple with these emerging issues rather than to shackle them with prematurely devised constitutional constraints").
99. United States v. Jones, 565 U.S. 400, 402 (2012).
100. *Id.* at 403.
101. *Id.* at 404.
102. *Id.*
103. *Id.* at 413.
104. *Id.* at 409.
105. *Id.* at 410–14.

Justice Alito's concurring opinion has drawn the most attention from commentators.[106] Justice Alito agreed with the outcome of the case, but instead of applying the trespass-based theory of the majority, he suggested an approach consistent with the *Katz* "reasonable expectation of privacy" test.[107] While he agreed with the majority that a trespass-based rule based on the original understanding of the Fourth Amendment is still appropriate, he found it is impossible to apply to today's technology.[108] He further argued, after a thorough analysis of the Court's precedent on electronic surveillance, the majority could not find much support for its trespass-based rule in any post-*Katz* cases.[109] Finally, he opined the use of the trespass-based rule alone would provide a particular problem for electronic surveillance that made no physical contact when it was tracking.[110] He questioned whether the post-*Katz* decisions were an actual change in the law or just taking the trespass-based rule and attempting to reapply it to an entirely new and technological field.[111]

Justice Alito went on to look at the *Katz* expectation of privacy test and found it also has some troubles of its own.[112] He noted "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[113] Further, he reasoned the *Katz* test worked for only a "well-developed and stable set" of a person's expectations of privacy.[114] However, he argued the rapid change in technology could quickly change what a person's expectation of privacy would be and what would be considered "reasonable."[115]

---

106. *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Erin Murphy, *Back to the Future: The Curious Case of* United States v. Jones, 10 OHIO ST. J. OF CRIM. L. 325 (2012); Jeffrey Neuburger, US v. Jones: *Unanimous Ruling, Disagreeing Justices*, LAW 360 (Jan. 24, 2012 1:13 PM), http://www.law360.com/articles/302750/us-v-jones-unanimous-ruling-disagreeing-justices (last visited Oct. 15, 2016); Dahlia Lithwick, Alito vs. Scalia, SLATE (Jan. 23, 2012, 6:38 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2012/01/u_s_v_jones_supreme_court_justices_alito_and_scalia_brawl_over_technology_and_privacy_.html.

107. *Jones*, 565 U.S. at 418–19 (Alito, J., dissenting).

108. *Id.* at 420 ("The Court argues—and I agree—that 'we must "assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."' But it is almost impossible to think of late-18th-century situations that are analogous to what took place in this case") (internal citations omitted).

109. *Id.* at 424.

110. *Id.* at 426–27.

111. *Id.*

112. *Id.* at 427–28.

113. *Id.* at 427.

114. *Id.*

115. *Id.* ("In addition, the 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

Justice Alito even went beyond the facts of this case and noted this shift in expectations of privacy may reach beyond just GPS tracking devices.[116] He specifically mentioned cell phones and other wireless devices as another possible area that will feel the effects of this shift in privacy and technology.[117] As part of his proposed solution, Justice Alito recommended it may be the best course of action to leave the privacy concerns and policy decisions to the legislative branch instead of having the courts decide where the "privacy line" should be.[118]

c. *Riley v. California*

The Court directly addressed the application of the Fourth Amendment to cell phones in *Riley v. California*. In this consolidated case, the Court faced the question whether law enforcement may search information contained within a cell phone seized from a person who has been arrested, without possessing a search warrant.[119] In both cases, each defendant had their cell phone taken and searched after each had been arrested.[120] Each defendant unsuccessfully argued the evidence taken from their cell phones was in violation of the Fourth Amendment and should be suppressed.[121] Both defendants were subsequently convicted and each conviction was affirmed on appeal.[122] The Supreme Court granted certiorari in both cases and consolidated them for decision.[123]

In a unanimous decision, the Court found police officers generally cannot search information contained within cell phones taken from defendants incident to the defendants' arrest without a search warrant.[124] In writing for the Court, Chief Justice Roberts primarily based the decision on a situation where the cell phone is being personally inspected by an arresting officer or detective after the defendant has been arrested.[125] Further, Chief

---

that new technology entails, they may eventually reconcile themselves to this development as inevitable").

116. *Id.* at 428–29.

117. *Id.* ("Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. . . . The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

118. *Id.* at 429–30 ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way").

119. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

120. *Id.* at 2480–82.

121. *Id.*

122. *Id.*

123. *Id.* at 2481–82.

124. *Id.* at 2485.

125. *Id.*

Justice Roberts gave very compelling arguments as to why cell phones should be afforded great protection under the Fourth Amendment.

Chief Justice Roberts noted cell phones in today's modern digital age are most notable for their "immense storage capacity."[126] Cell phone users carry with them "millions of pages of text, thousands of pictures, or hundreds of videos."[127] A cell phone contains all this information into one place, which is then carried by the owner almost everywhere they go.[128] The Court even noticed a recent poll found "nearly three-quarters of smart phone users report being within five feet of their phones most of the time…."[129] The Court continued that "it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives…."[130] Importantly, the Court even stated, "[a]llowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case."[131]

When discussing its holding, the Court discussed the application of a warrant to the search of a cell phone. The Court found while it "is not that the information on a cell phone is immune from search; it is instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."[132] The Court noted precedent has supported that "the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'"[133]

At the end of the decision, the Court made some of its most relevant observations related to cell phones and those observations contain relevant principles that could be used to argue that warrants should be required to use Stingrays. The Court recognized the basis of the Fourth Amendment is to prevent unreasonable searches and seizures and was written in the colonial era to prevent such searches and seizures by British officials.[134] The Court stressed privacy of modern cell phones are not "any less worthy of the protection for which the Founders fought."[135] In the final sentence of the opinion, the Court clearly stated: "Our answer to the question of what police

126. *Id.* at 2489.
127. *Id.*
128. *Id.*
129. *Id.* at 2490.
130. *Id.*
131. *Id.*
132. *Id.* at 2493.
133. *Id.* (quoting Coolidge v. New Hampshire, 403 U.S. 443, 481 (1971)).
134. *Id.* at 2494.
135. *Id.* at 2495.

must do before searching a cell phone seized incident to arrest is accordingly simple—get a warrant."[136]

In his concurring opinion, Justice Alito took a very similar position as he did when writing his concurrence in *Jones*. Justice Alito reasoned that because cell phones play such an integral part of society in the modern digital age, the Court is ill equipped to evaluate the privacy interests presented through their use.[137] He even noted modern technology is making it easier "for both government and private entities" to collect information about lives of American citizens.[138] Further, in a similar fashion as he reasoned in *Jones*, Justice Alito argued federal courts should not be left to decide privacy protections "using the blunt instrument of the Fourth Amendment,"[139] but rather that "[l]egislatures, elected by the people" are better suited to respond to the changes that have occurred and will likely occur related to cell phone privacy.[140]

C. Current Academic Literature on the Fourth Amendment

Stingrays have gathered a great amount of interest in the academic community and those that study the Fourth Amendment. Since they have only begun to enter the legal arena as defendants and privacy advocates learn more about them, Stingrays' legal operation is ripe for discussion and commentators have taken hold of the topic. With the ability to be operated as a pen register or a wiretap device, there is no solid rule on whether collection of data by a Stingray constitutes a search under the Fourth Amendment. However, commentators have offered different theories that may be able to assist Congress and the courts in finding that rule.

Professor Orin Kerr wrote one of the most interesting discussions of Stingray operation and legality in an article published in *The Washington Post*.[141] Professor Kerr conducted his analysis of the use of a Stingray through *State v. Andrews*, a case decided by the Maryland Court of Special Appeals.[142] As part of his analysis, Professor Kerr suggested five possible Fourth Amendment rules may apply to Stingrays.[143] These rules range from suggesting that using a Stingray is never a search to using a Stingray always

136. *Id.*
137. *Id.* at 2497 (Alito, J., concurring).
138. *Id.*
139. *Id.*
140. *Id.* at 2497–98.
141. Orin Kerr, *Applying the Fourth Amendment to Cell-Site Simulators*, THE WASHINGTON POST (Apr. 4, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/04/04/applying-the-fourth-amendment-to-cell-site-simulators/?utm_term=.08bb7513293f.
142. State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).
143. Kerr, *supra* note 141.

constitutes a search.[144] After describing the facts and the court's opinion in *Andrews*, Professor Kerr found that while the court likely got to the correct answer that a warrant is necessary to use a Stingray, their analysis was weak when finding that use of a Stingray always constitutes a search under the Fourth Amendment.[145]

Professor Kerr questioned why the court found using a Stingray *always* constitutes a search, especially if the Stingray, for example, located the defendant "walking down a public street nearby talking openly on his phone."[146] In a case like that, Professor Kerr argued the Fourth Amendment would not be implicated.[147] Additionally, Professor Kerr touched on the court's use of the oft-quoted concurring opinion by Justice Sotomayor in *Jones*. Professor Kerr questioned why the court would use Justice Sotomayor's argument of long-duration tracking as a basis for deciding a case that involved the use of a single tool at one time to locate a suspect.[148] He found Justice Sotomayor's *Jones* concurrence to be inapplicable to this case, so it should not have been a basis for the court's decision.[149]

Other commentators would likely disagree with Professor Kerr and find the use of a Stingray is always a search and should require a warrant. Commentators have found if the Supreme Court were to find that tracking a cell phone were to constitute a search under the Fourth Amendment, it is likely that the Court could find a person's location is private, which would require a warrant to track their real-time location.[150] Other commentators have also found current Fourth Amendment jurisprudence supports the belief that the use of a Stingray constitutes a search under the Fourth Amendment because interception of cell phone data and GPS tracking violates a reasonable expectation of privacy.[151]

144. *Id.*
145. *Id.*
146. *Id.*
147. *Id.*
148. *Id.*
149. *Id.*
150. MICHAEL C. GIZZI & R. CRAIG CURTIS, THE FOURTH AMENDMENT IN FLUX: THE ROBERTS COURT, CRIME CONTROL, AND DIGITAL PRIVACY, 151 (2016).
151. Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 HASTINGS L.J. 183 (2014); Brittany Hampton, Note, *From Smartphones to Stingrays: Can the Fourth Amendment Keep Up with the Twenty-First Century?*, 51 U. OF LOUISVILLE L. REV. 159 (2012).

D. Modern Statutory Law and Electronic Surveillance

As Justice Alito described in *Jones*, Congress has previously heard the concerns of the courts and privacy advocates, and has enacted multiple statutes that cover electronic surveillance and its use by law enforcement.[152] In response to the Court's decision in *Katz*, Congress enacted the Electronic Communications Privacy Act of 1986 (ECPA).[153] The ECPA has three titles: Title I, referred to as the Wiretap Act; Title II, referred to as the Stored Communications Act; and Title III, the Pen Register and Trap and Trace Devices title, also known as the Pen/Trap statute.[154]

Title I, the Wiretap Act,[155] "prohibits the intentional actual or attempted interception, use, disclosure, or 'procure[ment] [of] any other person to intercept or endeavor to intercept any wire, oral, or electronic communication.'"[156] However, there are exceptions provided by statutory amendments including the USA PATRIOT Act.[157] Title II, the Stored Communications Act,[158] "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers, such as subscriber name, billing records, or IP addresses."[159] Title III, the Pen/Trap statute,[160] allows law enforcement officials to install a pen register or a trap and trace device with authorization from a court order.[161]

By enacting the ECPA, Congress showed its understanding that technology was rapidly advancing and that it was necessary to enact updated statutory law that would protect citizens' Fourth Amendment rights to privacy and against unreasonable searches and seizures. In their report on the ECPA, the House Judiciary Committee noted that as long as technology advances, there is an ever-increasing chance the Fourth Amendment

152. United States v. Jones, 565 U.S. 400, 427–28 (2012).
153. *Id.*
154. U.S. Dep't of Just., *Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22.*, JUST. INFO. SHARING, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last updated Jul. 30, 2013).
155. 18 U.S.C. §§ 2510-2522 (2012).
156. JUST. INFO. SHARING, *supra* note 154.
157. *Id.* (These exceptions include issues of national security and emergency situations where it is impractical or impossible to secure a warrant before it is necessary to engage in wiretapping or recording activities.).
158. 18 U.S.C. §§ 2701-2712.
159. JUST. INFO. SHARING, *supra* note 154.
160. 18 U.S.C. §§ 3121-3127.
161. JUST. INFO. SHARING, *supra* note 154 ("[R]equires government entities to obtain a court order authorizing the installation and use of a pen register (a device that captures the dialed numbers and related information to which outgoing calls or communications are made by the subject) and/or a trap and trace (a device that captures the numbers and related information from which incoming calls and communications coming to the subject have originated). No actual communications are intercepted by a pen register or trap and trace.").

protections of citizens will begin to disappear.[162] Additionally, the Committee noted, like the Supreme Court, that there must still be "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[163]

This background section has provided a general overview of Stingrays, Fourth Amendment case law, and current statutory law in order to provide a foundation for the statutory scheme that will be proposed at the end of this note. Each can be used and supplemented into the proposed legislation that would create a statutory "guideline" for both law enforcement and the courts to use when evaluating and creating probable cause warrants when operating a Stingray as part of a criminal investigation.

III. ANALYSIS

For many years, Stingrays have been a closely guarded secret by law enforcement.[164] As details about their use have now begun to emerge in the courts, it has become clear that judges really do not know what they are or what they can do.[165] However, as details about the use and operation of Stingrays slowly make their way into the general public, it is apparent that the use of these devices are in need of some type of regulation. While these devices are being used today, there is no set legal standard in either the common law or federal statutory law that gives a precise standard for both law enforcement officials and the courts to follow.[166] Therefore, it is now necessary for Congress to step in and create a statutory standard that not only regulates how law enforcement can use Stingrays, but also the point at which they impinge on an individual's Fourth Amendment rights, whereby evidence collected by them must be excluded.

Stingrays produce a unique problem because of their ability to operate both as a pen register and as a wiretap device.[167] It is difficult to determine under which portion of the ECPA Congress should treat these devices in order to balance the investigative goals of law enforcement with the necessary protections of the Fourth Amendment. A line must be drawn down the middle, and based on recent policy shifts by the Department of Justice, that line has become clearer.

The following sections will describe the modern issues with Stingrays in the court system, briefly explain the Department of Justice's new policy

---

162. H.R. REP. NO. 99-647, at 19 (1986).
163. *Id.*
164. *See* Cox, *supra* note 2.
165. *See generally In re* Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 U.S. Dist. LEXIS 151811 at *2, *10 (N.D. Ill. 2015).
166. *See* Cox, *supra* note 2, at 30–31.
167. *See* Zetter, *supra* note 13.

on Stingrays, and argue that amending current statutory law will provide the greatest form of protection for both American citizens and law enforcement investigations.

A. Stingrays' Appearance in the Lower Courts

It is clear as Stingrays emerge in litigation that they are posing new problems for judges considering the use of evidence gathered via Stingrays. The first issue is that most judges have no idea what Stingrays are or what they can do because Stingrays have been kept secret for so long.[168]

In the Northern District of Illinois, U.S. Magistrate Judge Iain Johnston was presented with an application for a warrant to use a "cell-site simulator" (generally the name used by the government in an application to use a Stingray) in an investigation that was targeting the subject's cell phone.[169] Judge Johnston initially presented a troubling question: "So where is one, including a federal judge, able to learn about cell-site simulators?"[170] This question was followed by a series of even more troubling answers as found by the court: Federal agents and prosecutors were unwilling to divulge too much information, the Internet was an unreliable source, law review articles were lacking, and case law was undeveloped and unhelpful.[171]

Judge Johnston noted an excellent place to find information about a cell-site simulator was in a report published by the Department of Justice.[172] However, this manual presents a concerning issue that the court failed to take into consideration. The manual cited was published in 2005,[173] and the judge wrote the order in 2015.[174] Based on the rapid growth of technology in the 21st century, it is very difficult to believe that Stingrays' technological abilities failed to grow within the span of ten years. It is most likely that Judge Johnston was relying on heavily outdated information, which would have only provided a disservice when attempting to figure out what the government was actually applying to use.

One case that has shed a great deal of light on the use of Stingrays is *United States v. Rigmaiden*.[175] In *Rigmaiden*, the defendant was charged with multiple counts of mail and wire fraud, aggravated identity theft, and

168. *See In re* Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 U.S. Dist. LEXIS 151811 at *2 (N.D. Ill. 2015) at 2.
169. *Id.*
170. *Id.* at *3.
171. *Id.* at *3-5.
172. *Id.* at *5-6 (citing U.S. Dept. of Just., *Electronic Surveillance Manual* (June 2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf).
173. U.S. Dept. of Just., *Electronic Surveillance Manual* (June 2005), http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf.
174. *See In re* Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 U.S. Dist. LEXIS 151811 at *2, *10 (N.D. Ill. 2015).
175. United States v. Rigmaiden, 844 F. Supp. 2d 982 (D. Ariz. 2012).

conspiracy.[176] As part of his capture, the government located the defendant by tracking the aircard attached to his computer and the defendant sought discovery materials related to the technology used for that tracking, alleging that it violated his Fourth Amendment rights.[177] The government sought to exclude this discovery because it was subject to the law enforcement privilege stated in *Roviaro v. United States*.[178] The defendant responded that the law enforcement privilege did not apply because the technology used by the government in this case was already known to the public and that his need for the information overcame that privilege.[179]

In writing the opinion, Judge Campbell noted during the course of an *ex parte* hearing, an FBI agent described "how the equipment used in locating the aircard operates, how it was used in this particular case, and why disclosure of information regarding the equipment and techniques used to locate the aircard would hamper future law enforcement efforts."[180] Later in the opinion, the court noted the government was conceding, for purposes of a Fourth Amendment argument, the mobile tracking device was a cell-site simulator that replicated a Verizon Wireless cell tower; that FBI agents used the device on foot and acquired real time data while tracking the aircard; and the device used is a different device from a pen register or trap and trace device.[181] While not specifically mentioned in the opinion, it was later released that the device in question was in fact a Stingray.[182]

As the court went through each request for production by the defendant, the court denied almost every request based on law enforcement privilege.[183] What is surprising about this decision is the broad application the court used in applying the *Roviaro* rule, which provides for non-disclosure of certain law enforcement investigative techniques without much explanation.[184] While there is an obvious necessity for the use and application of the *Roviaro* rule, it becomes an issue when the defendant is afforded almost no opportunity to challenge the use of the technology used to find them, or to even discover anything about the technology that is necessary to prepare an adequate defense (subject, of course, to necessary national security exceptions and classified information). In investigations where a citizen's

176. *Id.* at 987.
177. *Id.*
178. *Id.* at 989 (citing Roviaro v. United States, 353 U.S. 53 (1957)).
179. *Id.*
180. *Id.* at 994.
181. *Id.* at 995.
182. Tim Dees, *New Tech at the Center of U.S. v. Rigmaiden Case*, POLICEONE.COM (June 10, 2013), https://www.policeone.com/csi-forensics/articles/6269067-New-tech-at-the-center-of-U-S-v-Rigmaiden-case/.
183. *Rigmaiden*, 844 F. Supp. 2d at 996-1005.
184. *Id.* at 994 ("The Court concludes that disclosure of the additional information sought by Defendant would compromise the ability of the FBI and other law enforcement agencies to combat crime.").

right to privacy and likely subsequent criminal proceedings occur, it becomes necessary for judges to consider the evidence and arguments from both parties to determine whether the use of these devices is consistent within the scope of the Fourth Amendment.

This suggestion not only helps protect citizens and their rights, but it also benefits law enforcement during their investigations. It should be a top priority of law enforcement investigations to ensure preservation of evidence that is collected for use during trial. If law enforcement tries to be too secretive in their use of these devices, they risk the suppression of entire blocks of evidence if a judge, because of a lack familiarity with the technology, errs on the side of caution in order to protect the defendant. It benefits law enforcement to be open with judges about the nature of Stingrays, which in turn will garner a greater sense of trust with both judges and the public that it affects.[185]

B. Federal Rule of Criminal Procedure Rule 41 and the Department of Justice's New Policy Regarding the Use of Stingrays

The Stingray has a complicated legal history in the federal system when used by the Department of Justice. Some legal scholars maintain current statutory language does not authorize Stingrays.[186] Even though Congress has not forbidden the use of Stingrays, they have failed to create any specific standards for their use or application for use. Currently, the only closely related articulable standard is set out in the Communications Assistance for Law Enforcement Act (CALEA), which forbids acquiring real-time location data based "solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of Title 18)."[187] However, this standard applies specifically to the service carrier when assisting the government with a lawful search pursuant to a court order,[188] not when the government conducts the search on its own with a Stingray. Further, this statute does not define an articulable standard as to what level of evidence is

185. *See* Dees, *supra* note 182 ("The lesson here, if there is one, is for cops to be forthcoming when seeking search warrants using technology that may be unfamiliar to the issuing judge. The police may need to educate the judge about how some of the new toys work. If that doesn't happen, a judge in another case may decide the government didn't meet its 'duty of candor' and suppress the evidence.").

186. *See* Pell & Soghoian, *supra* note 1, at 150.

187. 47 U.S.C. § 1002(a)(2) (1994).

188. *Id.* ("[A] *telecommunications carrier* shall ensure that its equipment, facilities, or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of . . . (2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is *reasonably available to the carrier*.") (emphasis added).

sufficient for the application of a Stingray, beyond what is necessary for a normal Pen/Trap order.[189]

In response to the Congressional amendments and reformation of electronic surveillance statutes, the Department of Justice created the "hybrid-order" for use of Stingrays.[190] The "hybrid-order" was created by the Department as an attempt to create a uniform application for the use of Stingrays because Congress failed to give them any articulable standard.[191] The "hybrid-order" combined both the Pen/Trap order, as well as elements of a Stored Communications Act order under 18 U.S.C. § 2703(d), which was created to compensate for the limitations of orders solely under the authority of the Pen/Trap statute.[192] However, this proposed order was not widely accepted by the judiciary and continued to create inconsistencies throughout the country.[193]

In response to the criticism by legal scholars, the judiciary, and the privacy bar, the Department released a brand new policy in 2015 that completely reshaped the way it would operate Stingrays through federal law enforcement agencies across the country.[194] In this release, the Department provided a wealth of information, including what Stingrays are, how they operate, and what the Department intended to do in order to effectively operate them within the scope and parameters of the law.[195]

There were a number of important details released with the new policy, including: (1) Stingrays would not be operated as GPS trackers;[196] (2) they would be configured to operate as *pen registers* within the scope of the Pen/Trap statute;[197] (3) subscriber information would not be collected;[198] (4) future orders authorizing the use of Stingrays would require obtaining a *probable cause warrant* within the scope of Rule 41 of the Federal Rules of Criminal Procedure;[199] and (5) data collected that was not related to the target number would have procedures in place to have such data deleted within 30 days.[200]

By creating this new policy, the Department of Justice began to move in the right direction to creating an acceptable legal standard for the application and use of Stingrays. However, there are still problems with this

189. *See* Pell & Soghoian, *supra* note 1, at 151.
190. *See id.*
191. *See id.*
192. *See id.*; see also Cox, *supra* note 2, at 30.
193. *See* Pell & Soghoian, *supra* note 1.
194. *Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology*, U.S. DEP'T OF JUST., http://www.justice.gov/opa/file/767321/download (last visited Sept. 14, 2017).
195. *Id.*
196. *Id.* at 2.
197. *Id.*
198. *Id.*
199. *Id.* at 3.
200. *Id.* at 6.

method, which will be further addressed later in this note. At least for now, it is sufficient to say that the new policy shift of the Department, while a great step in the right direction, cannot replace the statutory standard which the proposed solution will be able to offer.

It becomes necessary for Congress and the courts to establish a hard and fast rule on the use of Stingrays. This rule must be based on the language of the Fourth Amendment and current Supreme Court precedent, which has taken a drastic shift towards considering a suspect's "reasonable expectation of privacy." Additionally, the creation of a statutory standard for the application for use of Stingrays will also create a national standard that both the Department of Justice and the courts will be able to follow when applications for use are applied for and when search warrants are ordered.

C. Congress and the Stingray Privacy Act of 2015

It has become apparent Congress has heard the calls from the privacy bar and the courts for an articulable legal standard for the use of Stingrays. In November 2015, Congressman Jason Chaffetz introduced on the House floor a bill designed specifically to address the issue of Stingrays and their use by law enforcement. The Stingray Privacy Act of 2015[201] was introduced in order to create a statutory standard that requires federal law enforcement agencies to obtain a probable cause warrant before using a Stingray, with noted exceptions for emergency and national security situations.[202] Additionally, it would have created exclusionary rules that would have required that evidence obtained illegally and/or without a warrant would be inadmissible during any court or official proceeding.[203]

Furthermore, Congress attempted to target real-time location tracking with Stingray devices in another bill called the GPS Act of 2015.[204] The GPS Act would have prohibited Stingray devices, as well as other GPS enabling devices, from tracking cell phones, computers, and other electronic devices through the use of their GPS capabilities.[205] It would have additionally required a probable cause warrant to allow interception along with the exceptions and exclusions generally stated in the Stingray Privacy Act.[206]

While neither of these bills moved beyond the initial stages of their respective body of Congress during the 114th session, their introduction highlights the fact that Congress has heard the calls from private advocates

201. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015).
202. *Id.*
203. *Id.*
204. GPS Act of 2015, S. 237, 114th Cong. (2015).
205. *S. 237 – GPS Privacy Act of 2015*, U.S. CONGRESS, https://www.congress.gov/bill/114th-congress/senate-bill/237.
206. *Id.*

and the courts that the use of Stingrays needs to be regulated and that a statutory standard for their application and use is absolutely necessary. When Congress passed the ECPA, the Pen/Trap Statute, the Wiretap Act, the Stored Communications Act, and the CALEA, it showed its ability to pass necessary legislation in order to regulate electronic surveillance that benefits law enforcement investigations while protecting the Fourth Amendment rights of citizens.[207]

IV. PROPOSED SOLUTION

In order to create the most effective balance between citizens' privacy rights under the Fourth Amendment and law enforcements' investigative goals, the most effective way to regulate the use of Stingrays is by creating a new supplemental chapter, "Chapter 206A – Cell-Site Simulators," to Chapter 206 of Title 18, which regulates the use of Pen/Trap devices.[208] The proposed chapter would require Stingrays, operated by federal agencies, be operated only as pen registers, but would require a probable cause warrant under Rule 41 of the Federal Rules of Criminal Procedure in order to satisfy the requirements of the Fourth Amendment and current Supreme Court precedent. Additionally, the proposed chapter would include exclusionary rules that prevent abuse and regulate the admissibility of evidence in court. Finally, the proposed chapter must apply to federal law enforcement agencies with the goal of encouraging state legislatures to adopt the federal statutory standard in order to create a uniform national standard for the application and use of Stingrays.

A. Legislation is the Most Effective Solution to the Stingray Problem

When determining whether the more appropriate avenue is either the creation of legislative, executive, or judicial standards for Stingrays, it becomes apparent that the creation of legislation is the most effective action that both Congress and the courts should endorse. While courts act in more of a "reactionary" method by creating standards after a case or controversy has already occurred, and the Executive Branch creates policies with the ability to change them at any time, Congress is in the best position to attack problems once they occur. In the case of electronic privacy in the 21st century, legislative action has not only been endorsed by the Court, but it has been followed in practice by Congress.

The Justices of the Supreme Court have not been shy in lending their endorsement to proactive legislative action in the field of electronic privacy,

207. *See* Cox, *supra* note 2, at 35.
208. 18 U.S.C. §§ 3121-3127 (2012).

with Justice Samuel Alito being particularly outspoken. Justice Alito has indicated his belief that Congress is in a better position to create manageable electronic privacy rules and regulations than the Court may be in his opinions in *Jones* and *Riley*.[209] In *Jones*, Justice Alito noted that after *Katz* was decided, Congress quickly responded to the Court's decision by passing legislation related to wiretapping.[210]

Specifically when looking at rapidly-evolving technology, Justice Alito directly noted Congress may be in a better position to create rules and regulations related to that technology because it can do so quickly and effectively with the ability to hold hearings and conduct investigations and inquiries.[211] In *Riley*, Justice Alito again made clear his belief that in advancing technology cases such as this, "[l]egislatures, elected by the people" are better suited to respond to the changes that have occurred and will likely occur related to cell phone privacy.[212]

Congress has also shown its interest in not only considering the issues related to Stingrays, but has taken affirmative steps that would create legislative standards for both law enforcement and the courts to follow. As previously discussed, members of both the House and the Senate have attempted to pass legislation that would regulate both Stingrays[213] and GPS devices.[214] However, Congress continues to press for answers related to Stingrays and what it can to do better regulate their use by law enforcement.

In December 2016, the Committee on Oversight and Government Reform in the House of Representatives published a bi-partisan report on its findings related to Stingrays and other cell-site simulators in a Committee report titled "Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations."[215] In the report, the Committee laid out their year-long findings about cell-site simulators, including the finding that between 2010 and 2014, the Department of Justice owned 310 cell-site simulators and had spent at least $71 million on the technology.[216]

---

209. *See* United States v. Jones, 565 U.S. 400, 427–28 (2012) (Alito, J., concurring); *see also* Riley v. California, 134 S. Ct. 2473, 2497–98 (2014).

210. United States v. Jones, 565 U.S. 400, 427-28 (2012) (Alito, J., concurring) (". . . concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping. After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute, and since that time, the regulation of wiretapping has been governed primarily by statute and not by case law.")

211. *Id.* at 429–30 ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way").

212. Riley v. California, 134 S. Ct. 2473, 2497–98 (2014).

213. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015).

214. GPS Act of 2015, S. 237, 114th Cong. (2015).

215. COMM. ON OVERSIGHT AND GOV. REFORM, LAW ENFORCEMENT USE OF CELL-SITE SIMULATION TECHNOLOGIES: PRIVACY CONCERNS AND RECOMMENDATIONS 1 (2016).

216. *Id.* at 5.

It also found Stingrays were being operated by local and state law enforcement agencies with the "hybrid-order" warrant, similar to the one that the federal agencies operated on before the DOJ policy shift moved to probable cause warrants.[217] After noting its findings, the Committee specifically noted what Justice Alito said in the *Jones* case when he recommended that Congress may be in a better position to create rules and regulations related to quickly-advancing technology, which would include Stingrays.[218] As part of their recommendations, the Committee outright recommended that Congress should pass some type of legislation that would regulate the use of Stingrays by federal law enforcement.[219] The Committee also recommended that non-disclosure agreements be replaced with candid agreements that require disclosure to the courts whenever a Stingray is used by law enforcement officials in the course of an investigation.[220]

The proposed statutory chapter falls directly in line with both Congressional and judicial attempts to not only create national statutory standards, but to create a system of candor and apparent use of Stingrays so that Congress, the courts, and the American people all know and understand how and when Stingrays are used. Once officials remove the shroud of secrecy that Stingrays are still cloaked in, it will give the American people the ability to truly judge and evaluate the technology, and even give them the chance to give it their "seal of approval" if they see law enforcement using it for a positive purpose.

As Congress continues to investigate and collaborate on Stingrays, the proposed solution in the form of a statutory standard follows exactly what the Committee recommended as the first course of action that should be taken with Stingrays.[221] As the proposed chapter would recommend, it would also serve as a guideline for States to follow in creating a uniform national standard that local, state, and federal law enforcement agencies can all adopt and follow. The creation of this proposed chapter to serve as such a guide would adopt another Committee recommendation for a uniform standard.[222]

---

217. *Id.*
218. *Id.* at 35.
219. *Id.* at 35–36 ("Congress should establish a legal framework that governs government agencies, commercial entities, and private citizens' access to and use of geolocation data, including geolocation data obtained by the use of a cell-site simulator. Congress should pass legislation to establish a clear, nationwide framework for when and how geolocation information can be accessed and used.").
220. *Id.* at 36.
221. *Id.*
222. *Id.*

B. The Proposed Chapter

1. Create "Chapter 206A – CELL-SITE SIMULATORS" Under Title 18 to Create a Uniform National Standard for the Use and Application for Use of Stingrays

The current lack of a national legal standard on the application and use of Stingrays poses a risk to personal privacy and unreasonable searches and seizures under the Fourth Amendment. It is necessary to protect citizens' Fourth Amendment rights; it is also necessary to protect law enforcements' ability to conduct thorough investigations. Therefore, in order to provide "a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment,"[223] a solution that will provide such a balance is to create a supplemental chapter to the current Chapter 206, which deals with Pen Registers and Trap and Trace Devices. Through the creation of this supplemental chapter, Congress will be able to effectively establish a statutory rule that Stingrays will only be operated as a pen register, but will apply a probable cause standard for the application for their use.

While the text and rules of the proposed Stingray Privacy Act were on-point as far as creating an acceptable national standard for the application and use of Stingrays, it went too far in one aspect. The bill proposed an amendment of Chapter 205 of Title 18 to include a new section "§ 3119: Cell-site simulators."[224] 18 U.S.C. Chapter 205 covers "Searches and Seizures" and is the statutory language that defines acceptable law enforcement practices regarding general searches and seizures.[225] If Stingrays were operated to their full capacity to have the ability to operate not only as a pen register, but also as a wiretap device by recording conversations and text messages, it would be more agreeable to place Stingrays within the scope of this chapter. However, if Stingrays are configured as pen registers as suggested in the new policy, Stingrays would not intercept materials within the scope of a "search and seizure" under Chapter 205; they would instead only capture materials within the scope of the Pen/Trap statute under Chapter 206.

Therefore, it would only be necessary to place Stingrays within the Pen/Trap statute and to apply its current standard of "relevant to an ongoing criminal investigation."[226] However, since Stingrays can operate on a more intrusive scale than a pen register or trap and trace device, it would also be inappropriate to place Stingrays only within Chapter 206 with a "relevancy" standard.

---

223. Oliver v. United States, 466 U.S. 170, 181 (1984).
224. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015).
225. 18 U.S.C. §§ 3101-3118 (2012).
226. 18 U.S.C. § 3122.

By requiring that Stingrays be configured to operate only as pen registers as required by 18 U.S.C. § 3127(3)[227] and that they do not capture or record any information outside authorization of the Pen/Trap statute,[228] the Department of Justice is greatly limiting the scope of how Stingrays can be operated and what they can record. In order to reflect this new policy and to appeal to privacy advocates, Congress should place the new statutory language as a supplemental chapter to Chapter 206, which would give an indication to the courts that Stingrays must only be operated as pen registers. This new language would both reflect the Department of Justice's new policy, but would cement this policy shift as a new statutory basis that the Department and the courts would be required to follow.

In the language of the new chapter, Congress should specifically start by requiring cell-site simulators, including Stingrays, shall only be configured and operated as pen registers as defined under the Pen/Trap statute.[229] Next, Congress should instruct that use of a Stingray shall only be approved through authorization by a probable cause warrant under Rule 41 of the Federal Rules of Criminal Procedure by a court of competent jurisdiction.[230] In order to properly align with the Fourth Amendment, Congress should include the actual language of the Fourth Amendment in a "Purpose" section of the new chapter. Congress should specifically state it intends to follow the language of the Fourth Amendment[231] by requiring a judicially authorized probable cause warrant before a Stingray may be operated.

The requirement of a probable cause warrant not only falls under the language of the Fourth Amendment, but is supported by the Supreme Court's decision in *Katz v. United States*, where the Justice Harlan's oft-quoted concurrence found searches conducted without probable cause warrants violated the defendant's "reasonable expectation of privacy" and were a violation of the Fourth Amendment.[232] Additionally, as Chief Justice Roberts pointed out in *Riley v. California*, the best practice before searching a cell phone is a very simple one – get a warrant.[233] This observation is directly on point to a statutory standard that would require a probable cause warrant before operating a Stingray to intercept cell phone data.

Congress should also include that Stingrays shall only be configured and operated as pen registers as defined under the Pen/Trap statute to

227. U.S. DEP'T OF JUST., *supra* note 194.
228. *Id.*
229. 18 U.S.C. § 3127.
230. FED. R. CRIM. P. 41.
231. U.S. Const. amend. IV. (". . . 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.") (emphasis added).
232. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).
233. Riley v. California, 134 S. Ct. 2473, 2495 (2014).

conform with the Supreme Court's holding in *Smith v. Maryland*. Requiring Stingrays to operate only as a pen register will allow federal law enforcement agencies to intercept and collect data by using a Stingray without violating the suspect's "legitimate expectation of privacy" to more private information contained within the cell phone.[234]

While Rule 41 does cover warrants arising under a "search and seizure" situation, Stingrays themselves are unique technological entities and will require a mixture of language from both the Pen/Trap statute and elements of "search and seizure" warrants. By placing Stingrays in only Chapter 205 or 206, Congress would not only disapprove of the Department of Justice's attempts to operate Stingrays in an acceptable manner as a pen register device, but also instill a greater distrust both law enforcement who uses them to conduct investigations for the benefit of society, and in the device itself, which can be extremely helpful in tense and violent situations.

2. The Proposed Chapter Should Include Exclusionary Rules and Exceptions for Use During Emergencies and Issues of National Security

Beyond just this placement, the proposed chapter would further follow the language of the proposed Stingray Privacy Act in that it would create exclusionary rules and exceptions for the use of Stingrays during emergency situations and issues of national security. Law enforcement should not be hindered in moments of crisis, and the statutory language should not disturb that. The Supreme Court has noted in *Katz* that these are well-established exceptions where law enforcement may conduct a search without a warrant.[235] Additionally, to further alleviate fears that Stingrays will be used in a manner contrary to the Fourth Amendment, exclusionary rules should be included that will prevent evidence illegally obtained to be later used in court proceedings.

The creation of Chapter 206A would balance both the interest of law enforcement investigations and the concerns of citizens that their rights are being violated under the Fourth Amendment. The exceptions and exclusionary rules created would allow law enforcement a wider latitude to use Stingrays in emergency situations, while also limiting them in their use of evidence collected if they go too far.

234. Smith v. Maryland, 442 U.S. 735, 742 (1979).
235. *Katz*, 389 U.S. at 357.

3. The Proposed Chapter Could be Used as a Guideline by State Legislatures to Create a Uniform National Standard for the Use of Stingrays

The creation of a new statutory standard for the application and use of Stingrays necessitates the creation of uniformity on the state level as well. By creating Chapter 206A, Congress would only initially be able to regulate federal law enforcement agencies. However, through the creation of these new statutory guidelines, Congress should encourage state legislatures to adopt them as their own state laws to promote a uniform national standard for the use of Stingrays.

Local and state law enforcement agencies have previously been assisted with purchasing Stingrays with federal money, so clearly these state agencies are using Stingrays for their own investigations.[236] Since these agencies are using these devices for their own investigations, Congress should encourage the uniform standard in all 50 states for three purposes: First, this would assist law enforcement officials in conducting investigations because they could apply the same standards anywhere in the country at the local, state, and federal levels. Next, it would promote judicial economy and expediency in resolving issues in court because judges would be familiar with the standard for any type of investigation and at any location. Finally, it would settle concerns of privacy advocates by creating one standard that all citizens would be able to understand, which will make government activities more open and trustworthy to the American people.

C. The Proposed Chapter Creates Certainty that the Current Policy Does Not

As previously discussed, the Department of Justice released a brand new policy in 2015 that completely reshaped the way that it would operate Stingrays through federal law enforcement agencies across the country.[237] This new policy requires sweeping changes on how Stingrays operate and how law enforcement officials apply to use them, including requirements that a probable cause warrant within the scope of Rule 41 of the Federal Rules of Criminal Procedure must first be secured.[238] However, there is still a problem

---

236. Jeremy Scahill & Margot Williams, *Stingrays: A Secret Catalogue of Government Gear for Spying on Your Cellphone*, THE INTERCEPT (Dec. 17, 2015, 11:23 AM), https://theintercept.com/2015/12/17/a-secret-catalogue-of-government-gear-for-spying-on-your-cellphone/; Larry Greenemeier, *State and Local Law Enforcement Agencies Across the U.S. are Setting Up Fake Cell Towers to Gather Mobile Data, but Few Will Admit It*, SCI. AM. (June 25, 2015), https://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-stingray-surveillance/.

237. U.S. DEP'T OF JUST., *supra* note 194.

238. *Id.* at 3.

with this method because this policy does not establish a Congressional or judicial legal standard with the force of law. Without a legal standard, the Department retains the authority to change their policies at any time. While the Department should remain flexible in adapting to changes in technology, a statutory standard would provide a much firmer basis for both the Department and the courts to follow when developing policies on the use of Stingrays. Further, the policy guidance applies only to federal law enforcement agencies;[239] there is currently no nationwide standard for local and state law enforcement agencies.[240]

Most of all, the new policy creates confusion when applied to current statutory law. Chapter 205 of Title 18 governs "Searches and Seizures" and general applications and orders related to Wiretap investigations.[241] Chapter 206 governs "Pen Registers and Trap and Trace Devices" and general applications and orders related to pen registers and trap and trace devices.[242] In the new policy implemented by the Department, Stingrays will be operated as pen registers, but applications must be based on probable cause within Rule 41 of the Federal Rules of Criminal Procedure.

This creates substantial confusion because it applies the standards under both Chapters 205 and 206, which require a "probable cause" standard and a "relevant to the criminal investigation" standard, respectively. Based on the application of these two standards, it is impossible to know which standard the courts should rely on. The Department created more questions by stating that Stingrays must be operated as pen registers, but then failed to explain why an application for use must be at a higher "probable cause" standard. It would be understandable if the new policy required a "relevancy" standard under Chapter 206, but the higher standard requirement does not fall in line with the new policy.

Based on the current confusion on the proper statutory and legal standards, it becomes necessary for Congress to establish a hard and fast rule on the use of Stingrays. This rule must be based on the language of the Fourth Amendment and current Supreme Court precedent, which has taken a drastic shift towards considering a suspect's "reasonable expectation of privacy." Additionally, the creation of a statutory standard for the use of Stingrays will also create a national standard that both the Department of Justice and the courts could follow. The proposed Chapter 206A – CELL-SITE SIMULATORS would do exactly that.

---

239. Kim Zetter, *New Bill Would Force Cops to Get Stingray Warrants*, WIRED (Nov. 3, 2015, 3:27 PM), https://www.wired.com/2015/11/new-bill-would-force-cops-to-get-warrants-before-spying-with-stingrays/.

240. SUBSENTIO, *State Surveillance Statutes*, http://www.subsentio.com/calea-affairs/state-surveillance-statutes/.

241. 18 U.S.C. §§ 3101-3118 (2012).

242. 18 U.S.C. §§ 3121-3127.

V. CONCLUSION

As the age of technology continues to advance in unprecedented ways, it becomes necessary for the law to continue to advance at the same rate or risk being left behind along with the rights of American citizens. Law enforcement officials in this country, at every level, are required to deal with some of the worst that mankind has to offer. Their job is truly dangerous and citizens owe a great deal to the men and women who protect and serve this country each and every day. Our system of laws should do everything it can to assist them in their pursuit of those that seek to do us harm, but with that awesome power comes responsibility. While we strive to find those that live outside the law, it is also our job to preserve that system of laws that makes America unique.

The Fourth Amendment serves as a protection and guarantee under which this great country was founded. While the 21st century continues to pose new problems for the law and its enforcement, we cannot let ourselves slide into a position that deprives us of our constitutional rights and what they stand for. Stingrays present a new challenge that both law enforcement and the American people should embrace while still safeguarding our rights against unreasonable searches and seizures in violation of the Fourth Amendment. The proposed legislation allows Americans to sleep peacefully at night, knowing that while law enforcement tracks and apprehends dangerous individuals, they will do so within the boundaries of the law.