Santa Clara University School of Law

Santa Clara Law Review

Volume 56 | Number 1 Article 5

2-4-2016

The Need for Fourth Amendment Protection from Government Use of Cell Site Simulators

Henry Bernstein

THE NEED FOR FOURTH AMENDMENT PROTECTION FROM GOVERNMENT USE OF CELL SITE SIMULATORS

Henry Bernstein*

TABLE OF CONTENTS

*J.D. Candidate, Santa Clara University School of Law, Class of 2016. Senior Articles Editor, Santa Clara Law Review.

INTRODUCTION

Today, cell phones are almost ubiquitous: much of the population uses and carries them daily.[1] Of course, this means criminals can use cell phones to facilitate their criminal enterprises.[2] Law enforcement, in turn, has adopted methods to effectively exploit cell phone usage data for surveillance purposes.

One such method is better known: compelling cell service providers, by court order, to pass along data stored by their cell towers. Known as cell site tracking, this data can be used to track a phone's past or present location.[3] Debate has raged over whether cell site tracking implicates the Fourth Amendment, and courts that have taken up the subject have come to different conclusions.[4]

Far less attention has been paid to another method of cell phone tracking: the use of cell site simulators, or "Stingrays." Despite their rising use, and the equal implications to the Fourth Amendment, little open debate surrounds the Stingray device. As of September 2015, no federal appellate court has taken up the issue. Yet, as Stringrays become better known and more widely used, the judiciary might play a greater role in regulating its use.

This Comment analyzes the Fourth Amendment implications of police use of the Stingray device. In comparing the Stingray device to traditional cell site tracking, this Comment highlights the differences between the two methods of cell phone tracking and argues that the use of Stingrays should be subject to a higher standard.

Part II of this Comment discusses the current legal

1. Riley v. California, 134 S. Ct. 2473, 2490 (2014).
2. *See id.* at 2493.
3. *See* discussion *infra* Part II.A.
4. *See* discussion *infra* Part II.C.

framework of cell site tracking. Part II.A discusses the statutory foundation the government uses to authorize cell site tracking. Part II.B analyzes the Supreme Court's Fourth Amendment jurisprudence relevant to the debate about cell site tracking, including two relatively recent decisions that may have a greater impact. Part II.C presents two federal appellate court decisions analyzing cell site tracking, both reaching different conclusions about its Fourth Amendment implications. Part II.D introduces the Stingray device and discusses both the technology behind the device and the current authority the device operates under.

Part III of this Comment outlines the problems arising from the current legal treatment of the Stingray device. Part IV discusses the differences between the Stingray and traditional cell site tracking and why these differences warrant different legal treatment for the Stingray device. Finally, Part V proposes that requiring a probable cause warrant before a Stingray device can be used adequately balances privacy concerns with those of law enforcement.

I. BACKGROUND

A. Cell-Site Location Information

1. Definition

Cell phones operate by periodically sending out signals, or "pings" to nearby cell towers.[5] These signals allow the phone to determine which cell towers to route incoming and outgoing calls through in order to receive the best reception.[6] In the process, the phone is constantly relaying its location to the nearest cell tower.[7] Every phone has a Mobile Identification Number (MIN)—the number that another user must dial to reach the phone—and a unique Electronic Serial Number (ESN) assigned by the manufacturer.[8] A cell phone

5. William Curtiss, Article, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistency Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139, 144. (2011).

6. *See* In re Application of the United States for Order for Prospective Cell Site Location Info., 460 F. Supp. 2d 448, 450 (S.D.N.Y. 2006).

7. *Id.* at 450.

8. Curtiss, *supra* note 5, at 165.

"registers" to a cellular network by relaying its MIN and ESN to nearby cell towers, giving preference to the tower with the strongest signal.[9] As the phone moves, it will continually rank the signal strength of nearby cell towers from strongest to weakest.[10] This information can reveal where the phone was located at the time of a call[11] and is known as cell-site location information (CSLI).

Cell service providers use CSLI to locate the phone within the cell network when it receives a call.[12] Providers generally store CSLI, as it is useful information.[13] The amount of CSLI stored and how long it is kept varies across providers, but almost all providers store accurate location information of its users.[14]

2. Statutory Authority

The statutory authority for the use of CSLI is drawn mainly from the Stored Communications Act ("the SCA")[15] and the Pen/Trap statute,[16] both part of the larger Electronic Communications Privacy Act.[17] The main hurdle faced by the government in its use and acquisition of CSLI is Federal Rule of Criminal Procedure 41 ("Fed. Cr. Rule 41"),[18] which requires a warrant based on probable cause for the use of "tracking devices."[19] This burden—probable cause—is higher than the burden required under the SCA or Pen/Trap Statute./ To bypass Fed. Cr. Rule 41, the government uses a combination of the SCA and the Pen/Trap statute to argue

9. Curtiss, *supra* note 5, at 165.

10. In re Application of the United States for Order for Prospective Cell Site Location Info., 460 F. Supp. 2d at 451.

11. Because cell phones register with multiple cell towers with any given signal, the varying signal strengths can be used to "triangulate" the location of the phone. *See id.* at 451.

12. *Id.*

13. For example, providers use location information to determine when roaming charges apply, and to track the volume of cell phone calls in a given area. *See id.*

14. *See id.*

15. 18 U.S.C. § 2703–12 (2014).

16. 18 U.S.C. § 3121–27 (2014).

17. The Electronic Communications Privacy Act was amended by the Communications Assistance for Law Enforcement Act (CALEA). 47 U.S.C. § 1001–10.

18. Fed. R. Crim. P. 41(e)(2)(C).

19. *Id.*

that a warrant is not required for the acquisition of CSLI, despite its use in tracking individuals.[20]

a. Stored Communications Act

The SCA[21] allows a governmental entity to "require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service" if the government "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[22]

The government's position, in arguing that the SCA allows for the collection of CSLI, is that such data falls under the definition of a "record."[23] Under this interpretation, the SCA permits the collection of CSLI pursuant to a court order after a showing of Specific and Articulable facts, rather than a warrant based on probable cause as required for tracking devices.

b. Pen/Trap Statute

The Pen/Trap statute[24] was enacted in response to a Supreme Court decision holding that individuals have no reasonable expectation of privacy in the telephone numbers that they dial.[25] Following the decision, Congress saw a need to protect against the indiscriminate use of surveillance and recording devices, and thus enacted the Pen/Trap statute.[26] Under the statute, an application for an order granting the use of a pen/trap device[27] requires the applicant to certify that

20. *See* discussion *infra* Part II.A.2.c.

21. 18 U.S.C. § 2703–12.

22. 18 U.S.C. § 2703(c)–(d). This standard will be referred to as "Specific and Articulable facts."

23. *See* discussion *infra* Part II.A.2.c.

24. 18 U.S.C. § 3121–27.

25. Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

26. Curtiss, *supra* note 5, at 147.

27. A "pen register" is a device that records the telephone numbers of calls made from a particular phone line (*i.e.*, all outgoing numbers). *See* 18 U.S.C § 3127 (3). Conversely, a "trap/trace" device records all incoming numbers to a particular phone line. 18 U.S.C. § 3127 (4).

the information sought is reasonably likely to be relevant to an ongoing criminal investigation.[28] This is a low burden to meet, as courts merely rely on the certification itself, not the facts supporting it.[29]

c. Hybrid Theory

The government has relied on a combination of the SCA and the Pen/Trap statute in order to sidestep Fed. Cr. Rule 41, thus bypassing the requirement for a warrant for the use and acquisition of CSLI.[30] The Communications Assistance for Law Enforcement Act[31] states that information that may disclose the physical location of the subscriber cannot be acquired solely by use of a Pen/Trap order.[32] The government interprets this language to mean that a Pen/Trap order, combined with the authority from the SCA, is sufficient to acquire location information.[33] The SCA does allow subscriber information to be acquired, albeit on a showing of Specific and Articulable facts that the information is likely to be relevant to an ongoing criminal investigation.[34] The government's position is that this heightened standard of proof is sufficient to allow the court to grant an order for the collection of CSLI.[35]

The essence of the Hybrid Theory is that the Pen/Trap statute and the SCA together can allow what neither statute

---

28. 18 U.S.C. § 3122(b)(2).

29. *See* Curtiss, *supra* note 5, at 148.

30. *See id.* at 149; *See also* In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (analyzing the Hybrid Theory relied upon by the government in an application to obtain cell site location information).

31. 47 U.S.C. § 1001–10.

32. 47 U.S.C. § 1002(a)(2) (2014).

33. *See* In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d at 315 ("The government . . . vigorously contends that an application made under the SCA and the Pen/Trap Statute together accomplishes what separate applications under each statute might not.") For ease of reference, I will call this argument the "Hybrid Theory."

34. *See* discussion *infra* Part II.A.2.a.

35. *See* Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d at 315.

can alone: the collection of CSLI.[36] But this theory also rests on several assumptions and interpretations.[37] First, as mentioned above, the government interprets CSLI as a "record" and is thus governed by the SCA. Second, any use of tracking devices is covered by Fed. Cr. Rule 41, requiring a warrant.[38] Thus, the government characterizes CSLI as a "communication," requiring less than probable cause.[39]

B. Supreme Court and 4th Amendment Protections

In addition to statutory requirements, the collection of CLSI must also meet the requirements of the Fourth Amendment to the Constitution of the United States. The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,"[40] except on a showing of probable cause (upon which a warrant is issued). Below, several Fourth Amendment doctrines relevant to the discussion of Stingrays and CSLI[41] are discussed, as well as two relatively recent decisions that are likely to impact the debate in the future.

1. Third Party Doctrine

The third party doctrine stands for the principle that an individual has no expectation of privacy, and thus, no Fourth Amendment protection, in information voluntarily disclosed to a third party.[42] The basis of this doctrine is that the individual, in disclosing information to a third party, has assumed the risk that the third party might in turn disclose

---

36. *Id.*

37. *Id.* at 316 ("Although the essence of the hybrid theory is that two statutes together accomplish what neither can alone, the argument more precisely rests on a complex chain of inferences derived from several different legislative enactments . . . .").

38. Fed. R. Crim. P. 41.

39. For a more in-depth discussion of various courts' treatment of the Hybrid Theory, *see* Curtiss, *supra* note 5, at 149–56.

40. U.S. Const. amend. IV.

41. While CLSI collection and the use of the Stingray device have many parallels, they differ in important ways. See, infra, section III. D.

42. *See*, *e.g.*, United States v. Miller, 425 U.S. 435, 442–43 (1976)(holding that a bank depositor has no expectation of privacy in information he voluntarily conveyed to banks and their employees).

that information to the government.[43] An example of this doctrine is *Smith v. Maryland,*[44] where the Court held that an individual has no expectation of privacy in a telephone number voluntarily conveyed to a phone company in order to make a call.[45]

2. Knotts/Karo *and the Public/Private Distinction*

Smith v. Maryland established that an individual has no reasonable expectation of privacy in outgoing telephone numbers that he or she dials.[46] But when information is used to track an individual's location, the Supreme Court has shown greater concern for privacy. In 1983 the Supreme Court held in *United States v. Knotts* that an individual "in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[47] In 1984—only one year later—the Court explained in *United States v. Karo* that using a tracking device to monitor an individual in a private residence would violate the Fourth Amendment if not undertaken pursuant to a warrant and on a showing of probable cause.[48]

Thus, *Knotts* and *Karo* draw a distinction between public and private places. Courts generally follow this rule: for example, an individual can generally be tracked on public streets without a warrant. However, once tracking begins to focus on an individual's movements in a private place, the Fourth Amendment applies, and a warrant is needed.[49] The problem courts face in the context of CSLI is determining exactly when this distinction applies.

---

43. *Id.* at 443. ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

44. Smith v. Maryland, 442 U.S. 735 (1979).

45. *Id.* at 745–46.

46. *Id.* at 742.

47. United States v. Knotts, 460 U.S. 276, 281 (1983).

48. *Karo* was distinguished from *Knotts* on the basis that the,police in Karo used a GPS device to track a barrel as it moved from a highway to a private warehouse, without any accompanying visual surveillance. It was this shift to tracking movement in a "private" area that violated the Fourth Amendment. United States v. Karo, 468 U.S. 705, 714–15 (1984).

49. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511–12 (1961) (holding that the use of a surveillance device that penetrated the wall of a defendant's home violated the Fourth Amendment).

3. Reasonable Expectation of Privacy

A more basic doctrine relating to the collection and use of CLSI is the doctrine of a reasonable expectation of privacy. This doctrine stands for the proposition that the Fourth Amendment protects an individual where he has a subjective expectation of privacy in a situation or piece of information, and society recognizes the expectation as an objectively reasonable one.[50] The basic rule was established by *Katz v. United States*.[51] There, the Supreme Court analyzed police action in recording a conversation taking place within a phone booth.[52] The Court ultimately held that because the defendant, and society at large, would reasonably expect privacy in the phone booth, the government intrusion required a warrant.[53] Thus, under this doctrine, if one has a reasonable expectation of privacy in a situation or piece of information, the Fourth Amendment protects him or her.

The Court later distinguished this test in *Kyllo v. United States*.[54] There, the Court examined police use of thermal imaging technology to survey a private residence.[55] Applying the reasonable expectation of privacy test, the Court held that the warrantless search violated the Fourth Amendment.[56] Importantly, the Court reasoned in part that the fact that technology was not in general public use made a societal expectation of privacy more reasonable.[57]

4. GPS Trackers: United States v. Jones

The decision in *United States v. Jones*[58] also carries implications for the collection of CLSI. *Jones* involved the installation of a GPS tracking device by police onto the undercarriage of the defendant's car while it was parked in a public parking lot.[59] Although the police applied for and was granted a warrant to attach the device, the government

50. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. Concurring).
51. *Id.* at 350.
52. *Id.* at 354.
53. *Id.* at 360–61 (Harlan, J. concurring).
54. Kylio v. United States, 533 U.S. 27 (2001).
55. *Id.* at 40.
56. *Id.*
57. *Id.*
58. United States v. Jones, 132 S. Ct. 945 (2012).
59. *Id.* at 948.

admitted that the police did not comply with the terms of the warrant.[60] Thus, the Court's analysis treated the use of the GPS tracker as warrantless.[61]

In a unanimous decision, the Court held that placing the GPS on the defendant's car violated the Fourth Amendment.[62] The majority opinion, written by Justice Scalia, declared that because police physically trespassed on defendant's property to place the tracking device, the *Katz* analysis did not apply.[63] Instead, the majority noted that historically "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[64] Because the Fourth Amendment still provides protection against physical trespass by the government,[65] the majority concluded that the police placing the tracking device on the defendant's property violated the Fourth Amendment.[66]

The two concurrences, however, did discuss the *Katz* analysis. While not binding, these concurrences highlight many of the same concerns that are present where police use Stingray devices[67]. Justice Sotomayor wrote separately to discuss how *Katz* would bear on the case.[68] Justice Sotomayor noted that "physical intrusion is now unnecessary to many forms of surveillance,"[69] and that "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority

---

60. *Id.* at 948. The warrant authorized installation of the device within ten days and in the District of Columbia, but police attached it eleven days later, in Maryland.

61. *See id.*

62. *Id.* at 947, 949, 954.

63. United States v. Jones, 132 S. Ct. 945, 950 (2012) (holding that "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

64. *Id.*

65. *See id.* at 952 ("But as we have discussed, the Katz reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

66. *Id.* at 953.

67. *See infra* part III. A for an in depth discussion of the concerns raised by the use of Stingrays.

68. United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

69. *Id.* (Sotomayor, J., concurring).

opinion's trespassory test may provide little guidance."[70]

Further, Justice Sotomayor argued that GPS monitoring carries unique privacy concerns because it "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[71] Because of the unique nature of GPS monitoring, Justice Sotomayor questioned whether people reasonably expect that the sum of their movements in public will be aggregated and analyzed extensively by the government.[72]

Finally, Justice Sotomayor questioned the applicability of the third party rule in the digital age.[73] Justice Sotomayor reasoned that in today's digital age, a great deal of personal information is disclosed to third parties.[74] Justice Sotomayor concluded by stating that it should not be assumed that "all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[75]

Writing for the second concurrence, Justice Alito stressed that the degree of intrusion is what should determine whether the Fourth Amendment was violated.[76] Justice Alito lamented the fact that "the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be

---

70. *Id.* (Sotomayor, J., concurring).

71. *Id*. (Sotomayor, J., concurring). The notion that separate, less significant pieces of information may be combined to implicate the Fourth Amendment is known as the mosaic theory. For a more in-depth discussion and criticism of the mosaic theory, *see* Orin Kerr, *Article: The Mosaic Theory of The Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

72. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on.").

73. *Id.* at 957. (Sotomayor, J., concurring).

74. *Id.* (Sotomayor, J., concurring) ("This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.").

75. *Id.* (Sotomayor, J., concurring).

76. United States v. Jones, 132 S. Ct. 945, 961 (2012) (Alito, J., Concurring) ("[T]he Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) . . . .").

tracked."[77] In particular, Justice Alito noted that "cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . ."[78] Justice Alito concluded that, instead of the majority opinion's trespass test, the defining question should be "whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[79]

5. *Cell Phones:* Riley v. California

Another important case is *Riley v. California*.[80] While *Riley*, like *Jones*, has no direct bearing on the CSLI/Stingray debate, it illustrates how the Supreme Court views Fourth Amendment protections in the digital age. In *Riley*, the defendant was arrested for possession of concealed and loaded firearms.[81] Police searched the defendant incident to his arrest and seized his cell phone, which had "a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."[82] Examining the contents of the phone, police discovered photographs implicating the defendant in an earlier shooting.[83] Using this evidence, the defendant was charged with that shooting.[84]

In a unanimous decision, the Court held that such a search violates the Fourth Amendment.[85] Even more relevant to this Comment is the *Riley* Court's treatment of cell phones. First, the Court explicitly recognized the importance and pervasiveness of cell phones in daily life.[86] Second, the Court recognized that cell phones could be used to track where an individual has been, using historic location information stored within the phone.[87] The Court concluded

77. *Id.* at 962.
78. *Id.* at 963.
79. *Id.* at 964.
80. Riley v. California, 134 S. Ct. 2473 (2014).
81. *Id.* at 2480.
82. *Id.*
83. *Id.* at 2481.
84. *Id.*
85. Riley v. California, 134 S. Ct. 2473, 2495 (2014).
86. *Id.* at 2484. ("[Cell phones] are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.").
87. *Id.* at 2490. ("Data on a cell phone can also reveal where a person has

that because a cell phone contains such a density of information, a warrant is required to search one even if the search occurs incident to the owner's arrest.[88]

C. Differing Treatment of CSLI in the Circuit Courts

As of September 2015, no appellate level court has addressed the use of Stingray devices. However, the use of CSLI for traditional cell-site tracking has been addressed, and is relevant to the debate over the use of Stingrays. Currently, the two most prominent and recent cases have been from the Sixth and Eleventh Circuits..[89]

1. United States v. Skinner

The Sixth Circuit examined the use of CSLI in *United States v. Skinner*.[90] *Skinner* involved police using CSLI to track and intercept the defendant, as he transported drugs between Arizona and Tennessee.[91] Police obtained an order authorizing Skinner's phone company to release his subscriber information, cell-site information, and GPS information.[92] This allowed police to track Skinner's location as he traveled along interstate highways.[93] Police used this data to locate Skinner's motorhome in a Texas truck stop.[94] After searching the motorhome, police discovered 1,100 pounds of marijuana.[95]

---

been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

88. *Id.* at 2493.

89. These cases are not the only federal appellate level cases to deal with CSLI and cell site tracking. *See*, *e.g.*, In re United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (holding that CSLI does not automatically implicate the Fourth Amendment); *See also* In re Application of the United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (holding that requiring specific articulable facts for CSLI did not violate the Fourth Amendment). However, the cases discussed in this Comment have had the opportunity to review CSLI in light of the *Jones* decision, and are more relevant to the scope of this Comment.

90. 690 F.3d 772 (6th Cir. 2012).

91. *Id.* at 776.

92. *Id.*

93. *Id.*

94. *Id.*

95. United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012).

The Sixth Circuit held that police use of Skinner's CSLI to track his movements along public highways did not violate the Fourth Amendment.[96] Citing *Knotts*, the court held that because the CSLI revealed only public information, *i.e.* Skinner's location along public highways, Skinner had no reasonable expectation of privacy in this information.[97]

The court also compared the case to *Karo*. The court reasoned that, just as the defendant in *Karo* received the barrel with the tracking device included, Skinner had obtained the cell phone with GPS technology included.[98] Thus, he could not object to its use by police.[99]

Finally, the court distinguished the case from *Jones*, concluding that because no physical trespass occurred, *Jones* did not apply.[100] Interestingly, the court cited to Justice Sotomayor's concurrence, in which she opined that the digital age has outpaced the third party doctrine and the *Knotts*/*Karo* public/private distinction:[101] the same doctrines relied on by the Sixth Circuit in deciding *Skinner*. The court also discussed Justice Alito's concurrence in *Jones*.[102] The court seemingly accepted the notion that the extent of surveillance can have a bearing on whether or not that surveillance is constitutional.[103] However, the court concluded that this concern did not apply. Comparing the twenty-eight days of surveillance in *Jones* with the three days of surveillance of *Skinner*, the court concluded that "[n]o such extreme comprehensive tracking is present in this case."[104]

---

96. *Id.* at 778.

97. *Id.* ("There is no inherent constitutional difference between trailing a defendant and tracking him via such technology.").

98. *Id.* at 781.

99. *Id.*

100. United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012) ("*Jones* does not apply to Skinner's case because, as Justice Sotomayor stated in her concurrence, 'the majority opinion's trespassory test' provides little guidance on 'cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property.'" (quoting *United States v. Jones*, 132 S. Ct. 945, 955 (Sotomayor, J., concurring)).

101. *See* discussion *infra* Part II.B.4.

102. *Skinner*, 690 F.3d at 780.

103. *Id.* ("There may be situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.").

104. *Id.*

Ultimately the Sixth Circuit held that because Skinner voluntarily accepted a phone with GPS capabilities, and traveled along public roads, the police making use of CLSI to track him was not a violation of the Fourth Amendment.[105]

2. United States v. Davis

United States v. Davis[106] provides an alternate view.[107] In *Davis*, the defendant, was convicted on several counts of armed robbery.[108] At trial, the prosecution introduced records from cell phone service providers that Davis "had placed and received cell phone calls in close proximity to the locations of each of the charged robberies around the time that the robberies were committed . . . ."[109] Because this information was obtained without a warrant,[110] Davis argued on appeal that the information violated his Fourth Amendment rights.[111]

The Eleventh Circuit held that CSLI "is within [a] subscriber's reasonable expectation of privacy."[112] The court began by discussing *Jones*.[113] Unlike the court in *Skinner*, the Eleventh Circuit held that *Jones* implicitly endorsed the application of the privacy theory to electronic information.[114] The court then determined that unlike GPS data gathered on a public highway, CSLI is more private in nature, whether or not its collection creates a sufficient "mosaic" to expose that

105. *Skinner*, 690 F.3d at 777.

106. United States v. Davis, 754 F.3d 1205 (11th Cir. 2014).

107. The *Davis* decision has since been vacated pending a rehearing en banc. Yet while not binding authority, it is useful in providing an alternative view of how courts treat CSLI.

108. *Davis*, 754 F.3d at 1209.

109. *Id.* at 1209–10.

110. *Id.* at 1210. The information was obtained pursuant to the SCA, specifically, U.S.C.A. § 2703 (d), which requires only an offer of "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." *See* discussion *infra* Part II.2.a.

111. United States v. Davis, 754 F.3d 1205, 1210 (11th Cir. 2014).

112. *Id.* at 1217.

113. *Id.* at 1213.

114. *See id*. ("In light of the confluence of the three opinions in the Supreme Court's decision in *Jones*, we accept the proposition that the privacy theory is not only alive and well, but available to govern electronic information of search and seizure in the absence of trespass.").

which otherwise would be private.[115]

The Eleventh Circuit also rejected the argument that disclosure of CSLI is inherently voluntary, and thus, unprotected under *Maryland v. Smith*.[116] The court conceded that in placing a call, a subscriber voluntarily discloses the number that is called.[117] However, it is unlikely that most subscribers realize that they are also disclosing their location, making such disclosure involuntary.[118] Further, a subscriber who merely answers a call has not voluntarily disclosed any information.[119] Thus, the Eleventh Circuit held that a reasonable expectation of privacy exists in one's CSLI.[120]

D. Stingray Devices and Their Place in the Current Legal Framework

1. Definition and Workings

Stingrays[121] (the name derives from a popular manufacturer of the device), also known as cell site simulators or International Mobile Subscription Identity (IMSI) Catchers, take advantage of the same underlying features of cell phones as traditional cell site tracking.[122]

---

115. *Id.* at 1216. ("One's cell phone, unlike an automobile, can accompany its owner anywhere. Thus, the exposure of the cell site location information can convert what would otherwise be a private event into a public one. When one's whereabouts are not public, then one may have a reasonable expectation of privacy in those whereabouts. Therefore, while it may be the case that even in light of the *Jones* opinion, GPS location information on an automobile would be protected only in the case of aggregated data, even one point of cell site location data can be within a reasonable expectation of privacy.").

116. United States v. Davis, 754 F.3d 1205, 1216–17 (11th Cir. 2014).

117. *Id.* at 1217.

118. *Id.*

119. *Id.*

120. *Id.* at 1215. However, the court did not exclude evidence gathered by the Stingray, because the officers had acted in good faith reliance on a court order and thus, the "good faith" exception to the exclusionary rule applied. *See Davis*, 754 F.3d at 1217–18 (citing United States v. Leon, 468 U.S. 897 (1984)).

121. Devlin Barrett, *American's Cell Phones Targeted in Secret U.S. Spy Program*, WALL STREET JOURNAL, (Nov. 13, 2014), http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

122. U.S. Department of Justice, ELECTRONIC SURVEILLANCE MANUAL 38-40 (2005), *available at* http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf. This manual is dated, and its procedural aspects cannot be relied upon as the law has changed. Despite this, it is still useful in detailing the underlying operation of the Stingray device.

Stingrays operate by imitating a cell tower.[123] To a cell phone, the Stingray appears to have the strongest and nearest signal, compelling the phone to register with the device.[124] When registering, the phone sends location information, as well as identifying information such as the ESN and the MIN.[125]

Using data that a target phone sends when it registers, the phone's location can be revealed.[126] The government has closely guarded information about its use Stingrays, so it is difficult to determine exactly how accurate they are.[127] Evidence of how Stingrays are being used has led some to estimate that the device is comparably accurate, and perhaps more so, than traditional cell site tracking.[128]

Not only can a Stingray track a target phone, but because it acquires data directly from the phone, it can be used to identify that phone's number as well.[129] In addition, Stingrays can intercept the contents of a call,[130] but because this almost certainly falls under the Fourth Amendment as a wiretap, police must configure the device to disable this capability.[131] In effect, the Stingray combines the features of many surveillance tools into one package. It is capable of: (1) acquiring CSLI and tracking the location of a phone in real time[132]; (2) identifying a target's phone number;[133] and (3) obtaining outgoing and incoming call information like a Pen/

123. *See* Barrett, *supra* note 121.

124. *See* Barrett, *supra* note 121; *See also* U.S. Department of Justice, *supra* note 122, at 40 (stating that Stingrays will "electronically force a cellular telephone to register [with the device]. . .").

125. U.S. Department of Justice, *supra* note 122, at 40.

126. U.S. Department of Justice, *supra* note 122, at 40.

127. For example, in a notable case in Florida, during appeal it was revealed that police used the Stingray device around 200 times without disclosing this to the court. Police claimed that a non-disclosure agreement signed with the manufacturer prevented them from disclosing their use of the device, even to the court. *See* Kim Zetter, *Florida Cops Secret Weapon: Warrantless Cell Phone Tracking*, WIRED,, (Mar. 3, 2014), http://www.wired.com/2014/03/stingray/.

128. Curtiss, *supra* note 5, at 166.

129. U.S. Department of Justice, *supra* note 122, at 40. This is unlike traditional cell site tracking, where advance knowledge of the target phone number is needed before CSLI can be acquired from cell providers.

130. U.S. Department of Justice, *supra* note 122, at 41.

131. U.S. Department of Justice, *supra* note 122, at 41.

132. U.S. Department of Justice, *supra* note 122, at 40.

133. U.S. Department of Justice, *supra* note 122, at 40.

Trap device.[134] Further, it acquires this information directly, so cell service providers do not need to be compelled to cooperate.[135]

Unsurprisingly for such a useful device, use of Stingrays is reportedly on the rise: police can use vehicles and planes[136] to transport the device, creating a highly mobile surveillance tool. Yet details about the device are scarce, not least because of the government's secrecy surrounding the device.[137]

2. Statutory Authority for use of the Stingray

The USA PATRIOT Act of 2001[138] revised the Pen/Trap statute to include "signaling information," which the Department of Justice construes as permitting the collection of cell phone registration "pings."[139] Thus, generally the government will seek a pen/trap order before using the device.[140] However, many of these orders are under seal, and it is unclear what level of specificity police are using when obtaining a court order to use a Stingray, and in some cases it seems unlikely that the court has been made fully aware of the scope of an order that police are seeking.[141] For example, in Tacoma, Washington, superior court judges unwittingly

---

134. U.S. Department of Justice, *supra* note 122, at 39–40.

135. U.S. Department of Justice, *supra* note 122, at 41.

136. *See* Jon Campbell, *LAPD Spied on 21 Using StingRay Anti-Terrorism Tool*, LA WEEKLY NEWS, http://www.laweekly.com/news/lapd-spied-on-21-using-stingray-anti-terrorism-tool-2612739, (discussing LAPD use of the Stingray over four-month period); *See also* Barrett, *supra* note 121 (discussing Department of Justice use of a Stingray-like device attached to a small fixed wing aircraft and then flown above urban areas).

137. *See* Justin Fenton, *Judge threatens detective with contempt for declining to reveal cellphone tracking methods*, THE BALTIMOR SUN, http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html (discussing prosecutors abandoning evidence rather than reveal details about how or if the Stingray device was used in locating a suspect).

138. UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) ACT OF 2001, 107 P.L. 56, 115 Stat. 272.

139. *See* Curtiss, *supra* note 5, at 167; *See also* U.S. Department of Justice, *supra* note 122, at 41.

140. U.S. Department of Justice, *supra* note 122, at 41–48.

141. *See e.g.*, Barrett, *supra* note 121 ("Christopher Soghoian, chief technologist at the American Civil Liberties Union, called it 'a dragnet surveillance program. It's inexcusable and *it's likely—to the extent judges are authorizing it—[that] they have no idea of the scale of it*.'" (emphasis added)).

signed over 170 pen/trap orders that police used as authorization to use a Stingray.[142] The judges first learned that they were authorizing the use of a Stingray device in those orders when a newspaper reported on it.[143]

Recently, it appears that the Federal Bureau of Investigation has enacted a policy that requires a warrant to be obtained before a Stingray is used.[144] However, the FBI leaves a broad exception for use of the device in public areas[145] and in any event local police departments are not bound by the policies of the FBI.

II. IDENTIFICATION OF LEGAL PROBLEM

Applying the Fourth Amendment to the use of Stingrays is far from the neatest solution. For one, there is a complete lack of any direct precedent involving Stingrays. The nearest analogy comes in the form of cases involving CSLI acquired under the SCA or Pen/Trap statutes, and even then, judicial treatment of CSLI is muddled.[146]

Further, the use of Stingrays is likely an issue best suited for the legislature.[147] This is complicated, however, by the fact that the government closely guards any information about the Stingray device.[148] Recently, at least two Senators

---

142. Adam Lynn, *Tacoma police change how they seek permission to use cellphone tracker*, THE NEWS TRIBUNE (Nov. 15, 2014), http://www.thenewstribune.com/news/local/crime/article25894096.html.

143. *Id.*

144. This policy was revealed by FBI officials in private briefings with staff of Senators Chuck Grassley and Patrick Leahy, after the Senators sought information regarding the use of Stingrays. *Leahy and Grassley Press Administration on Use of Cell Phone Tracking Program*, (12/31/2014), http://www.grassley.senate.gov/news/news-releases/leahy-grassley-press-administration-use-cell-phone-tracking-program.

145. *Id.* "For example, we understand that the FBI's new policy requires FBI agents to obtain a search warrant whenever a cell-site simulator is used as part of a FBI investigation or operation, unless one of several exceptions apply, including (among others): (1) cases that pose an imminent danger to public safety, (2) cases that involve a fugitive, or (3) cases in which the technology is used in public places or other locations at which the FBI deems there is no reasonable expectation of privacy."

146. *See infra* Part I.C.

147. *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

148. *See* Fenton, *supra* note 137; *See also* Lynn, *supra* note 142.

have taken an interest in the device and questioned law enforcement officials on its use, but it is unclear where this will lead.[149]

Currently, the government's ability to use the Stingray device is only constrained by having to seek a pen/trap order, which might not provide sufficient protection.[150] Further, using a pen/trap order as sufficient for both CSLI and Stingrays ignores the inherent differences between the two tracking methods.[151] Because police do not have to work with cell service providers to acquire information, the SCA does not apply.[152] The general lack of awareness of the Stingray in the media and the public, along with the government's secrecy regarding the device, makes it unlikely that any uniform legislative guidance will arise soon. Therefore, if the use of Stingrays is to be effectively governed, it must fall on the judiciary to determine if such use violates the Fourth Amendment.

III. ANALYSIS

A. Applicability of Current CSLI Analysis to Stingrays

Even if *Skinner* and *Davis* gave definitive rules on CSLI, both cases dealt with law enforcement acquiring CSLI from cell service providers, pursuant to a court order.[153] The use of Stingrays is quite different, as the CSLI is acquired directly from the subscriber, without having to involve the cell service provider.[154] Thus, the same arguments regarding whether Fourth Amendment protection exists for CSLI should not be used to analyze devices like the Stingray.

1. Third Party Doctrine

One argument against there being a reasonable expectation of privacy in the context of traditional cell site

149. *See Leahy and Grassley Press Administration on Use of Cell Phone Tracking Program, supra* note 144 and accompanying text.

150. *See* Lynn, *supra* note 142.

151. *See* discussion *infra* Part III.

152. *See* discussion Part III.A.1.

153. *See* United States v. Davis, 754 F.3d 1205, 1210 (11th Cir. 2014); *See also* United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012).

154. U.S. Department of Justice, *supra* note 122, at 41.

tracking is that a subscriber who places a call on a cell phone is voluntarily disclosing his CSLI to the cell provider, thus waiving his Fourth Amendment protection.[155] This argument is generally based on the third-party doctrine, proposing that an individual has no reasonable expectation of privacy in information that is voluntarily disclosed to a third party.[156] The strongest example comes from *Smith v. Maryland,*[157] where the Supreme Court held that no reasonable expectation of privacy exists in a telephone number that is voluntarily conveyed to the a phone company to make a call.[158] The principle of the doctrine is that one who voluntarily discloses otherwise protected information to a third party voluntarily assumes the risk that the information will become unprotected or public.[159] In the context of CLSI, some courts have held that a user no longer has an expectation of privacy in his location information once it is disclosed to cell service providers.[160]

This argument simply does not apply to the use of a Stingray. While cell phones do convey information to third-party service providers, this is not the information that Stingrays collect.[161] Stingrays acquire data directly from the target phone, circumventing the cell service provider and eliminating the third party altogether.[162] Therefore, when discussing the use of a Stingray, the argument that a cell phone user has disclosed information to a third-party is defeated by the fact that no third-party is involved.

Further, the notion that a cell phone user assumes the risk of third party disclosure of his location information does not apply to Stingrays. By design, Stingrays are far more proactive than cell site tracking. The DOJ manual speaks of "forcing" the target phone to register with the device as the

155. *See, e.g.*, United States v. Skinner, 690 F.3d at 778.
156. *See* discussion *infra* Part II.B.3.
157. Smith v. Maryland, 442 U.S. 735 (1979).
158. *Id.* at 745–46.
159. *See* discussion *supra* Part II.B.3.
160. United States v. Skinner, 690 F.3d at 778 ("Similar reasoning [as Smith v. Maryland] compels the conclusion here that Skinner did not have a reasonable expectation of privacy in the location of his cell phone while traveling on public thoroughfares.").
161. U.S. Department of Justice, *supra* note 122, at 40–41.
162. U.S. Department of Justice, *supra* note 122, at 41.

phone believes it to be a genuine cell tower.[163] Cell phones automatically transmit CSLI to the Stingray, without any action from the user[164] (aside from possessing a phone and having it switched on). Thus, rather than passively collecting data as it is turned over to a third party, Stingrays actively force users to reveal information.[165] In such a situation there is no assumption of the risk on the part of the user, and so the third party doctrine does not apply to the use of a Stingray.

2. Knotts/Karo

The *Knotts/Karo* analysis, inquiring into whether a search penetrated into the private sphere, is often discussed in cases involving cell phone tracking.[166] Proponents of this view assert that tracking an individual's movements in public, where he could be visually tracked by law enforcement without a warrant, does not penetrate into the private sphere.[167] This argument has been criticized in the context of cell site tracking, because cell site tracking is far more accurate than the tracking devices in *Knotts* and *Karo*.[168] The same argument is even stronger applied to Stingrays.

First, there is evidence that Stingrays are at least as accurate, if not more so, than traditional cell site tracking.[169] Further, as the underlying technology continues to improve, Stingrays will only become more accurate. Where an individual can be tracked so precisely, there is a far greater

---

163. U.S. Department of Justice, *supra* note 122, at 40 (A cell site simulator . . . can *electronically force* a cellular telephone to register [with the device]." (emphasis added)).

164. U.S. Department of Justice, *supra* note 122, at 40–41 ("The necessary signaling data (ESN/MIN,channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on.").

165. U.S. Department of Justice, *supra* note 122, at 40–41.

166. *See, e.g.*, United States v. Skinner, 690 F.3d at 777.

167. *See id*. at 778 (holding that "[w]hile the cell site information aided the police in determining Skinner's location, that same information could have been obtained through visual surveillance.").

168. *See* Curtiss, *supra* note 5, at 173; *See also Riley v. California*, 134 S. Ct. 2473, 2490 (2014) ("Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

169. *See* Curtiss, *supra* note 5, at 166.

risk that the use of a Stingray will penetrate into the private sphere.[170]

Beyond the increased accuracy of the devices, the analogy to visual surveillance in public that *Knotts/Karo* relies on is an inaccurate portrayal of how Stingray devices work. Stingrays simply function differently than the tracker used in *Knotts*. Rather than simply tracking a specific target, a Stingray can both find the target phone and force it to reveal its location.[171] This is more intrusive than merely following an individual on a public road, in the sense that a Stingray not only tracks a targets location but can identify a target as well. Thus, the analogy to visual surveillance in public is not accurate.

3. Reasonable Expectation of Privacy

Following the *Katz v. United States* decision,[172] the "reasonable expectation of privacy" test has become a central inquiry into Fourth Amendment issues.[173] The basic rule is that the Fourth Amendment applies if an individual had a subjective expectation of privacy in a location or situation, and if society as a whole recognizes that expectation as objectively reasonable.[174] This rule was expanded on in *Kyllo v. United States,*[175]where the Court examined the use of thermal imaging technology to monitor a private residence. The Court held that society's objective understanding of what is reasonable was shaped by the fact that thermal imaging technology was not in general public use.[176]

The *Kyllo* analysis is particularly relevant when analyzing use of the Stingray. Stingrays are not in general public use,[177] and are not within society's reasonable expectations. It has been argued that with the growing use of smart phones and location-based technology, the average user

170. *See* Curtiss, *supra* note 5, at 173.
171. U.S. Department of Justice, *supra* note 122, at 40.
172. Katz v. United States, 389 U.S. 347 (1967).
173. *See* discussion *supra* Part.II.B.3.
174. *Katz*, 389 U.S. at 361 (Harlan, J. concurring) (1967).
175. Kyllo v. United States, 533 U.S. 27 (2001).
176. *Id.* at 40.
177. Just as with the thermal imaging technology in *Kyllo*, the inquiry is not actually focused on raw usage of the device, but whether the public generally knows of the device. *See Kyllo*, 533 U.S. at 34.

knows that cell phones innately convey location information.[178] Even so, the specifics of how Stingrays work are not general knowledge to either the media or the general public.[179] In fact, the government has been notably tight-lipped about disclosing any details about its use of Stingray devices or about how the devices function.[180] Given this, Stingrays could be seen as outside society's reasonable expectations.

This view is reinforced with the recent decisions of *Jones* and *Riley*. In her concurrence in *Jones*, Justice Sotomayor questioned "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[181] Though *Jones* involved a GPS tracking device,[182] Justice Sotomayor's concern is even more relevant to the use of Stingrays. Unlike a GPS unit attached to a car, a Stingray can track an individual wherever he goes, even within a particular room of a building, so long as he has his cellular phone with him.[183] Thus, even if people might have a general

178. *See* Orin Kerr, *Cell Phones, Magic Boxes and the Fourth Amendment*, THE VOLOKH CONSPIRACY (Nov. 8, 2010, 6:05 PM), http://volokh.com/2010/11/08/cell-phones-magic-boxes-and-the-fourth-amendment/ ; *See also* United States v. Skinner, 690 F.3d 772, 781 (6th Cir. 2012) (holding that Skinner knew his phone was GPS enabled when he obtained it and thus did not have a reasonable expectation of privacy in his location information).

179. Only recently, with a spate of public records requests, has the use of the device been under real scrutiny from the public. *See* Hanni Fakhoury, *Stingrays Go Mainstream: 2014 in Review*, ELECTRONIC FRONTIER FOUNDATION, (Jan. 2, 2015), https://www.eff.org/deeplinks/2015/01/2014-review-stingrays-go-mainstream.

180. *See* Fenton, *supra* note 137; *See also* Lynn, *supra* note 142.

181. United States v. Jones 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

182. *Id.* at 948.

183. Courts have recognized that the increased role cell phones play in people's lives increases the concerns surrounding their privacy. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (noting that cell phones and their users are rarely apart: "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception. According to one poll, nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower."); *See also* United States v. Davis, 754 F.3d 1205, 1216 (11th Cir. 2014) ("One's cell phone, unlike

idea about how GPS technology could track them, it is unlikely that they understand that a cell phone (which typically accompanies a person everywhere he goes)[184] could be used to record their every movement.

Even more illuminating is the Court's opinion in *Riley v. California*.[185] There, the Court determined that a warrant is required to search an individual's cell phone incident to his arrest.[186] One of the bases for the Court's opinion was that cell phones contain location information that can reconstruct an individual's movements with great precision.[187] This indicates the Court's recognition that CSLI is within an objectively reasonable expectation of privacy, and thus, should be protected by the Fourth Amendment. There is no compelling reason why this protection would apply to location information obtained in a search of a cell phone incident to its owner's arrest, but would not apply to the use of a Stingray to force that same phone to reveal the same information. In fact, because a person has somewhat less Fourth Amendment protection from a search incident to arrest,[188] there is an even stronger argument that the Court's reasoning in *Riley* extends Fourth Amendment protection to location information acquired by a Stingray. In light of the *Riley* decision, courts should be more inclined to require a warrant before allowing the use of a Stingray device to acquire location information.

4. Other Concerns

Stingrays also raise several Fourth Amendment concerns that are unique to the device. As Justice Sotomayor noted in *Jones*, law enforcement surveillance techniques that are relatively cheap, simple, and covert have a greater potential of being used by law enforcement in ways that violate constitutional rights.[189] This analysis would also apply to the

---

an automobile, can accompany its owner anywhere.").

184. *Id.*

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

186. *Id.* at 2493.

187. *Id.* at 2490.

188. *Id.* at 2482. ("[I]t has been well accepted that such a search constitutes an exception to the warrant requirement.")

189. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring). ("[B]ecause GPS monitoring is cheap in comparison to conventional

use of Stingrays, which is shrouded in secrecy from the public, and is uncomplicated compared to working with or compelling a cell service provider to obtain CSLI. This is further aggravated by the government's reticence concerning the device.[190] Simply put, it is difficult to determine whether Stingrays are being used in ways that violate the Fourth Amendment when the government will scarcely admit that they are being used at all.[191] Even if law enforcement can be trusted to show restraint when using the device, the fact remains that exercising such restraint should not be left to the discretion of law enforcement.[192]

Judicial oversight of the use of Stingrays is especially important in light of the fact that a Stingray does not discriminate amongst which phones it forces to register.[193] By their operation, Stingrays masquerade as a cell tower, forcing *all* cell phones in proximity to register with the device, revealing their location information.[194] This means Stingrays invariably collect the location information of non-target phones as well as that of its target.[195] In fact, certain reports have stated that police may now be using specialized Stingray-like devices that are attached to small planes, which are flown along a certain path.[196] This collects a massive amount of "incidental" location information.[197] Reportedly, police delete this information and do not store it.[198] But the

---

surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting *Illinois v. Lidster*, 540 U.S. 419, 426 (2004)).

190. *See* Fenton, *supra* note 137; *See also* Lynn, *supra* note 142.

191. *See* Fenton, *supra* note 137; *See also* Lynn, *supra* note 142.

192. *See* Katz v. United States, 389 U.S. 347, 356–57 (1967) ("It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer . . . [T]his Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.").

193. *See* Barrett, *supra* note 121.

194. *See* Barrett, *supra* note 121.

195. *See* Barrett, *supra* note 121.

196. *See* Barrett, *supra* note 121.

197. *See* Barrett, *supra* note 121.

198. *See* Barrett, *supra* note 121.

police's lack of transparency about the use of the device,[199] and the lack of judicial oversight this leads to,[200] again leads to a situation where the only guard against constitutional violations is an officer's restraint.[201]

The lack of clear rules has another cost. Even if the use of a Stingray device is found to violate the Fourth Amendment, a court might allow evidence gathered by its use under the "good faith exception" to the exclusionary rule.[202] In *Davis*, the court found that police had violated Davis' Fourth Amendment rights in acquiring his CSLI without a warrant.[203] But because police obtained the information pursuant to the SCA, the court held that it could be admitted under a good faith exception, as police relied in good faith on a court order.[204] The same argument could be made for Stingrays, even if, as with the case in Tacoma, an application for an order did not make it clear that a Stingray was being used.[205]

IV. PROPOSAL

The Stingray has outpaced even the statutes that allow collection of CSLI from cell phone providers. Collection of CSLI by Stingrays involves no component of voluntary disclosure, one of the main rationales for allowing police to collect CSLI on a lesser showing than probable cause.[206] Additionally, Stingrays are not only used to track target phones but also to identify the phone, and are precise enough to determine a phone's location within a few meters.[207] This makes the public/private distinction of *Knotts*/*Karo* less

199. *See* Fenton, *supra* note 137; *See also* Lynn, *supra* note 142.

200. *See* Lynn, *supra* note 142. Judges in this case would not have been able to effectively rein in police abuse, because they were unaware of the methods police were using.

201. *See* Katz v. United States, 389 U.S. 347, 356–57 (1967).

202. *See*, *e.g.*, United States v. Davis, 754 F.3d 1205, 1217–18 (11th Cir. 2014) (holding that because police relied in good faith on a court order, the evidence gathered by their search should not be excluded, even where the search was unconstitutional).

203. *Id*. at 1217.

204. *Id.*

205. *See* Lynn, *supra* note 142.

206. *See* discussion *infra* Part IV.A.1.

207. *See* discussion *infra* Part IV.A.2.

relevant in the context of Stingrays.[208] Perhaps most troubling is the higher potential a Stingray has to violate the privacy not only of a target of surveillance, but of any cell phone users in its vicinity.[209] Because of the differences between Stingrays and cell site tracking, this Comment proposes that the use of Stingrays should not be governed by a lesser showing than probable cause, as cell site tracking is. Instead, a warrant should be required before a Stingray can be deployed.

A warrant requirement would largely mitigate the risks of Stringray abuse. By requiring a warrant, judges can ensure that they are more informed about the specifics of how the device will be deployed, avoiding situations where a judge grants an order authorizing what he believes is traditional cell site tracking, but in reality is interpreted by police as Stringray authorization.[210]

Requiring a warrant would introduce an element of judicial oversight into the use of the Stingray. Judges could demand that precautions be taken to avoid storing the data of non-target phones and ensure that police have a process in place for deleting this data. This would serve to curb potential abuse of the Stingray.[211] Further, having an element of judicial oversight might ease the concerns of those who believe the Stingray is being used too broadly.[212]

This comment is mindful of the fact that a warrant requirement inevitably hinders law enforcement's ability to combat crime.[213] In the midst of privacy concerns, it must be remembered that the Stingray, and cell site tracking in general, are incredibly useful tools for law enforcement to solve crimes quickly and prevent other crimes from occurring at all.[214] In events involving kidnappings or missing persons,

---

208. *See* discussion *infra* Part IV.A.2.

209. *See* discussion *infra* Part IV.A.4.

210. *See*, *e.g.*, Lynn, *supra* note 142.

211. *See* United States v. Jones, 132 S. Ct. 945, 956 (2014) (Sotomayor, J., concurring).

212. *See*, *e.g.*, *supra* note 140 and accompanying text.

213. *See* Riley v. California, 134 S. Ct. 2473, 2493 (2014) ("We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime . . . [p]rivacy has a cost.").

214. *See* In re United States for Order for Prospective Cell Site Location Info., 460 F. Supp. 2d 448, 452 (S.D.N.Y. 2006).

where time is of the essence, the Stingray can save lives.[215] It has been argued that the process of a warrant significantly hinders rapid police response to time-sensitive crises.[216]

Riley recognized that a warrant requirement will hinder law enforcement's efforts.[217] Yet it also recognized 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.'"[218] Further, the Court noted that exceptions to a warrant requirement exist where "exigencies of the situations" will justify a warrantless search, including "the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury."[219] The emergency exception is well established,[220] and would encompass time-sensitive situations such as kidnappings and missing persons. Fears that attaching a warrant requirement to a Stingray would stifle law enforcement response during these critical times are overstated.

The requirement of a warrant protects the privacy of a cell phone user in his movements without overly burdening the needs of police to gather information and respond to crises. Additionally, requiring a warrant provides a clear standard to follow when using a Stingray: courts will not need to speculate as to exactly what length of surveillance implicates the Fourth Amendment, or whether the surveillance intruded into the private sphere.

CONCLUSION

Stingrays reveal more information than traditional cell site tracking, are simpler to deploy, and may ensnare non-target's phone data as easily as that of a target. With such serious privacy concerns, the minimal protection of a Pen/Trap order is not sufficient. The SCA does not apply to the use of a Stingray because Stingrays bypass the need to

215. *See* Curtiss, *supra* note 5, at 145.
216. *See Riley*, 134 S. Ct. at 2494.
217. *Id.* at 2493.
218. *Id.*
219. *Id.* at 2494.
220. *Id.*

acquire stored communications.

In the absence of decisive legislative action, the only viable protection from the overreach of the Stingray device is the Fourth Amendment. The recent decisions of *Jones* and *Riley* provide a sturdy legal basis for the argument that the use of a Stingray device to intercept CLSI requires probable cause, rather than a lesser standard. Courts should look to these cases in extending Fourth Amendment protection against use of the Stingray device.