Washington Law Review

Volume 91 | Number 3

10-1-2016

Legislative Solutions to StingRay Use: Regulating Cell Site Simulator Technology Post-*Riley*

Ada Danelo

LEGISLATIVE SOLUTIONS TO STINGRAY USE: REGULATING CELL SITE SIMULATOR TECHNOLOGY POST-*RILEY*

Ada Danelo*

Abstract: In *Riley v. California*, the United States Supreme Court held that law enforcement must generally obtain a warrant before searching the contents of an individual's cell phone. However, *Riley* did not address whether the warrant requirement extended to cell phone metadata, e.g. non-content information such as location information. This gap creates uncertainty as to whether law enforcement officers must obtain a warrant to use Cell Site Simulators, a portable technology that mimics a cell tower to get location information metadata from cell phones. Law enforcement has justified the warrantless gathering of cell site information under the third-party doctrine, which provides that there is no Fourth Amendment-protected privacy interest in information made available to a third party such as a phone service provider. *Riley* did not explicitly address the warrant requirement in the context of metadata. And until recently, post-*Riley* circuit courts were split on whether a warrant is required for metadata. A legislative resolution of this uncertainty is thus useful, both to safeguard individual privacy and to provide clear but not overly restrictive rules for law enforcement. This Note will address what legislative solutions states have pursued, and the benefits and shortcomings of each option.

INTRODUCTION

A cell site simulator, more commonly known as a StingRay, is a portable device that mimics a cell tower so that nearby cell phones will connect to it.[1] A StingRay can obtain cell site location information (CSLI) without the cell phone user's knowledge or consent.[2] Law enforcement finds this information very useful, but media and citizens groups have criticized StingRays.[3] One group argues that "[y]ou don't have to be a criminal to be caught in this law enforcement snare. You

* With thanks to Professor Mary D. Fan for her excellent guidance, and to Peter Danelo, Bruno da Silva, and the admirable staff of *Washington Law Review* for their help in editing.

1. Jennifer Valentino-DeVries, *'StingRay' Phone Tracker Fuels Constitutional Clash*, WALL ST. J. (Sept. 22, 2011), http://www.wsj.com/articles/SB10001424053111904194604576583112723197574 [https://perma.cc/5BPH-2NE7].

2. *Id.* ("A stingray works by mimicking a cellphone tower, getting a phone to connect to it and measuring signals from the phone. It lets the stingray operator 'ping,' or send a signal to, a phone and locate it as long as it is powered on[.]").

3. Kate Martin, *Tacoma Police Using Surveillance Device to Sweep up Cellphone Data*, NEWS TRIB. (Aug. 26, 2014), http://www.thenewstribune.com/news/local/article25878184.html [https://perma.cc/L28S].

just have to be near one and use a cellphone."[4] This Note seeks an approach that strikes a balance between these safety and privacy concerns.

StingRays raise conflicting interests between law enforcement and the communities they protect. They provide legitimate benefits to society by helping officers quickly find violent criminals and individuals in need, yet they present privacy concerns that officers will overstep their bounds and use StingRays for warrantless snooping into the lives of ordinary civilians.

Law enforcement officers use StingRays to, among other purposes, locate crime suspects and assist search-and-rescue teams.[5] One police department's records indicate that the department used its StingRay nearly 100 times between 2011 and 2015.[6] In seventy-six of those instances, the department obtained a judge's approval to use the StingRay in searches for fugitives, murder suspects, or other violent criminals.[7] In twenty-one cases, the department used the StingRay without a warrant under emergency circumstances: to find missing persons, kidnapping victims, or other people in peril.[8]

Despite the technological advantages that StingRays present to law enforcement in their efforts to protect the public, privacy advocates are concerned that law enforcement uses these devices to track bystanders without a warrant.[9] "They are essentially searching the homes of innocent Americans to find one phone used by one person," according to Christopher Soghoian of the American Civil Liberties Union (ACLU), who characterizes the technology as akin to "kicking down the doors of 50 homes and searching 50 homes because they don't know where the bad guy is."[10] Soghoian describes StingRay technology as a high-tech game of "Marco Polo," in which the StingRay sends a "Marco" signal, and all cellphones within range are indiscriminately compelled to

4. *Id.*

5. Valentino-DeVries, *supra* note 1. ("The device has various uses, including helping police locate suspects and aiding search-and-rescue teams in finding people lost in remote areas or buried in rubble after an accident.").

6. Glenn E. Rice, *Secret Cellphone Tracking Device Used by Police Stings Civil Libertarians*, KAN. CITY STAR (Sept. 5, 2015, 3:24 PM), http://www.kansascity.com/news/business/technology/article34185690.html [https://perma.cc/8V8G-4CK5].

7. *Id.*

8. *Id.*

9. Martin, *supra* note 3.

10. *Id.*

respond "Polo" without the owner's knowledge that the cell phone passed data to government equipment instead of a cellphone tower.[11]

While individual law enforcement organizations' practices vary, many, such as the Department of Justice, maintain that they take precautions to limit their StingRay use.[12] The United States Department of Justice deletes data no less than once daily, and does so as soon as the target cell phone is located.[13] The Police Department of Tacoma, Washington, issued a press release stating that the department's investigators "only use the device to locate suspects named in search warrants."[14]

This Note details potential state legislation to address law enforcement's StingRay use. Part I explains StingRay technology. Part II provides background on the United States Supreme Court's relevant Fourth Amendment precedent and describes how circuit courts have treated CSLI. Part III explains why United States Supreme Court action is unlikely in the near future and advocates for a legislative solution to the issue. Part IV explains state legislative solutions currently in use and other options available to state legislatures.

I. THE RISE OF LAW ENFORCEMENT USE OF STINGRAY TECHNOLOGY

Cell phones are widely used in the United States.[15] As of January 2014, ninety percent of American adults owned a cell phone.[16] As of October 2014, sixty-four percent of American adults owned a smartphone.[17] People use their cell phones to email, text, get directions, and even to share their location by "checking in" at physical sites.[18] For a cell phone to provide many of these services, it must connect to a

11. *Id.*

12. Press Release, U.S. Dep't of Justice, Justice Department Announces Enhanced Policy for Use of Cell-Site Simulators (Sept. 3, 2015), https://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators [https://perma.cc/7HFE-QSU8].

13. *Id.*

14. Drew Mikkelsen, *Tacoma, Wash., Police Use Cell-Phone Tracking Device*, U.S.A. TODAY (Aug. 28, 2014, 4:59 PM), http://www.usatoday.com/story/news/nation-now/2014/08/28/cell-phone-tracking-stingray/14751105/ [https://perma.cc/TQS3-CUKD].

15. *Mobile Technology Factsheet*, PEW RESEARCH CTR. (Dec. 27, 2013), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet [https://perma.cc/HVJ5-P7YN].

16. *Id.* (rising to 97% and 98% for the 30–49 and 18–29 age groups).

17. *Id.*

18. Maeve Duggan, *Cell Phone Activities 2013*, PEW RESEARCH CTR. (Sept. 19, 2013), http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013 [https://perma.cc/HJT2-2VVL].

cellular network.[19] Cell towers achieve this connection by transmitting the network's data to a phone and simultaneously capturing the phone's location.[20]

Cell phones operate by connecting to cell towers, regularly updating their location to those towers, and then paging those towers to receive or transmit calls.[21] To make calls, a cell phone must constantly relay its location to the nearest cell towers.[22] The cell towers identify each phone by its assigned ten-digit phone number as well as by the phone's unchangeable electronic serial number.[23] Cell phones connect with cell towers approximately every seven seconds.[24] When a cell phone pings surrounding cell towers, it connects to up to seven nearby towers.[25] Phones transmit these location signals on a separate frequency from the frequencies that relay cell phone calls and data.[26] The cellular network uses these signals to locate a phone whenever it receives a call.[27]

Unlike real-time tracking, historical CSLI refers to the location information from cell towers collected over time.[28] Historical CSLI is "non-content" information: it does not include the content of any calls or data transmitted.[29] Cellular networks retain historical CSLI for billing purposes.[30] The amount of CSLI retained by a cellular network depends

---

19. *See Cell Phone and Service Buying Guide*, CONSUMER REP. (Mar. 2016), http://www.consumerreports.org/cro/cell-phones-services/buying-guide.htm?pn=2 [https://perma.cc/XZ6E-C995].

20. *See Hearing on Electronic Communications Privacy Act Reform Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. 5 (2010) [hereinafter *Hearing*] (statement of Prof. Orin Kerr).

21. Heath Hardman, *The Brave New World of Cell-Site Simulators*, 8 ALB. GOVT. L. REV. 1, 12, 14–16 (2015).

22. *See* Transcript of Record at 7–8, United States v. Sims (E.D. Pa. Nov. 13, 2007) (No. 06-674) http://www.eff.org/files/filenode/celltracking/shutetestimony.pdf [https://perma.cc/97JA-D2JM] (testimony of William Shute).

23. Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 309 (2004).

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

25. Transcript of Record, *supra* note 22, at 9 (testimony of William Shute).

26. McLaughlin, *supra* note 24, at 426.

27. *Id.*

28. *See Hearing*, *supra* note 20, at 5.

29. *Id.* at 6.

30. Transcript of Record, *supra* note 22, at 10 (testimony of William Shute).

on that network's policy, though most networks retain CSLI for over a year.[31]

Law enforcement commonly requests historical or real-time CSLI from cellular providers for use in investigations.[32] Officers can use this information to ascertain from where and with whom a suspect communicates.[33] A cell phone's proximity to a given cell tower, the signal strength, and the cell phone's movement between towers reveal the phone's location.[34]

Courts have begun to address historical CSLI.[35] The evidentiary standard that officers must show when requesting CSLI varies by jurisdiction and by type of CSLI.[36] Depending on the jurisdiction, officers may obtain CSLI by requesting a subpoena, court order, or warrant.[37] A subpoena, which commands the production of documents or a personal appearance before a court, requires no showing of suspicion.[38] A court order, on the other hand, requires reasonable suspicion that a suspect is involved in criminal activity.[39] A warrant, the most protective standard, requires probable cause that a suspect has committed a crime or that a search will reveal evidence of a crime.[40]

Jurisdictions differ in how they address CSLI, even before the added layer of complexity presented by StingRay use. A StingRay, as described earlier, is a portable device that pretends to be a cell tower so

---

31. U.S. DEP'T OF JUSTICE, RETENTION PERIODS OF MAJOR CELLULAR SERVICE PROVIDERS (Aug. 2010), https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart [https://perma.cc/PVN3-8VTC].

32. *See* Zachary Ross, Note, *Bridging the Cellular Divide: A Search for Consensus Regarding Law Enforcement Access to Historical Cell Data*, 35 CARDOZO L. REV. 1185, 1187 (2014).

33. Scott A. Fraser, Comment, *Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell-Site Location Jurisprudence*, 52 SANTA CLARA L. REV. 571, 582 (2012).

34. *Id.*

35. *Id.* at 574–76 (discussing the judiciary's treatment of CSLI).

36. Ross, *supra* note 32, at 1187.

37. *Id.* at 1187, 1198–99. *See also* Part II.B.2.iii.

38. U.S. DEP'T. OF JUST., OFF. OF LEGAL POL'Y, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES, https://www.justice.gov/archive/olp/rpt_to_congress.htm#2a1 [https://perma.cc/QB3K-WDPX] ("Administrative subpoena authorities allow executive branch agencies to issue a compulsory request for documents or testimony without prior approval from a grand jury, court, or other judicial entity."); U.S. MARSHALS SERV., SERVICE OF PROCESS: CRIMINAL SUBPOENA, http://www.usmarshals.gov/process/subpoena.htm [https://perma.cc/2ZHX-UZ7E].

39. 18 U.S.C. § 3583 (2012); Devallis Rutledge, *Probable Cause and Reasonable Suspicion*, POLICE MAGAZINE (June 7, 2011), http://www.policemag.com/channel/patrol/ articles/2011/ 06/probable-cause-and-reasonable-suspicion.aspx [https://perma.cc/W4YZ-N3NY].

40. Rutledge, *supra* note 40.

that it can measure a target phone's signal strength from multiple locations to determine where that phone is located.[41] In many cases, the government has first gathered historical CSLI to determine the general area of the target cell phone.[42] After simulating a cell tower, StingRays page the target cell phone.[43] They continue paging the target phone until they have sufficient readings to locate the phone.[44] The Federal Bureau of Investigation (FBI) has used StingRays since at least 1995.[45] More recently, local law enforcement agencies have begun to use StingRays.[46]

Cell phone companies' newfound resistance to CSLI requests has contributed to an increase in law enforcement's use of StingRays.[47] Historically, law enforcement agencies could easily request CSLI from phone companies under the Stored Communications Act (SCA).[48] But as concern has grown about maintaining digital privacy, phone companies have become more resistant to cooperating with law enforcement.[49] The *New York Times* notes that "[w]ith the rapid expansion of cell surveillance have come rising concerns—including among carriers—about what legal safeguards are in place to balance law enforcement agencies' needs for quick data against the privacy rights of consumers."[50] Many companies now employ legal staff specifically to

41. *EPIC v. FBI: StingRay/Cell Site Simulator*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org/foia/fbi/stingray/ [https://perma.cc/6WZ8-L557].

42. *Id.*

43. Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED MAG. (Apr. 9, 2013, 6:30 AM), https://www.wired.com/2013/04/verizon-rigmaiden-aircard/ [https://perma.cc/3B5U-L63W].

44. *Id.* (describing how coordinates are overlaid to find a phone's location). Although some cell-site simulators are capable not only of tracking but also of listening to phone calls, this Note only addresses the location-specific StingRay technology. *See* Andy Greenberg, *Despite FCC "Scare Tactics," Researcher Demos AT&T Eavesdropping*, FORBES (July 31, 2010, 5:35 PM), http://www.forbes.com/sites/firewall/2010/07/31/despite-fcc-scare-tactics-researcher-demos-att-eavesdropping/ [https://perma.cc/HZ2V-4TRZ].

45. *EPIC v. FBI: StingRay/Cell Site Simulator*, *supra* note 41.

46. *See, e.g.*, Martin, *supra* note 3.

47. *See, e.g.*, Hope King, *Tech Companies Standing up to Government Data Requests*, CNN MONEY (June 18, 2015, 6:06 PM), http://money.cnn.com/2015/06/18/technology/data-protection-government/ [https://perma.cc/JE3F-EB9J]; Ellen Nakashima, *Apple Vows to Resist FBI Demand to Crack iPhone Linked to San Bernadino Attacks*, WASH. POST (Feb. 17, 2016), https://www.washingtonpost.com/world/national-security/us-wants-apple-to-help-unlock-iphone-used-by-san-bernardino-shooter/2016/02/16/69b903ee-d4d9-11e5-9823-02b905009f99_story.html [https://perma.cc/BK69-GCWM].

48. Stored Communications Act, 18 U.S.C. § 2703 (2002), 18 U.S.C. §§ 2701–2712 (2002).

49. Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html [https://perma.cc/4XEY-SZXH].

50. *Id.*

respond to law enforcement records requests, perhaps in response to public perception that these companies are overly compliant with the government.[51] Companies including AT&T and T-Mobile require a warrant before they will allow law enforcement access to a user's current location data, while others, including Verizon and Cricket, say they cannot provide current location data at all.[52]

StingRays bypass the need to request real-time CSLI from a cellular provider by enabling law enforcement to track a cell phone independently.[53] StingRays are a major technological improvement for law enforcement over historical CSLI. However, they raise privacy concerns because they enable law enforcement to bypass a third party, the phone company, to obtain CSLI. According to the ACLU, the prevalence of StingRays is worrisome; as of early 2016, they were used by at least fifty-seven agencies in twenty-two states.[54] Until now, legislatures and courts have failed to adequately address CSLI's effect on the competing values of efficient law enforcement and individual privacy.

II. THE FOURTH AMENDMENT AND TECHNOLOGY-AIDED INVESTIGATION

The Fourth Amendment provides that the

> right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[55]

The United States Supreme Court has held that the Fourth Amendment protects only an expectation of privacy that is "reasonable"

---

51. *See* Brian X. Chen, *A Senator Plans Legislation to Narrow Authorities' Cellphone Data Requests*, N.Y. TIMES (Dec. 9, 2013), http://www.nytimes.com/2013/12/09/technology/a-senator-plans-legislation-to-narrow-authorities-cellphone-data-requests.html [https://perma.cc/SDG5-8WMK].

52. *Id.*

53. *See supra* notes 1–3 and accompanying text.

54. American Civil Liberties Union, *Stingray Tracking Devices: Who's Got Them?*, https://www.aclu.org/map/StingRay-tracking-devices-whos-got-them [https://perma.cc/6RMP-6VWK].

55. U.S. CONST. amend. IV.

or "legitimate."[56] Once a court has determined that a search occurred, the question becomes whether that search was reasonable under the Fourth Amendment, and whether a warrant was necessary.[57] The Fourth Amendment itself does not define "reasonable," but courts, including the United States Supreme Court, have defined its limitations by providing many exceptions to the warrant requirement.[58] In fact, "[t]he vast majority of searches conducted by government agents are lawful despite the absence of a warrant; a substantial number of these are lawful despite the lack of probable cause."[59]

The Court has acknowledged that its own reasonable-expectation-of-privacy standard may be "subjective and unpredictable."[60] The standard is particularly unpredictable when applied to electronic surveillance, which presents fact patterns that are hard to analogize to past cases.[61] Indeed, the Court has tried to keep up with emerging technology for nearly five decades using the *Katz v. United States*[62] reasonable-expectation-of-privacy test—from infrared imaging in *Kyllo v. United States*,[63] to GPS tracking in *United States v. Jones*,[64] and now smartphones in *Riley v. California*.[65]

The Fourth Amendment requires a warrant based on probable cause to search homes and other private premises or to intercept

---

56. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (holding that a phone company's use of a pen register to provide police with a record of phone numbers that a suspect dialed from his landline was not a Fourth Amendment search); Katz v. United States, 389 U.S. 347, 361 (1967) ("there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

57. *See* U.S. CONST. amend. IV.

58. Clifford S. Fishman, *Searching Cell Phones After Arrest: Exceptions to the Warrant and Probable Cause Requirements*, 65 RUTGERS L. REV. 995, 999–1000 (2013).

59. *Id.* at 1001.

60. Kyllo v. United States, 533 U.S. 27, 34 (2001) (holding that a person has a reasonable expectation of privacy against the government's use of surveillance to learn about the inside of that person's home, particularly when the technology used is not available to the general public—thus the government's use of thermal imaging technology to measure the heat emanating from defendant's home was a search).

61. *See* 1 FISHMAN & MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE §§ 1:3–1:6 (3d ed. 2007).

62. *See generally* 389 U.S. 347 (1967).

63. *See generally* 533 U.S. 27 (2001).

64. *See generally* 565 U.S. __, 132 S. Ct. 945 (2012).

65. *See generally* 573 U.S. __, 134 S. Ct. 2473 (2014); *see also* Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, THE ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/tech078nology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ [https://perma.cc/6KMA-5L7C].

communications.[66] A warrant is not required under the following exceptions, when: (1) a search occurs incident to a lawful arrest; (2) an object is in plain view; (3) the suspect gives consent to the search; (4) an officer is engaged in a "stop and frisk" rather than a full search; (5) an officer has probable cause to believe that an automobile contains evidence of a crime; or (6) exigent circumstances exist (such as emergencies or hot pursuit of a criminal).[67] The most commonly used exceptions to the warrant requirement are exigent circumstances based on imminent risk of physical danger or destruction of evidence, and the search of a person incident to arrest.[68] Of special relevance to cell phone searches is the plain view exception, which provides that information in plain view, such as the photo on a cell phone's screensaver, is not a search.[69] Under the plain view doctrine, police may answer a suspect's cell phone or respond to incoming text messages immediately following arrest if officers have probable cause to believe that the phone was used in connection with the crime.[70] The exceptions to the warrant requirement serve to balance efficiency and public safety with personal privacy.

A. Reasonable Expectations of Privacy and the Third Party Exposure Doctrine

As described more thoroughly in Section III below, Fourth Amendment jurisprudence is unclear as to whether a warrant is required

66. Fishman, *supra* note 58, at 1001–02; *see also* THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION 217-82 (2008) (discussing arrests and seizures, only a small fraction of which require a warrant).

67. *See, e.g.*, Kentucky v. King, 563 U.S. 452, 452 (2011) (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978)) (holding that no warrant is required for exigent circumstances); Horton v. California, 496 U.S. 128, 141 (1990) (holding that officers can seize objects in plain view without a search warrant); United States v. Ross, 456 U.S. 798, 823–24 (1982) (holding that no warrant is required if the officer has probable cause that the automobile contains evidence of a crime), *overruled by* Arizona v. Gant, 556 U.S. 332, 332 (2009) (concluding that once a driver has been removed from a car and arrested, there is no longer any possibility that the driver could seize anything in the vehicle and destroy it or use it as a weapon, and thus there is no justification for a warrantless search of the car); Schneckloth v. Bustamonte, 412 U.S. 218, 228 (1973) (holding that consent-based searches are constitutionally acceptable); Chimel v. California, 395 U.S. 752, 759 (1969) (quoting Trupiano v. United States, 334 U.S. 699, 708 (1948)) (establishing the search incident to arrest exception); Terry v. Ohio, 392 U.S. 1, 27 (1968) (holding that officers can stop and frisk if there is reasonable suspicion to believe the individual is dangerous).

68. Fishman, *supra* note 58, at 1002–03.

69. *Id.* at 1002.

70. 1 FISHMAN & MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 5:177 (3d ed. 2007).

for CSLI. However, the third-party doctrine may wholly exempt CSLI from Fourth Amendment protections.[71] The third-party doctrine provides that information voluntarily conveyed to a third party receives no Fourth Amendment protection.[72] Thus, the government can seize without a warrant any information that an individual has willingly shared with a third party.[73]

Under the third-party doctrine, when someone voluntarily conveys information to another entity, such as a bank or a telephone company, that person assumes the risk that the third party could disclose that information to the government.[74] In *United States v. Miller*,[75] the Court found that the defendant did not have a reasonable expectation of privacy in the documents he provided to his bank.[76] The government could thus obtain those documents from the bank without a warrant, even though the defendant may have assumed that the bank would only use them for a limited purpose.[77]

There is also no reasonable expectation of privacy in phone numbers that an individual dials. In *Smith v. Maryland*,[78] the United States Supreme Court found that the defendant had no expectation of privacy in phone numbers that he called, since he voluntarily conveyed those same numbers to the telephone company, a third party.[79] The Court noted that the disclosure statement at the front of a phone book alerts phone users to their lack of privacy expectations when dialing a phone number.[80] The Court thus held that the installation of pen registers on the defendant's phone line was not a Fourth Amendment search.[81] A pen register is an electronic device that records the numbers dialed from a particular phone

71. *See, e.g.*, United States v. Graham, 796 F.3d 332, 355 (4th Cir. 2015), *rev'd en banc* United States v. Graham, 2016, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797, at *19–20 (4th Cir. May 31, 2016) (holding that police did not need a warrant to obtain over 200 days worth of CSLI, as they could instead rely on the third-party doctrine).

72. *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that government's use of a pen register to record the phone numbers dialed from defendant's phone line was not a search).

73. *See Smith*, 442 U.S. at 735; United States v. Miller, 425 U.S. 435 (1976).

74. *See Smith*, 442 U.S. at 735; *Miller*, 425 U.S. at 443.

75. 425 U.S. 435 (1976).

76. *Id.* at 443.

77. *Id.*

78. 442 U.S. 735 (1979).

79. *Id.* at 744.

80. *Id.* at 742–43. ("Most phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'")

81. *Id.* at 746.

line.[82] Unlike in *Katz*, where the Court held that the government eavesdropping on defendant's phone calls was a search requiring a warrant,[83] the pen registers in *Smith* did not capture the *contents* of defendant's phone calls.[84] Furthermore, "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company . . . ."[85] Because a telephone user is aware that the phone company monitors the numbers dialed to connect a call, under the *Katz* test that person has no legitimate expectation of privacy.[86] Courts have applied the third-party doctrine to the address on the outside of an envelope,[87] and even to the interception of a telephone conversation by a portable radio.[88]

Although the United States Supreme Court has not addressed CSLI, all Circuit Courts of Appeals to rule on the issue have held that cell phone users have no reasonable expectation of privacy in their CSLI.[89] Because CSLI is information shared with a third party (the cellular provider), users assume the risk of its disclosure.[90] As in *Smith*, the lower courts found that a defendant's reasonable expectation of privacy is negated by the average person's knowledge of how phones work and the fact that they expose location information to third parties.[91]

In *Smith*, the United States Supreme Court found several ways in which a telephone subscriber objectively receives notice that the phone company is documenting the subscriber's dialing activity.[92] By dialing, the user realizes those digits are conveyed to the phone company to complete the call; by reviewing the itemized bill, the user realizes that the digits dialed are recorded; and by using a telephone book, the

82. *Id.* at 741–42.

83. Katz v. United States, 389 U.S. 347, 350–53 (1967).

84. *Smith*, 442 U.S. at 741.

85. *Id.* at 742.

86. *Id.*

87. United States v. Huie, 593 F.2d 14, 15 (5th Cir. 1979).

88. Tyler v. Berodt, 877 F.2d 705, 706–07 (8th Cir. 1989) (discussing situation in which officers intercepted a conversation on a portable phone using a radio).

89. *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 883 (6th Cir. 2016); United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797, at *13 (4th Cir. May 31, 2016) (holding that 200 days' worth of CSLI was available under the third-party doctrine, and thus no warrant was required); United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015) (holding the same for 67 days' worth of CSLI); *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013). Note that some circuits have not reached this conclusion until en banc review.

90. *Davis*, 785 F.3d at 510.

91. *See, e.g.*, *id.* (discussing *Historical Cell Site Data*, 724 F.3d at 613).

92. Smith v. Maryland, 442 U.S. 735, 742–43 (1979).

consumer is put on notice that telephone companies monitor dialing activity.[93] Thus, even if an individual subjectively believed that dialed digits were private, that belief would be unreasonable, and under the *Katz* test, not protected by the Fourth Amendment.[94]

By the same logic, users should be aware that a phone company tracks their location—for example, to impose surcharges for roaming, to provide directions, or to locate lost or stolen phones. Even if an individual cell phone user purports not to know that she is tracked, and thus claims a *subjective* expectation of privacy, the broad public awareness of cell phone tracking indicates that there is no *reasonable* expectation of privacy. According to the Department of Justice, "'a customer's Fourth Amendment rights are not violated when [a] phone company reveals to the government its own records that show where a mobile device placed and received calls."[95]

It is unclear whether the third-party doctrine applies to StingRays.[96] While cell phone users might know that their phones automatically transmit a signal, they likely do not know that the government can use a StingRay to capture that signal without their consent or action.[97] Since a phone user makes no voluntary transmission to a third party under this analysis, the third-party doctrine would not apply.[98]

Furthermore, the third-party doctrine itself has come under substantial criticism—some scholars believe it is outdated in light of modern technology, and believe that although lower courts are still following the doctrine, the United States Supreme Court is likely to revisit it.[99] The

93. *Id.*

94. *Id.* at 743–44.

95. Declan McCullagh, *Court Allows Warrantless Cell Location Tracking*, CNET NEWS (Sept. 7, 2010, 1:44 PM), http://www.cnet.com/news/court-allows-warrantless-cell-location-tracking/ [https://perma.cc/3SNM-BPD8].

96. *See* Hardman, *supra* note 21, at 21.

97. *See id.*

98. *See id.* at 22.

99. *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009) (defending "the controversial rule that information loses Fourth Amendment protection when it is knowingly revealed to a third party."); Hanni Fakhoury, Smith v. Maryland *Turns 35, but Its Health Is Declining*, ELECTRONIC FRONTIER FOUND. (June 24, 2014), https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining [https://perma.cc/DKF7-XD9H]; Jenna McLaughlin, *Appeals Court Delivers Devastating Blow to Cellphone-Privacy Advocates*, THE INTERCEPT (May 31, 2016, 12:58 PM), https://theintercept.com/2016/05/31/appeals-court-delivers-devastating-blow-to-cell-phone-privacy-advocates/ [https://perma.cc/4ELP-GC27].

Fourth Circuit recently noted that the "Supreme Court may in the future limit, or even eliminate, the third-party doctrine."[100]

B. The Courts Grapple with Technology and the Fourth Amendment

1. Early United States Supreme Court Cases

There is little United States Supreme Court precedent on cell phones or on tracking technology, and none indicates how the court would rule on CSLI.[101] The cases relevant to the use of CSLI date back to the 1970s, far before a majority of Americans owned a cell phone.[102] In *Katz v. United States*, the Court established the contemporary framework for Fourth Amendment analysis, requiring both a subjective and an objective expectation of privacy.[103] In *United States v. Knotts*,[104] the Court held that people have no reasonable expectation of privacy on public roadways.[105] In *United States v. Karo*,[106] the Court restricted *Knotts* and held that using technology to monitor inside a private residence, not open to visual surveillance, is a search.[107] Recently, the Court addressed the use of a GPS device in *United States v. Jones*,[108] holding that a warrant was required to place a GPS device on a defendant's car because placement of the GPS device was a trespass to chattels.[109] And in *Riley v. California*,[110] the Court required a warrant for any search of the contents of a cell phone.[111] But the Court has yet to address cell phone metadata or location information.

---

100. United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797, at *5 (4th Cir. May 31, 2016).

101. Some of the only examples will be discussed further below: United States v. Jones, __ U.S. __, 132 S. Ct. 945 (2012) and Riley v. California, __ U.S. __, 134 S. Ct. 2473 (2014).

102. Cell phones were invented in 1973 and weighed 1.1 kilos. Richard Goodwin, *The History of Cell Phones from 1973 to 2008: The Handsets that Made It All Happen*, KNOW YOUR MOBILE (Apr. 16, 2015, 2:15 PM), http://www.knowyourmobile.com/nokia/nokia-3310/19848/history-mobile-phones-1973-2008-handsets-made-it-all-happen [https://perma.cc/S7MW-UADE].

103. 389 U.S. 347, 361 (1967).

104. 460 U.S. 276 (1983).

105. *See id.* at 281–82.

106. 468 U.S. 705 (1984).

107. *See id.* at 713–16.

108. 565 U.S. __, 132 S. Ct. 945 (2012).

109. *See id.* at 949–51.

110. __ U.S. __, 134 S. Ct. 2473 (2014).

111. *See id.* at 2495.

In *Katz v. United States*, the United States Supreme Court provided a test to determine whether a search requiring a warrant has taken place.[112] Justice Harlan's concurrence set forth what has become the traditional two-prong test.[113] The first prong is whether a person has shown "an actual (subjective) expectation of privacy," and the second is whether that expectation is "one that society is prepared to recognize as 'reasonable.'"[114] *Katz* thus expanded Fourth Amendment protections from a given place—the home—to other aspects of an individual's life. Furthermore, *Katz* reduced Fourth Amendment protection of the home, holding that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[115]

Technology-aided surveillance of people in public places is not a Fourth Amendment search.[116] In *United States v. Knotts*, the Court found that police use of a radio transmitter to track the movement of a defendant's car on public roads was not a violation of the Fourth Amendment because "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[117]

However, the Court limited *Knotts* to its facts in *United States v. Karo*, where law enforcement used a radio transmitter to track defendant's movement inside a private home.[118] The Court distinguished this from the actions of the agents in *Knotts*, who stopped tracking when the transmitter reached its destination.[119] The Court limited the government to information that could be obtained "by observation from

112. 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring) (holding that the government's recording of conversations in a public telephone booth merited Fourth Amendment protection). *See also* Smith v. Maryland, 442 U.S. 735, 739–40 (1979).

113. *See Katz*, 389 U.S. at 361.

114. *Id.*

115. *See id.* at 351 (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927)).

116. *See* United States v. Knotts, 460 U.S. 276, 282 (1983) ("Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them.").

117. *See id.* at 281. Thus, a beeper that agents placed in a container of chemicals and used to track the suspect was acceptable. *See id.* at 277, 285.

118. 468 U.S. 705, 708–10, 713–15 (1984).

119. *See id.* at 714–15.

outside the curtilage of the house."[120] The use of a radio transmitter, then, requires a warrant only when it implicates private areas.[121]

In *Kyllo v. United States*, the Court found that the use of sense-enhancing technology "not in general public use" was a search under the Fourth Amendment.[122] The sense-enhancing technology in question in *Kyllo* was heat imaging, which allowed police to see that a wall of Kyllo's home was emitting abnormally high amounts of heat, indicating a marijuana grow operation.[123] Like heat imaging, a StingRay could also be considered sense-enhancing technology: while heat imaging obviates the need for police to use more labor-intensive methods of detecting heat, StingRays reduce the need for physically tailing suspects. But the speed at which technology advances and becomes widely available casts doubt on the scope of society's actual expectations of privacy. For example, the heat-imager at question in *Kyllo* can now be inexpensively obtained online by the general public, which fulfills the Court's "in general public use" dicta.[124]

This line of cases demonstrates that the United States Supreme Court precedent has not kept pace with rapidly evolving modern technology. *Knotts* and *Karo* established a distinction between public and private places; *Kyllo* only applies as long as the technology is not widely available for public purchase; and *Katz* is difficult to reconcile with a quickly changing concept of privacy.

2. The Judicial Shift

a. United States v. Jones*: the Trespass to Chattels Theory*

Recent United States Supreme Court decisions have broached issues of technology and their effects on privacy. The Court makes clear that "[a]t bottom, [the Court] must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[125] Drawing an analogy to now-ancient technology, in

120. *See id.* at 715.

121. *See id.*; *Knotts*, 460 U.S. at 281, 284.

122. 533 U.S. 27, 34 (2001).

123. *See id.* at 29–30.

124. The Flir One, among many products of its kind available, costs $249.99 as of the editing of this Note, attaches to a smartphone, and is widely available online. *See, e.g.*, FLIR, http://www.flir.com/flirone/display/?id=69324 [https://perma.cc/B9NN-CM84].

125. United States v. Jones, __ U.S. __, 132 S. Ct. 945, 950 (2012) (quoting *Kyllo*, 533 U.S. at 34).

United States v. Jones[126] the Court found that a GPS device placed in a vehicle was akin to an eighteenth-century constable hiding in a horse-drawn carriage.[127] Both are unlawful trespasses to property, and thus unlawful searches.[128] But *Jones* departed from the *Katz* reasonable expectation of privacy test that the Court used exclusively for decades, instead deciding the GPS issue on a trespass-to-chattels theory.[129] This allowed the Court to sidestep addressing whether a warrant is required for GPS tracking outside of a suspect's home: we only know that a warrant is required if the GPS device interferes with a suspect's property rights.[130]

Because *Jones* was decided on a trespass-to-chattels theory outside of the Fourth Amendment framework established by the Court in *Katz*, its holding is unhelpful when analyzing whether a warrant is required for CSLI. Although the Court previously found that use of technology widely available to the public may not be a search requiring a warrant,[131] it sidestepped that question entirely in *Jones*.[132]

The lower court in *Jones* established the mosaic theory, which is popular among those who believe a full warrant should be required for CSLI tracking.[133] Under the mosaic theory, even if a particular act of surveillance would be permissible under the Fourth Amendment, it may violate a suspect's reasonable expectation of privacy when used long-term, since the aggregate information allows the government to infer intimate details about a suspect's life.[134] Under this theory, the D.C. Circuit found that a month of warrantless GPS surveillance violated the suspect's Fourth Amendment rights.[135] And after *Jones*, lower courts

126. __ U.S. __, 132 S. Ct. 945 (2012).

127. *See id.* at 951 n.3.

128. *See id.*

129. *See id.* at 949–51. *Jones* additionally distinguished itself from *Knotts* on two grounds. First, *Knotts* did not claim any physical trespass, whereas *Jones* did. *See id.* at 951–52. Second, the *Jones* Court stated that the *Katz* test is not exclusive, and therefore, even if a technique does not constitute a search under *Katz*, it might still qualify under the trespass test. *See id.* at 952–55.

130. *See id.* at 953–54. From *Kyllo*, we know that tracking movements through GPS is a search if it shows details *inside* the home. *Kyllo*, 533 U.S. at 42 (Stevens, J., dissenting).

131. Thus, if the general public had a certain device that permitted intrusion into a person's private space, no warrant would be required for law enforcement's use of that device.

132. *See Jones*, 132 S. Ct. at 957–64 (Alito, J., concurring).

133. *See generally*, Gabriel R. Schlabach, Note, *Privacy in the Cloud: The Mosaic Theory and the Stored Communications Act*, 67 STAN. L. REV. 677 (2015).

134. *Id.* at 678–79.

135. United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010); *cf.* Halkin v. Helms, 598 F.2d 1, 8 (D.C. Cir. 1978) (holding that intelligence agencies should be not required to disclose

have held that prolonged warrantless searches violate the Fourth Amendment.[136] But the United States Supreme Court has not adopted the mosaic theory—the closest the Court came to acknowledging the theory was in the *Jones* concurrences.[137] Justice Sotomayor noted that long-term GPS monitoring can create a "precise, comprehensive record" of a person's movements that reveals a "wealth of detail" about that individual, and should require a full warrant.[138] Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, noted that the issue the Court should have addressed was the duration of the tracking, echoing Justice Sotomayor's concerns.[139]

Lower courts have failed to adopt a consistent rationale for *Jones*' application to CSLI. *United States v. Sereme*[140] denied a motion to suppress CSLI under the SCA post-*Jones*, holding that without the physical intrusion present in *Jones*, there was no unlawful search: "the *Jones* opinion does nothing to preclude the Government's monitoring of individuals through the use of cell site technology."[141] *United States v. Graham*[142] did the same, categorizing CSLI as voluntary "business records . . . created and maintained by the cellular providers."[143] *Graham* required only a reasonable suspicion standard of "specific and articulable facts" for CSLI.[144] *United States v. Skinner*[145] saw CSLI as an essential investigative tool too valuable to law enforcement to limit with a warrant requirement.[146] The *Skinner* court also found "no inherent constitutional difference between trailing a defendant and tracking him

---

"seemingly innocuous information" since those "bits and pieces" can be added together to reveal "how the unseen whole must operate").

136. *See, e.g.*, the panel opinions in *Davis* and *Graham*, both of which followed the Mosaic theory. United States v. Graham, 796 F.3d 332 (4th Cir. 2015); United States v. Davis, 754 F.3d 1205 (11th Cir. 2014).

137. *See Jones*, 132 S. Ct. at 954–57 (J. Sotomayor, concurring); *id.* at 957–59 (J. Alito, concurring).

138. *Jones*, 132 S. Ct. at 955 (J. Sotomayor, concurring); *see also* Schlabach, *supra* note 133, at 679.

139. *See Jones*, 132 S. Ct. at 957–58 (J. Alito, concurring).

140. No. 2:11-CR-97-FtM-29SPC, 2012 U.S. Dist. LEXIS 68202 (M.D. Fla. Mar. 26, 2012).

141. *Id.* at *29–30.

142. 846 F. Supp. 2d 384 (D. Md. 2012), *aff'd. by* United States v. Graham, 2016 U.S. App. LEXIS 9797 (4th Cir. May 31, 2016).

143. *Id.* at 398. The court noted, however, that CSLI, unlike business records which are "voluntary commercial transactions," records "transmissions of radio signals in which the cell phone service subscriber may or may not be an active and voluntary participant." *Id.* at 356–57.

144. *See id.* at 386–87.

145. 690 F.3d 772 (6th Cir. 2012).

146. *See id.* at 774.

via [CSLI]."[147] The Fifth Circuit characterized CSLI as a "record[] of transactions to which [the cell phone provider] is a party." Thus, no warrant is required, provided that the government does not obtain communication content.[148] The Fifth Circuit distinguished *Jones* and *Karo* from CSLI cases by asking *who* collected the location information.[149] In *Jones* and *Karo*, the government collected location information, while the service provider collected CSLI.[150] These cases illustrate that while *Jones* could be interpreted to limit the government's power to track individuals, different courts interpret *Jones* differently when determining the standard required for CSLI.

Although *Jones* indicates the Court's awareness of tracking devices, it provides no clear standard that courts can apply to later tracking cases. While both GPS and CSLI provide a person's location, a suspect being "tracked surreptitiously with a GPS device has no knowledge" of the location recording, whereas a cell phone user knows that in order to use the phone, that phone must be connected to the cellular network.[151] Additionally, because *Jones* was decided based on a trespass theory instead of under the *Katz* test, its logical extension to CSLI, which does not involve physical trespass, is weakened.[152]

b. Riley v. California*: Warrant Requirement for Cell Phone Contents*

When police search the contents of a suspect's phone, even one seized incident to arrest, they conduct a Fourth Amendment search.[153] Chief Justice Roberts stated *Riley*'s holding bluntly: "[o]ur answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[154]

In *Riley v. California*, the Court unanimously held that police could not conduct a warrantless search of the contents of a cell phone seized incident to arrest absent exigent circumstances.[155] The key issue in *Riley*

147. *Id.* at 778.

148. *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 612 (5th Cir. 2013).

149. *See id.* at 609.

150. *Id.* at 609–10. Note that this analysis does not apply to StingRays, which are devices the government uses to collect location information.

151. Elizabeth Elliott, Comment, United States v. Jones*: The (Hopefully Temporary) Derailment of Cell-Site Location Information Protection*, 15 LOY. J. PUB. INT. L. 1, 8 (2013).

152. *See id.* at 9; United States v. Jones, __ U.S. __, 132 S. Ct. 945, 954 (2012).

153. Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2495 (2014).

154. *Id.* at 2495.

155. *Id.* at 2493–95.

was whether the search-incident-to-arrest exception, which permits police to seize and search anything found in an arrestee's possession, extended to files stored on a cell phone.[156] *Riley* found that it did not, stating that cell phones are in effect digital containers with "immense storage capacity" for private data,[157] and accordingly "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet or a purse."[158]

The *Riley* Court considered two cases presenting a "common question."[159] In the first, the police arrested David Riley after discovering firearms hidden under the hood of his car.[160] Upon searching Riley incident to arrest, the police found evidence that Riley was associated with a gang.[161] The police then seized and searched Riley's cell phone without a warrant, finding further evidence of Riley's gang affiliation.[162] The trial court judge found that the search of the cell phone was admissible because it was conducted incident to arrest.[163] Based in part on the evidence from Riley's cell phone, he was convicted of attempted murder, assault with a semiautomatic firearm, and shooting at an occupied vehicle.[164]

In the second case, Brima Wurie was arrested shortly after dealing drugs outside a convenience store.[165] Officers took Wurie's cell phone and observed several missed calls from "my house."[166] Without a warrant, officers flipped open the phone, noted the caller's number, and tracked that number back to Wurie's home.[167] After obtaining a search warrant for the home, officers found large quantities of drugs, a gun, and cash.[168] The district court found that the cell phone search was constitutional, since it occurred incident to arrest.[169] Wurie was charged with, and subsequently convicted of, felony possession of a firearm and

156. *See generally Riley*, 134 S. Ct. 2473.

157. *Id.* at 2489.

158. *Id.* at 2488–89.

159. *Id.* at 2480.

160. People v. Riley, No. D059840, 2013 WL 475242, at *1 (Cal. Ct. App. Feb. 8, 2013).

161. *Riley*, 134 S. Ct. at 2480.

162. *Id.*

163. *Riley*, 2013 WL 475242, at *3.

164. *Id.* at *1.

165. United States v. Wurie, 612 F. Supp. 2d 104, 106 (D. Mass. 2009).

166. *Id.*

167. *Id.* at 106–07.

168. *Id.* at 107.

169. *Id.* at 109–11.

ammunition, distribution of crack cocaine, and possession of crack cocaine with intent to distribute.[170] In both cases, the convictions were overturned.[171]

One of the most significant principles from the Court's decision in *Riley* is that "digital is different, and the difference matters."[172] Chief Justice Roberts discussed privacy interests, positing that cell phones may provide "detailed information about all aspects of a person's life."[173] The type and quantity of information on a phone can present a significant privacy intrusion.[174] Phones are like "minicomputers" with telephone capability, collecting various details about a person's life that may tell "more in combination than any single record."[175] "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person."[176] For the above reasons, searching cell phone data is "materially indistinguishable" from a physical search.[177]

Like *Jones*, *Riley* was a "rather unusual excursus" in the Court's Fourth Amendment jurisprudence.[178] The *Riley* decision may have turned on "the justices' own sense of what is intuitively private."[179] The Court provided an "indeterminate reasonableness test" which barely figures in search-incident-to-arrest precedent.[180] Indeed, "in case after case, the Roberts Court has liquidated bright-line rules about when a search is unreasonable" in favor of reasonableness balancing.[181] This marks the Court's turn towards "reasonableness" as the "dominant mode of [Fourth Amendment] constitutional inquiry."[182]

---

170. *Id.* at 105; Riley v. California, 573 U.S. __, 134 S. Ct. 2473, 2482 (2014).

171. *Riley*, 134 S. Ct. at 2495.

172. Brianne J. Gorod, *Agreement at the Supreme Court: The Three Important Principles Underlying* Riley v. California, 9 N.Y.U. J. L. & LIBERTY 70, 75 (2015).

173. *Riley*, 134 S. Ct. at 2490.

174. *Id.* at 2489–91.

175. Charles D. Weisselberg, *Cell Phones and Everything Else: Criminal Law Cases in the Supreme Court's 2013–2014 Term*, 50 CT. REV. 164, 164–65 (2014).

176. *Riley*, 134 S. Ct. at 2489.

177. *Id.* at 2488.

178. *See* Noah Feldman, *Justices Don't Want their Smartphones Searched*, BLOOMBERG VIEW (June 25, 2014, 11:24 AM), https://www.bloomberg.com/view/articles/2014-06-25/justices-don-t-want-their-smartphones-searched [https://perma.cc/P397-9C73?type=image].

179. *Id.*

180. *Fourth Amendment—Search and Seizure—Searching Cell Phones Incident to Arrest*—Riley v. California, 128 HARV. L. REV. 251, 255–56 (2014) [hereinafter *Fourth Amendment—Search and Seizure*].

181. *Id.* at 257.

182. *Id.*; *see* Maryland v. King, __ U.S. __, 133 S. Ct. 1958 (2013) (holding the government may reasonably collect arrestees' DNA without a warrant or individualized suspicion); Florence v. Bd. of

The *Riley* Court, eager to find a middle ground but unable to do so, settled for the clarity of requiring a warrant.[183] The Justices' desire for a moderate approach is reflected by the Court's "handwringing about the lack of limiting principles" as well as the Justices' repeated demands for an in-between rule during oral arguments.[184] In their separate opinions, Justices Roberts and Alito emphasized that courts should construe *Riley* narrowly, and Justice Alito noted that he did not see a "workable alternative" to the majority's rule.[185] Thus, in one reading, *Riley* may indicate that the Court is adapting to the times and will not blindly apply law from an earlier age to today's digital media.[186] By another reading, although *Riley* itself was a victory for privacy advocates, the Court is unlikely to be as solicitous about defendants' rights in future cases relying on the reasonableness approach, because the facts in *Riley* were particularly favorable to the defendants.[187] Lacking a more moderate solution, the *Riley* court favored clarity because bright-line rules are particularly valuable for law enforcement: per Alito's concurrence, "[l]aw enforcement officers need clear rules regarding searches incident to arrest."[188]

Riley's reasoning clears the way for even more doctrinal change. "[L]ower courts are on notice" that they should not readily "follow broad statements from pre-digital opinions, even if those opinions emanated from the Supreme Court itself."[189] In his concurrence in *Riley*, Justice Alito noted that "we should not mechanically apply the rule used in the predigital era to the search of a cell phone" and that modern

---

Chosen Freeholders, __ U.S. __, 132 S. Ct. 1510, 1520–23 (2012) (finding that an extensive strip search of all new detainees regardless of the severity of their infractions was reasonable).

183. *Fourth Amendment—Search and Seizure*, *supra* note 180, at 259.

184. *Id.* at 259–60; *see also* S.M., *There's No App for That*, THE ECONOMIST (Apr. 30, 2014, 2:01 PM), http://www.economist.com/blogs/democracyinamerica/2014/04/mobile-phone-privacy [https://perma.cc/X7LK-GS8F]. In oral arguments, the Justices repeatedly demanded an "in-between rule." Transcript of Oral Argument at 38, Riley v. California, __ U.S. __, 134 S. Ct. 2473 (2014) (No. 13-132) (Breyer, J.), http://www.supremecourt.gov/oral_arguments/argument_transcripts/13-132_h315.pdf [https://perma.cc/D4W9-XZ84] (citing *Fourth Amendment—Search and Seizure*, *supra* note 180).

185. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring in part and concurring in the judgment).

186. Michael D. Ricciuti & Kathleen D. Parker, *My Phone Is My Castle: Supreme Court Decides That Cell Phones Seized Incident to Arrest Cannot Be Subject to Routine Warrantless Searches*, 58 B.B.J. 7, 9 (2014).

187. *Fourth Amendment—Search and Seizure*, *supra* note 180, at 260.

188. *Riley*, 134 S. Ct. at 2497 (Alito, J., concurring in part and concurring in the judgment).

189. Richard Re, *Symposium: Inaugurating the Digital Fourth Amendment*, SCOTUS BLOG (June 26, 2014, 12:37 PM), http://www.scotusblog.com/2014/06/symposium-inaugurating-the-digital-fourth-amendment/ [https://perma.cc/GV3D-9PA6?type=image].

technology "calls for a new balancing of law enforcement and privacy interests."[190]

In this vein, the Court rejected the government's reliance on the third-party doctrine's seminal case, *Smith v. Maryland*.[191] Whereas in *Smith*, no Fourth Amendment search occurred, here the Court found there *was* a physical search.[192] The Court additionally refused to permit searches of cell phone data even if law enforcement could have obtained the same information from a pre-digital counterpart, such as a personal journal, found during a search incident to arrest.[193] The third-party doctrine is decades old, and in the light of changing technology, the Court may overrule or substantially modify it.[194] Yet to date, the third-party doctrine stands.[195] In fact, it is the authority under which law enforcement is gaining access to CSLI.[196]

Riley has not produced clarity in the circuit courts on the question of whether a warrant is required to obtain CSLI.[197] Until recently, there was a circuit split, with the Fourth Circuit holding that a warrant was required and the Fifth, Sixth, and Eleventh Circuits holding that no warrant was necessary, as CSLI is information shared with a third party.[198] Indeed, "CSLI does not comfortably fit into any Fourth Amendment line of cases: it is difficult to simply label the data 'records' under the assumption of risk doctrine, or to call a cell phone just a tracking device under *Knotts* or *Karo*."[199] *Riley* "did not address whether

190. *Riley*, 134 S. Ct. at 2496–97 (Alito, J., concurring in part and concurring in the judgment).

191. *Id.* at 2492–93.

192. *Id.* (comparing Wurie's case with the facts in *Smith* and finding that while *Smith* "concluded that the use of a pen register was not a 'search' at all under the *Fourth Amendment* . . . . There is no dispute here that the officers engaged in a search of Wurie's cell phone.") (citations omitted).

193. *Id.*

194. Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 506 (2012).

195. *See, e.g.*, United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *rev'd en banc* United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797, *4 (4th Cir. May 31, 2016) (holding that the government's acquisition of historical CSLI from defendants' cell phone provider did not violate the Fourth Amendment).

196. *Id.*

197. *Cf.* United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015) (holding that a court order compelling the production of a third-party telephone company's business records containing CSLI did not violate the defendant's Fourth Amendment rights); *Graham*, 796 F.3d at 338 (holding that the government's warrantless procurement of CSLI was an unreasonable search in violation of the Fourth Amendment).

198. *C.f.* United States v. Carpenter, 819 F.3d 880, 883 (6th Cir. 2016); *Davis*, 785 F.3d at 500; *Graham*, 796 F.3d at 338; *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

199. Elliott, *supra* note 151, at 15.

the Fourth Amendment applies to remote intrusions of a cell phone, such as the collection of metadata."[200] In *Riley*, the Court "gingerly skirted the legal morass" posed by metadata.[201] It is unclear how *Riley*'s concerns for privacy can be reconciled with the Court's trespass theory from *Jones*, and it thus remains uncertain whether expectations of privacy diminish when the government remotely tracks information.[202]

Justice Sotomayor touched on metadata in her aforementioned *Jones* concurrence,[203] noting that long-term location monitoring can reconstruct someone's specific movements precisely, resulting in a level of information that police would typically need a warrant to obtain: "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[204] Justice Sotomayor's concurrence indicates that she is inclined to require law enforcement to show at least reasonable suspicion before tracking CSLI.[205] Nevertheless, the Court found the vast personal information available in a cell phone seized incident to arrest to be distinguishable from metadata: location does not provide information about a user's applications, photos, or web browsing history. Until the Court addresses the issue, we must look to lower courts and legislatures to find a balance between law enforcement and privacy interests.

c. How the Circuit Courts Have Treated CSLI

The enhanced protections *Riley* afforded cell phone contents have not translated to protections for CSLI in the lower courts. The Fourth, Fifth,

---

200. Adam Lamparello & Charles E. MacLean, *Riley v. California: Privacy Still Matters, But How Much and in What Contexts?*, 27 REGENT U. L. REV. 25, 28 (2014).

201. *Fourth Amendment—Search and Seizure*, *supra* note 187, at 253 n.31.

202. Lamparello & MacLean, *supra* note 200, at 36.

203. *See supra* section II.B.2.

204. Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2490 (2014) (citing United States v. Jones, __ U.S. __, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

205. *See, e.g.*, Terry v. Ohio, 392 U.S. 1, 21 (1968) (establishing the reasonable suspicion standard, which requires law enforcement "to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion"). Several scholars indicate that reasonable suspicion is sufficient for the government to gather metadata. *See* Adam Lamparello & Charles MacLean, Riley v. California*: The New* Katz *or* Chimel*?*, 21 RICH. J. L. & TECH. 1, 23 (2014); Lamparello & MacLean, *supra* note 200, at 27 (asserting that government monitoring of calls or location is only acceptable if government has "good reason . . . often referred to as probable cause or reasonable suspicion").

Sixth, and Eleventh Circuits do not require a warrant for CSLI, finding that it falls under the third-party doctrine.[206]

In *United States v. Davis*, the Eleventh Circuit held that law enforcement may obtain historical cell site location information without a search warrant, because:

> Cell tower location records do not contain private communications of the subscriber. This type of non-content evidence, lawfully created by a third party telephone company for legitimate business purposes, does not belong to [defendant], even if it concerns him . . . . [m]ore importantly, like the bank customer in Miller and the phone customer in Smith, Davis has no subjective or objective reasonable expectation of privacy[.][207]

After a two-month string of robberies leading to Davis's arrest, prosecutors obtained a court order under the SCA for his cell location records during the relevant period.[208] The prosecution introduced these location records at trial, which only tracked Davis to the nearest mile at any given time yet still linked Davis to six of the seven armed robberies for which he stood trial.[209] Davis appealed his conviction, arguing that a warrant should have been required for the cell location records.[210]

The Eleventh Circuit's three-judge panel found that the government's warrantless gathering of CSLI violated Davis's reasonable expectation of privacy under the Fourth Amendment.[211] The en banc panel disagreed, holding that Davis's phone records were indeed third party records for which no warrant was required.[212]

The court distinguished *Davis* from *Jones* and *Katz*.[213] Unlike in *Jones*, in *Davis* the government neither used a GPS device nor physically trespassed.[214] Unlike in *Katz*, where the government recorded conversations without a warrant, in *Davis* the government did not record any conversations.[215] Furthermore, *Davis* did not fulfill the *Katz* test:

---

206. United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797 (4th Cir. May 31, 2016); United States v. Carpenter, 819 F.3d 880, 883 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015); *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

207. *Davis*, 785 F.3d at 528–29.

208. *Id.* at 502.

209. *Id.* at 503–04.

210. *Id.* at 504–05.

211. United States v. Davis, 754 F.3d 1205, 1217 (11th Cir. 2014).

212. *Davis*, 785 F.3d at 518.

213. *Id.* at 505.

214. *Id.*

215. *Id.* at 507 (citing United States v. Katz, 389 U.S. 347, 354–56 (1967)).

Davis had no reasonable expectation of privacy in his phone records since cell phone users are aware that phone companies track their locations.[216] Addressing *Riley*, the Eleventh Circuit found that cell phone location information is categorically different from the cell phone contents at question in *Riley*.[217] Additionally, the *Davis* court notes that the *Riley* court "made a special point of stressing that the facts before it 'do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances'"—i.e. that *Riley* did not address the mosaic theory.[218] The Eleventh Circuit found that changing technology should not be afforded any special considerations under the third-party doctrine:

> If our expectation of privacy in our personal communications has not changed from what it was when we only wrote letters to what it is now that we use telephones to conduct our personal interactions, it has not changed just because we now happen to use email to personally communicate.[219]

The court did not require a warrant for Davis's CSLI, finding that Davis's phone records fell under the third-party doctrine.[220] Although a circuit split existed at the time, the United States Supreme Court denied certiorari to *Davis*.[221]

The Fourth Circuit tracks the Eleventh: as in *Davis*, in *Graham* the three-judge panel ruled that a warrant was required for CSLI, but the en banc court overturned that decision.[222] The panel in *Graham* relied on the mosaic theory to find that, although a single CSLI data point does not constitute a search, a large number of data points (here, 221 days' worth) does.[223] This opinion created a circuit split between the Fifth, Sixth, and Eleventh Circuits (holding no warrant required for CSLI) and the Fourth Circuit (holding until recently that a warrant was required for

---

216. *Id.* at 511. ("[C]ell users know that they must transmit signals to cell towers within range, that the cell tower functions as the equipment that connects the calls, that users when making or receiving calls are necessarily conveying or exposing to their service provider their general location within that cell tower's range, and that cell phone companies make records of cell-tower usage.").

217. *Id.* at 516 n.19.

218. *Id.* (citing Riley v. California, __ U.S. __, 134 S. Ct. 2473 (2014)). The Eleventh Circuit additionally noted that "[i]t is not helpful to lump together doctrinally unrelated cases that happen to involve similar modern technology." *Id.*

219. *Id.* at 528–29.

220. *Id.*

221. *Davis*, 785 F.3d 498 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 479 (2015).

222. United States v. Graham, 796 F.3d 332 (4th Cir. 2015), *rev'd en banc*, United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797 (4th Cir. May 31, 2016).

223. *Graham*, 796 F.3d at 347–349.

CSLI).[224] But the *Graham* en banc panel found that CSLI falls under the third-party doctrine and held that no warrant was required since law enforcement had obtained a court order under the SCA.[225] The en banc decision noted, however, that the United States Supreme Court may overrule the third-party doctrine, as discussed in Section II.A.[226]

The Fifth Circuit similarly found that a court order under the SCA was adequate for CSLI.[227] The Fifth Circuit held that "orders to obtain historical cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional."[228] It also found that historical CSLI is not subject to a reasonable expectation of privacy because users knowingly expose this information to cell providers.[229]

Citing Justice Alito's concurrence in *Jones*, the Fifth Circuit noted that "[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."[230] The court additionally noted that "Congress has crafted such a legislative solution in the SCA," and that the SCA "conforms to existing Supreme Court Fourth Amendment precedent."[231] Thus, the court "decline[d] to create a new rule to hold that Congress's balancing of privacy and safety is unconstitutional."[232]

The Sixth Circuit has ruled that real-time tracking using GPS data from a suspect's cell phone does not implicate the Fourth Amendment when the tracking lasts only a few days—a question left open by *Jones*.[233] The *Skinner* court found that police use of CSLI to track a

---

224. *C.f.* United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); *Graham*, 796 F.3d at 347–49; *Davis*, 785 F.3d at 511–13; *In re* Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

225. *See generally Graham*, 796 F.3d 332, *rev'd en banc*, United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797 (4th Cir. May 31, 2016).

226. *Id.*, 2016 U.S. App. LEXIS 9797, at *5–6.

227. *Historical Cell Site Data*, 724 F.3d at 611–15.

228. *Id.* at 615 (emphasis omitted).

229. *Id.* at 613, 615 (noting that users likely do not have a reasonable expectation of privacy in their cell location information). *See also* United States v. Guerrero, 768 F.3d 351, 360–61 (5th Cir. 2014) (noting that the academic debate created post-*Riley* does not affect lower court precedent, under which CSLI still falls under the third party doctrine).

230. *Historical Cell Site Data*, 724 F.3d at 614 (quoting United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring)).

231. *Id.*

232. *Id.* at 615.

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

defendant's movements along public highways did not violate the Fourth Amendment because individuals have no reasonable expectation of privacy in their public movements.[234] Furthermore, the court compared a cell phone that has tracking capabilities to the location beeper that law enforcement planted in a barrel of ether in *Karo*—in both cases, defendants obtained the object with a tracking device already present.[235] Because the defendant voluntarily purchased a phone with tracking, he eroded his own reasonable expectation of privacy; thus, the police could use those tracking capabilities to track him along public roads.[236]

Unlike the topic of CSLI use, there are few cases involving use of StingRays.[237] Although there was speculation that the United States Supreme Court would grant certiorari to the *Davis* case in order to follow *Riley* with a decision on metadata, the Court denied certiorari—as in *Jones*, sidestepping the issue.[238] Both courts and privacy advocates assert that technology has ushered civil liberties into the virtual world, and the law must adapt by "providing legal protections to individuals who speak, associate, and assemble in that world."[239] Since existing jurisprudence leaves that question open, and a circuit split no longer exists to increase the likelihood of United States Supreme Court review, this Note seeks to show how to afford adequate legal protections to individuals in the absence of United States Supreme Court action.

234. *Id.* at 778.

235. *Id.* at 781 (citing United States v. Karo, 468 U.S. 705 (1984)).

236. *Id.* at 777.

237. Another relevant decision notable only for the confusion it lends is the Third Circuit's opinion concluding that historical location information generally may be obtained without a search warrant but that a court could require a warrant under some circumstances. *See In re* United States for an Order Directing Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010).

238. Mary-Elizabeth M. Hadley, *A Circuit Split Emerges: At Least for Now, the Protection Afforded to Cell Location Information Depends on Where You Are*, CAVEAT VENDOR BLOG (Aug. 10, 2015), http://www.lexology.com/library/detail.aspx?g=f9fa2829-d608-474e-a525-085b1cceb74c [https://perma.cc/29C7-3XP7]; Editor's Blog, *Circuit Split: Eleventh Circuit Creates Division on Standard to Obtain Cell Site Location Information*, FED. EVID. REV. (June 19, 2014), http://federalevidence.com/blog/2014/june/circuit-split-eleventh-circuit-creates-division-standard-obtain-cell-site-location-in [https://perma.cc/4FVD-N8JP].

239. Lamparello & MacLean, *supra* note 208, at 20.

III. LEGISLATIVE SUPPLEMENTATION OF JUDICIAL STANDARDS

Following the Court's decisions establishing the third-party doctrine,[240] Congress enacted federal legislation that goes above the constitutional baseline in protecting communications.[241] Title III, the SCA, and the Pen/Trap statute are examples of when Congress has stepped in to supplement the Court's Fourth Amendment jurisprudence. These federal statutes prescribe protections for various technology-related searches. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 regulates wiretapping and eavesdropping;[242] the SCA regulates the search and interception of electronic communications;[243] and the Pen/Trap Statute regulates the use of pen registers to capture numbers dialed from a telephone.[244]

Title III, enacted in the wake of the Court's decisions in *Katz* and *Berger*, regulates nonconsensual interception of oral, wire, or electronic communications.[245] Most states have enacted additional statutes subsequent to Title III.[246] Title III was written to provide uniform rules for law enforcement engaging in wiretapping or eavesdropping, to comply with United States Supreme Court precedent, and to protect the privacy of communications.[247] It includes procedural and substantive safeguards that surpass constitutional requirements.[248] In addition, Title III requires that law enforcement have not only probable cause to obtain a wiretap, but also particularization of the person and place to be wiretapped, as well as limitations on time and types of conversations to be seized.[249]

The SCA regulates government access to the contents of electronic communications held by third parties, such as phone companies and internet service providers.[250] It is one of the primary mechanisms

240. *See supra* Part II.A.

241. *See generally* 18 U.S.C. §§ 2510–2522 (2012); §§ 2701–2712; §§ 3121–3127.

242. §§ 2510–2522.

243. §§ 2701–2712.

244. §§ 3121–3127.

245. *See* §§ 2510–22.

246. RONALD J. ALLEN ET AL., CRIMINAL PROCEDURE: INVESTIGATION AND RIGHT TO COUNSEL 901 (Wolters Kluwer, 2d ed. 2011).

247. *Id.* at 901–02.

248. *Id.*

249. *Id.*

250. 18 U.S.C. §§ 2701–2712 (2012).

currently regulating CSLI.[251] The SCA criminalizes unauthorized access to users' stored communications,[252] restricts providers from sharing those communications,[253] and regulates the government's requests for data governed by the SCA.[254] For non-content information, such as a user's account details, address, or credit card number, only a subpoena is required.[255] For transactional records, such as a list of addresses to which an individual has sent emails or phone numbers an individual has called, the SCA requires a court order showing "reasonable grounds to believe that the . . . information sought [is] relevant and material to an ongoing criminal investigation."[256] This court order is an intermediate evidentiary standard: lower than the probable cause requirement of a warrant, but higher than a subpoena.[257] Many courts have ruled CSLI accessible with a court order under the SCA.[258] Courts that allow historical CSLI access under the SCA treat CSLI as a transactional record and require only a court order.[259]

The Pen/Trap statute,[260] like the SCA, provides "that law enforcement agencies may record and store indefinitely all of the digits dialed from a specific telephone without a warrant, without notification to the user, and without a showing of probable cause."[261] The Pen/Trap Statute regulates law enforcement's use of pen registers (which record the phone numbers a telephone user dials) and trap-and-trace devices (which perform the opposite function, recording the digits of all incoming calls to a given telephone).[262] Though pen registers were once used only for telephone communications, they are now used for a variety of electronic media.[263]

---

251. Ross, *supra* note 32, at 1197.

252. 18 U.S.C. § 2701 (2012).

253. 18 U.S.C. § 2702 (2012).

254. 18 U.S.C. § 2703 (2012).

255. *Id.*

256. *Id.*

257. S. REP. NO. 103-402, at 31 (1994).

258. Fraser, *supra* note 33, at 585.

259. Ross, *supra* note 32, at 1199.

260. 18 U.S.C. §§ 3121–3127 (2012).

261. Marcus M. Baldwin, Note, *Dirty Digits: The Collection of Post-Cut-Through Dialed Digits Under the Pen/Trap Statute*, 74 BROOKLYN L. REV. 1109, 1109 (2009).

262. *Id.* at 1109 n.3; 18 U.S.C. §§ 3121–3127 (2012) (collectively the "Pen/Trap Statute"). For the statutory definition of a pen register, see § 3127(3).

263. Baldwin, *supra* note 261, at 1109.

In the case of cell phones, pen registers can calculate a user's physical location or track their movements in real time.[264] Courts have approved court orders under the Pen/Trap Statute for technology that eavesdrops on actual phone conversations as well as for technology that monitors URLs that a suspect visited and addresses he emailed.[265] This shows that the classification of a device as a pen register is "primarily functional"—use of the statute is not inextricably linked to the use of an actual pen register.[266] But the pen register statute itself mandates that information gathered "shall not include the contents of any communication . . . ."[267] Indeed, courts have found that actual pen registers pose a lesser threat to privacy than traditional wiretaps because pen registers cannot reveal the contents of a communication.[268] This follows the holding in *Smith v. Maryland* that Fourth Amendment protections do not apply to dialed digits.[269] For these reasons, the government has relied on *Smith* to support CSLI collection.[270]

Title III, the SCA, and the Pen/Trap statute show that when Congress has intervened to provide greater privacy for communications above the constitutional baseline, it still has not required a warrant for non-content communication. Instead, Congress requires court orders or subpoenas.

IV. LEGISLATIVE SOLUTIONS FOR CSLI AND STINGRAY USE

Given that law enforcement's use of CSLI is a controversial and pressing issue, what should be done about its use? As noted above, the United States Supreme Court has refrained from addressing the issue of metadata,[271] and the Court recently denied certiorari in a case that would have resolved the issue of whether warrants are required for CSLI.[272]

---

264. *Id.* at 1113.

265. People v. Kramer, 706 N.E.2d 731, 737 (N.Y. 1998) (holding that if a device's digital and audio functions were "sufficiently discrete" and there was only a remote likelihood of misuse, the presence of audio-capable technology would not disqualify a device from use as a pen register); United States v. Forrester, 512 F.3d 500, 504, 510 n.6 (9th Cir. 2008) (holding that a Pen/Trap court order allowed law enforcement to obtain defendant's URLs visited and addresses emailed).

266. Baldwin, *supra* note 261, at 1114.

267. 18 U.S.C. §3127(3). *See also* § 3121(c), also requiring that no communication contents be captured.

268. United States v. New York Tel. Co., 434 U.S. 159, 165–68 (1977).

269. Smith v. Maryland, 442 U.S. 735 (1979); *see also* Smith v. State, 389 A.2d 858, 868 (Md. 1978) (state court of last resort holding).

270. Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y. 757, 866–67, 871 (2014).

271. *See supra* Part II.B.2.ii.

272. *See* United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc).

This may indicate that the Court is not ready to address the metadata issue. Until the Court does, there is no clear rule for how location information is protected.

In the absence of Court action, a legislative solution is appropriate. In *Riley*, Justice Alito made a strong suggestion for legislation in his concurrence, stating he "would reconsider the question presented here if either Congress or state legislatures . . . enact legislation that draws reasonable distinctions . . . ."[273] Some courts point out that establishing "bright-line rules regarding legal protection for . . . CSLI is a task for the legislature, which is better suited to striking a delicate balance between the needs of law enforcement and the civil liberties of American citizens."[274]

The legislature is better suited than the courts to solve this issue because it is not bound by its own precedent; it can better assess facts; and it can act quickly to reflect the changes and expansions in technology.[275] It is better to formulate privacy law by legislation because, unlike the courts, legislatures can pass sweeping but intricate laws.[276] While courts are limited to developing rules based on the cases that come to them, legislatures can tailor laws to a wide range of circumstances and are not bound by stare decisis.[277] Courts adjudicate past disputes, which means that judicial holdings on issues of technology or other fast-changing subjects tend to be "outdated on arrival," whereas legislatures can simultaneously address both present and future concerns.[278]

Historically, congressional action is unlikely: multiple efforts to regulate CSLI have stalled.[279] In 2012 a bipartisan group of Senators proposed a bill regulating CSLI.[280] In 2015, the group reformulated the

---

273. Riley v. California, __ U.S. __ 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring).

274. Ross, *supra* note 32, at 1212, *citing In re* United States for an Order Authorizing the Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 585 (E.D.N.Y. 2010).

275. Orin Kerr, *Governor Brown Vetoes Bill on Searching Cell Phones Incident to Arrest*, VOLOKH CONSPIRACY (Oct. 10, 2011, 2:39 PM), http://www.volokh.com/2011/10/10/governor-brown-vetoes-bill-on-searching-cell-phones-incident-to-arrest/ [https://perma.cc/7LBF-NMHL].

276. *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004).

277. Schlabach, *supra* note 133, at 699.

278. *Id.*

279. *See* Elliott, *supra* note 151, at 3; Robinson Meyer, *Do Police Need a Warrant to See Where a Phone Is?*, THE ATLANTIC (Aug. 8, 2015), http://www.theatlantic.com/technology/archive/2015/08/warrantless-cell-phone-location-tracking/400775/ [https://perma.cc/3LT4-LUSR] ("[A] bipartisan bill about CSLI has lingered in [Congress'] higher chamber for years").

280. Cybersecurity Act of 2012, S. 3414, 112th Cong. (2012) (amendment proposed by Wyden), https://www.wyden.senate.gov/download/?id=081B52AA-0F9B-4B5E-88C2-911CF39E6D86

bill as the Geolocation Privacy and Surveillance Act, which would require law enforcement to obtain a warrant before acquiring an individual's geolocation information.[281] Despite these efforts, there is an intractable debate between privacy advocates and law enforcement over appropriate legislative reform, which continuously prevents federal legislation regulating CSLI from passing.[282] Thus, the prospect of congressional action is far from certain.

Since Congress is either unwilling or unable to pass an appropriate legislative solution, state legislatures should step in. Not only are states more nimble in addressing the technology questions that paralyze Congress, they also accommodate differing local tastes for the balance between privacy and effective law enforcement.[283]

Furthermore, state legislation is necessary to regulate police policy at the local level. According to data maintained by the ACLU, there is no clear consensus among states about how to treat CSLI.[284] Even individual states have yet to determine statewide StingRay policies: for example, in Washington State, the Seattle Police Department does not use StingRays, but the nearby Tacoma Police Department does.[285] Federally, the Justice Department and the IRS have recently begun to require warrants.[286] In the absence of Congressional action, state

---

&download=1 [https://perma.cc/4WBJ-YMCZ]; *see also* Ron Wyden, *Amendments Offered to the Cybersecurity Act of 2012* (July 30, 2012), https://www.wyden.senate.gov/news/blog/post/cybersecurity-act-of-2012 [https://perma.cc/GUP5-BYQN].

281. Geological Privacy and Surveillance Act (GPS Act), S. 237, 114th Cong. (2015), https://www.wyden.senate.gov/priorities/gps-act [https://perma.cc/BSK7-6VAZ].

282. Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 123–24 (2012).

283. *See, e.g.*, Schlabach, *supra* note 133, at 699.

284. The status of the law is as follows: no warrant requirement in fourteen states, location information is unprotected in nineteen states and the District of Columbia, "some protections" in three states (indicating that "judges have discretion to require warrant for historical CSLI"), and a warrant required for *all* cell phone location information in six states. Robinson Meyer, *Where Americans Can Be Tracked Without a Warrant*, THE ATLANTIC (Nov. 12, 2015), http://www.theatlantic.com/technology/archive/2015/11/where-americans-can-be-tracked-without-a-warrant/415461/ [https://perma.cc/K3U8-FR6B].

285. Ansel Herz, *Seattle Police Deny Having or Using "Stingray" Data Sucking Device*, THE STRANGER (Aug. 28, 2014, 1:22 PM), http://slog.thestranger.com/slog/archives/2014/08/28/seattle-police-deny-having-or-using-StingRay-cell-phone-data-sucking-device [https://perma.cc/84PK-YR9X]; Martin, *supra* note 3.

286. Nicholas Fandos, *Justice Dept. to Require Warrants for Some Cellphone Tracking*, N.Y. TIMES (Sept. 3, 2015), http://www.nytimes.com/2015/09/04/us/politics/justice-dept-to-require-warrants-for-some-cellphone-tracking.html [https://perma.cc/VW87-EMES]; Ron Wyden, *IRS Commits to Follow Justice Department Guidelines on StingRays in Letter to Wyden* (Dec. 1, 2015),

legislatures can ensure a clear standard at the local level.[287] Some states, including Washington, have stepped up to the challenge.[288]

This Note details three separate approaches for potential legislation. The options are as follows: require no warrant or other judicial approval, require a court order based on reasonable suspicion, or, the most protective, require a warrant based on probable cause.

A. Require No Warrant

As of 2015, seventeen states had not passed legislation that required any showing of suspicion, through either a court order or a warrant, for StingRays.[289] Without legislation, Americans are limited to the minimum constitutional protection. The circuit courts that have addressed this issue require no warrant for CSLI collection: under their interpretation, CSLI is information voluntarily conveyed to a third party.[290] These courts find that CSLI falls under the third-party doctrine and therefore is not subject to Fourth Amendment protection.[291] Beyond

---

https://www.wyden.senate.gov/news/press-releases/irs-commits-to-follow-justice-department-guidelines-on-StingRays-in-letter-to-wyden [https://perma.cc/TND7-ZWD5].

287. Larry Greenemeier, *What Is the Big Secret Surrounding StingRay Surveillance?* SCI. AMERICAN (June 25, 2015), http://www.scientificamerican.com/article/what-is-the-big-secret-surrounding-StingRay-surveillance/ [https://perma.cc/856A-9LSS] ("You're dealing with outdated statutes concerning new and very different technology. It's possible in five years maybe that Congress will step in and do something. More likely, state legislatures will take most of the action to monitor this type of surveillance. Washington State, California [and others] have already acted, and Texas is evaluating the standards for approving StingRay use.").

288. WASH. REV. CODE § 9.73.260 (West 2015).

289. *Status of Location Privacy Legislation in the States: 2015*, ACLU (Aug. 26, 2015), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015 [https://perma.cc/5VB4-QHVV] (discussing relevant legislation in Georgia, Kansas, Mississippi, Missouri, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, Tennessee, Texas, Vermont, West Virginia and Wisconsin. Currently these states are at a constitutional minimum, but may soon legislate to provide enhanced constitutional protections, as this is a quickly changing area of law.).

290. United States v. Graham, Nos. 12-4659, 12-4825, 2016 U.S. App. LEXIS 9797, at *13 (4th Cir. May 31, 2016) (en banc); United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015) (en banc); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

291. *See Graham*, 2016 U.S. App. LEXIS 9797, at *4 (noting that "[a]ll of our sister circuits to have considered the question have held, as we do today, that the government does not violate the *Fourth Amendment* when it obtains historical CSLI from a service provider without a warrant [under the third party doctrine].").

these circuit court decisions, additional law enforcement departments currently rely on the third-party doctrine to gather warrantless CSLI.[292]

The third-party doctrine applies to CSLI under the theory that the cell phone user voluntarily conveys a phone's location information to the cell provider.[293] Cell phone users understand that, for billing and general use purposes, they must convey their location information to the provider.[294] This awareness is reflected not only by cell phone bills but also by common knowledge. Under this interpretation, CSLI is not subject to constitutional protection.

Proponents of this position argue that cell phone users are readily aware that their CSLI information is available to others.[295] According to the Pew Research Center, more than half of "app" users have uninstalled or decided not to install an app due to concerns about their personal information being shared.[296] Additionally, one in five cell phone owners have turned off the location tracking feature on their phone, and one in three have cleared their cell phone browsing or search history.[297] These actions indicate that cell phone users know that the government may collect their information and that they can take steps to protect that information.[298] It is under this rationale that the circuit courts found no subjective or objective expectation of privacy in CSLI.[299]

Conversely, the third-party doctrine may not apply to StingRays. StingRays may not comply with *Karo's* enhanced privacy afforded to the home: "'[n]o matter how the StingRay is used—to identify, locate or intercept—they always send signals through the walls of homes,' which should trigger a warrant requirement" since the signals "penetrate a

---

292. *See, e.g.*, Mathew Keys, *California Cops Used Stingrays 300 Times Without Warrant*, THE BLOT (May 28, 2015), https://www.theblot.com/report-california-cops-used-stingrays-300-times-without-warrant-2-7744246 [https://perma.cc/R4LK-A7BG].

293. Kyle Malone, Comment, *The Fourth Amendment and the Stored Communications Act: Why the Warrantless Gathering of Historical Cell Site Location Information Poses No Threat to Privacy*, 39 PEPP. L. REV. 701, 739 (2012).

294. *Id.*

295. *Graham*, 2016 U.S. App. LEXIS 9797, at *10–12.

296. Pew Research Center, *supra* note 15.

297. *Id.*

298. *See The Problem with Mobile Phones*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/en/module/problem-mobile-phones [https://perma.cc/2CUQ-Y99Z] (describing mobile phone privacy and how to get more of it).

299. *Graham*, 2016 U.S. App. LEXIS 9797 at *13; United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 511–13 (11th Cir. 2015) (en banc); *In re* Application of United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

space protected by the Fourth Amendment."[300] Under this theory, *Karo* precludes the third party analysis, since the government cannot use technology to access information about the inside of a person's home without obtaining a warrant.[301]

B. Require a Court Order Based on Reasonable Suspicion

While the Fourth, Fifth, Sixth, and Eleventh Circuits did not require a warrant for CSLI, the officers in all cases had obtained court orders to gather CSLI pursuant to the SCA.[302] A court order requirement is the middle ground between no warrant and a full warrant, since individuals have already "exposed" their CSLI information by using a cell phone, reducing their expectation of privacy therein.[303]

Requiring a court order based on reasonable suspicion is the moderate approach, but no state legislature has adopted it yet.[304] The rationale supporting a court order standard tracks Congress' intent in adopting the SCA.[305] With the SCA, Congress sought a "fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies."[306] The SCA, which requires a court order to access electronic non-content data,[307] was written to protect privacy lest it "gradually erode as technology advances."[308]

Search warrants require probable cause, but under typical definitions, subpoenas and court orders do not.[309] A court order generally requires specific and articulable facts showing that there are reasonable grounds to believe that the records or other information sought is relevant and material to an ongoing criminal investigation.[310] Reasonable suspicion

---

300. Ellen Nakashima, *Little-Known Surveillance Tool Raises Concerns by Judges, Privacy Activists*, WASH. POST (Mar. 27, 2013), https://www.washingtonpost.com/world/national-security/little-known-surveillance-tool-raises-concerns-by-judges-privacy-activists/2013/03/27/8b60e906-9712-11e2-97cd-3d8c1afe4f0f_story.html [https://perma.cc/9F6R-7JE9] (quoting Chris Soghoian).

301. United States v. Karo, 468 U.S. 705, 716 (1984).

302. *Graham*, 2016 U.S. App. LEXIS 9797 at *13; *Davis*, 785 F.3d at 511–13; *Carpenter*, 819 F.3d at 886; *Historical Cell Site Data*, 724 F.3d at 615.

303. *Graham*, 2016 U.S. App. LEXIS 9797 at *12; *see also id.*at *16–22.

304. ACLU, *supra* note 289.

305. S. REP. NO. 99-541, at 5 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3358.

306. *Id.*

307. 18 U.S.C. § 2703 (2012).

308. S. REP. NO. 99-541, at 5.

309. Fishman, *supra* note 58, at 1010.

310. 18 U.S.C. §2703(d) (2002).

means that the police, acting under a reasonable person standard, have specific and articulable facts connecting a suspect to criminal activity. In contrast, a warrant requires probable cause, meaning a reasonable person under the circumstances would believe that a crime either had been or was about to be committed.[311]

Thus the reasonable suspicion required by a court order is an intermediate standard, below probable cause but above the *mere relevance* standard required for federal use of a pen register or trap-and-trace device.[312] Professor Orin Kerr, a scholar well-versed in these issues, approves of a reasonable suspicion standard even for content data, which has traditionally received more protection than metadata.[313]

C. Require a Warrant Based on Probable Cause

Requiring a warrant based on probable cause was, until recently, an uncommon solution.[314] A warrant based on probable cause ensures heightened privacy protections for CSLI.[315] Under this approach, law enforcement would fill out a standard form describing the nature of the search, the place to be searched, and the items to be "seized" (here, location information).[316] The requesting officer would need to detail the probable cause linking the items to be seized with a particular endeavor and the specified location.[317]

Advocates for a full warrant requirement argue that tracking CSLI enables the government to track a defendant across public and private spaces and discover some of the private activities and personal habits of the user.[318] Under this analysis, cell phone users have a reasonable

311. *See supra* text accompanying note 39.

312. *In re* United States for an Order Directing Provider of Elec. Commc'n. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010).

313. 18 U.S.C. §2703(d) (2012); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1234–35 (2004); *see also* discussion of Fourth Amendment protections of content data, *supra* Part III.

314. Kim Zetter, *New Bill Would Force Cops to Get Stingray Warrants*, WIRED MAG. (Nov. 3, 2015, 3:27 PM), https://www.wired.com/2015/11/new-bill-would-force-cops-to-get-warrants-before-spying-with-stingrays/ [https://perma.cc/EW88-E4PB] (noting widespread use of Stingrays without a warrant, and the new warrant requirement).

315. The Fourth Amendment requires that warrants be issued based on probable cause. U.S. CONST. amend. IV.

316. Andrew D. Huynh, Note, *What Comes After "Get a Warrant": Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 CORNELL L. REV. 187, 197 (2015).

317. *Id.*

318. United States v. Graham, 796 F.3d 332, 345 (4th Cir. 2015).

expectation of privacy in their aggregate location information, so a warrant based on probable cause should be required.[319]

A full warrant has traditionally been required for *content* searches of homes and even of cell phones.[320] Location information, however, is not content data; it merely discloses where an individual is at a given time, providing much less information about a person than the contents of their home or the contents of communications on their phone. Even those advocating for a general warrant requirement for CSLI note that serious crimes, such as terrorism and kidnappings, should be exceptions to a general warrant requirement for CSLI.[321] Yet the United States Supreme Court has repeatedly refused to differentiate between the seriousness of different crimes in determining when probable cause is required.[322] A full warrant requirement could therefore be an undue burden on law enforcement, as it would require the highest level of privacy protection at an early stage of the investigation—when officers are unlikely to have enough evidence to obtain a warrant.

D. Examples of Enacted Legislation

Washington, California, Virginia, Minnesota, Utah, and the Department of Justice have adopted statutes and policies regulating law enforcement's use of cell site simulators.[323] The DOJ policy requires law enforcement to include all of the information required under a federal pen register order[324] when applying to use a cell site simulator.[325] The

---

319. *Id.*

320. Riley v. California, __ U.S. __, 134 S. Ct. 2473 (2014) (unless an exception to the warrant requirement applies).

321. Elliott, *supra* note 151, at 15.

322. ALLEN, *supra* note 246, at 432–35; Jeff Welty, *Probable Cause: The Same for All Crimes?*, N.C. CRIM. L. (June 28, 2011), http://nccriminallaw.sog.unc.edu/probable-cause-the-same-for-all-crimes/ [https://perma.cc/WS2R-2M3N].

323. *See* CAL. GOV'T CODE. § 53166 (West 2016); MINN. STAT. § 626A.42 (West 2014); UTAH CODE ANN. § 77-23c-102 (West 2016); VA. CODE ANN. 19.2-70.3 (West 2016); WASH. REV. CODE § 9.73.260 (West 2015); Matthew McCoy, *New StingRay Policies for Both Washington State and the Department of Justice*, WASH. J.L., TECH. & ARTS BLOG (Oct. 14, 2015), https://wjlta.wordpress.com/2015/10/14/new-StingRay-policies-for-both-washington-state-and-the-department-of-justice/ [https://perma.cc/AHK8-K9SC]. *See also* HB 1408, 2015 Gen. Assemb., Reg. Sess. (Va. 2015), https://www.richmondsunlight.com/bill/2015/hb1408/ [https://perma.cc/W4N8-44NG]; Sub. HB 5640, 2016 Gen. Assemb., Reg. Sess. (Ct. 2016), https://www.cga.ct.gov/2016/ACT/pa/2016PA-00148-R00HB-05640-PA.htm [https://perma.cc/PGX4-LJXG]; SB 178, 2015 Leg., Reg. Sess. (Ca. 2015), https://leginfo. legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB178 [https://perma.cc/4NYD-9H97].

324. 18 U.S.C. § 3123 (2012).

325. McCoy, *supra* note 323.

DOJ's policy also "follows Washington's lead" on data retention and deletion, requiring the application to detail how the data will be collected and that it will be disposed of within 30 days.[326]

Washington's efforts in this area are of note because Washington has historically been more protective of privacy than other jurisdictions.[327] After the United States Supreme Court held that individuals had no reasonable expectation of privacy in the contents of garbage left on their curb for collection,[328] the Washington State Supreme Court granted greater protections, holding that an officer's search of a suspect's trash required a warrant.[329] The Washington Constitution surpasses the protections against unreasonable search and seizure afforded by the Fourth Amendment.[330] Article I section 7, which provides that "[n]o person shall be disturbed in his [or her] private affairs, or his home invaded, without authority of law," protects people from warrantless searches.[331] The Washington legislature's solution to CSLI and StingRay use is based in enhanced privacy protections, and has been lauded by privacy advocates.[332]

1. Details of the Washington Statute

The Washington legislation requires a court order for StingRays under the pen register statute, based on probable cause.[333] The Washington statute is "one of the most aggressive anti-tracking measures in the nation."[334] Washington's heightened concerns and protections of privacy surpass that of the majority of states, which have not imposed privacy requirements beyond those required by the Fourth

326. *Id.*

327. State v. Boland, 115 Wash. 2d 571, 577–78, 800 P.2d 1112, 1115 (1990) (discussing historical protections that the Washington State Supreme Court has imposed under article 1, section 7 of the Washington State Constitution, beyond those provided by the Fourth Amendment).

328. California v. Greenwood, 486 U.S. 35, 43–45 (1988).

329. Boland, 115 Wash. 2d at 578–80, 800 P.2d at 1116–17.

330. WASH. CONST. art. I, § 7.

331. *Id.*

332. Cyrus Farivar, *Cops Must Now Get a Warrant to Use Stingrays in Washington State*, ARS TECHNICA (May 12, 2015, 6:49 AM), http://arstechnica.com/tech-policy/2015/05/cops-must-now-get-a-warrant-to-use-stingrays-in-washington-state/ [https://perma.cc/HPV9-HJZR].

333. WASH. REV. CODE § 9.73.260 (West 2015).

334. Russell Brandom, *Washington State Will Require a Warrant for Stingray Cell-Phone Tracking*, THE VERGE (May 12, 2015), http://www.theverge.com/2015/5/12/8591491/StingRay-cell-phone-trackers-washington-state-law-tacoma [https://perma.cc/SY5J-RASC].

Amendment.[335] Indeed, the ACLU has lauded Washington's leadership in regulating StingRays.[336]

The amendment expands Chapter 9.73 of the Revised Code of Washington to require either informed consent or a warrant based on probable cause for general collection of a person's electronic data or metadata.[337] The regulations applicable to pen registers and trap-and-trace devices now extend to regulate cell site simulators: law enforcement must obtain a warrant to install and use a cell site simulator, unless there is "probable cause to believe an emergency exists."[338]

When applying for a warrant to use a StingRay, law enforcement must provide an extensive list of precise information to the issuing judge.[339] This information includes: (A) the telephone or account number the officers or agents are trying to trace; (B) the physical location of the device sought (if known); (C) the type of device the officers or agents are trying to trace; (D) the geographic area where the StingRay will be used; (E) all categories of metadata, data, or information that will be collected; (F) whether or not the device will collect that data of third parties; and (G) any disruptions to communications that the device may cause.[340] As further protection, the statute requires law enforcement to proactively limit and immediately delete any third party data collected.[341] They must also delete the suspect's metadata within thirty days, unless there is probable cause to suggest that the metadata provides evidence of a crime.[342]

Washington's requirement that law enforcement explain StingRay technology to judges approving use of the devices is in keeping with privacy advocates' admonitions that "if the government wants to use invasive surveillance technology like [StingRays], it must explain the

---

335. *See* Jack L. Landau, *Should State Courts Depart from the Fourth Amendment? Search and Seizure, State Constitutions, and the Oregon Experience*, 77 MISS. L.J. 369, 373 n.17 (2007).

336. *Washington Becomes a Leader in Restricting Use of Invasive Stingrays*, ACLU (May 13, 2015), https://www.aclu.org/news/washington-becomes-leader-restricting-use-invasive-stingrays [https://perma.cc/3L4P-5NCS]. As of the editing of this Note, Virginia, Connecticut, and California have followed suit. *See supra* note 323.

337. WASH. REV. CODE § 9.73.260 (West 2015).

338. S. REP. NO. 1440, 2015 Reg. Sess., (Wa. 2015) http://app.leg.wa.gov/documents/billdocs/2015-16/Htm/Bill%20Reports/Senate/1440-S.E%20SBR%20LAW%2015.htm [https://perma.cc/QX5A-XZFL] (Note that the statute contains an emergency situation exception to the warrant requirement).

339. WASH. REV. CODE § 9.73.260 (4)(c)(ii) (West 2015).

340. *Id.*

341. WASH. REV. CODE § 9.73.260 (6)(c) (West 2015).

342. *Id.*

technology to the courts so they can perform their judicial oversight function as required by the Constitution."[343] Understanding the technology is "critical to deciding who may possess and use cell site simulators, to what extent, and for what purposes."[344] Under the statute, the requested warrant must clearly explain the technology to the issuing magistrate.[345]

A statute requiring law enforcement to describe how StingRays work is helpful because it reduces the societal costs of secrecy around the technology.[346] The less the public knows about the workings, availability, and use of StingRays, the less demand the public creates for secured communications.[347] This accordingly increases individuals' risk of being intercepted.[348] The FBI's response to this concern is that over-disclosure of CSLI technology will enable criminals and terrorists to thwart investigations by modifying their behavior.[349] Yet many agents are still using StingRays with a pen register application that does not explain the use of the technology, and there are multiple reports of judges approving pen register orders without knowing that they are actually approving StingRay use.[350] Leaving judges in the dark as to what they are approving could lead to general noncompliance by magistrates or burdensome litigation to overturn improperly obtained court orders.[351]

---

343. Linda Lye, *In Court: Uncovering Stingrays, A Troubling New Location Tracking Device*, ACLU BLOG (Oct 22, 2012, 12:45 PM), https://www.aclu.org/blog/court-uncovering-stingrays-troubling-new-location-tracking-device [https://perma.cc/CZ9R-DSLP].

344. Hardman, *supra* note 21, at 28.

345. WASH. REV. CODE § 9.73.260 (4)(c)(ii)(C) (West 2015).

346. *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret StingRay's No Secret Anymore: The Vanishing Government Monopoly Over Cell Phone Surveillance and Its Impact on National Security and Consumer Privacy*, 28 HARV. J. L. & TECH. 1, 6–7 (2014).

347. *Id.*

348. *Id.*

349. Affidavit of FBI Supervisory Special Agent Bradley S. Morrison, Chief, Tracking Technology Unit, Operation Technology Division in Quantico Division, at 2, Apr. 11, 2014, attachment to City's Verified Answer, Hodai v. City of Tucson, No. C20141225 (Ariz. Sup. Ct. Apr. 14, 2014).

350. *See* Nakashima, *supra* note 300; E-mail from Miranda Kane, Chief, Criminal Div., U.S. Attorney's Off. N.D. Cal., to USACAN-Attorneys-Criminal, U.S. Dep't of Justice (May 23, 2011, 11:55 AM), https://www.aclu.org/files/assets/doj_emails_on_stingray_requests.pdf [https://perma.cc/3VUR-TNQH].

351. *See, e.g.*, Martin, *supra* note 3.

2. Other State Statutes

Like Washington, California, Minnesota, Utah, and Virginia require a warrant for both historical and real-time CSLI.[352] The statutes are substantially similar, with differences as noted below.

California requires a high level of public disclosure: in order for an agency to acquire a StingRay, the local legislative body must approve the acquisition at a public meeting.[353] Once the agency has acquired the device, they must provide conspicuous public notice of the acquisition on their department's website.[354]

Minnesota, Utah, and Virginia explicitly list the permissible exceptions to the warrant requirement.[355] Minnesota permits officers to obtain location information without a tracking warrant when the device is lost or stolen; when the owner has called to request emergency services or has given affirmative consent to the search; or in another emergency situation involving risk of death or serious physical harm.[356] Utah does not require a warrant if the owner has reported the device stolen; has consented to the search; has "voluntarily and publicly disclosed the location information;" or if there is a judicially recognized exception to the warrant requirements, such as exigent circumstances.[357] Virginia follows in the same vein, but also allows a user's legal guardian or next of kin to consent to a StingRay search if they believe that the user is in personal danger.[358]

Some states with a warrant requirement allow for a grace period. The Washington statute grants a grace period to officers who use a StingRay without a warrant: they have forty-eight hours within which to obtain court authorization.[359] If they fail to obtain authorization, the evidence gathered is not admissible in a legal proceeding.[360] Virginia grants a longer grace period of three days.[361] None of the other states grants any grace period, requiring officers to either obtain a warrant or lose any

352. CAL. GOV'T CODE. § 53166 (West 2016); MINN. STAT. § 626A.42 (West 2014); UTAH CODE ANN. § 77-23c-102 (West 2016); VA. CODE ANN. § 19.2-70.3 (West 2016); WASH. REV. CODE § 9.73.260 (West 2015).

353. CAL. GOV'T CODE. § 53166(c)(1) (West 2016).

354. CAL. GOV'T CODE. § 53166(c)(2).

355. MINN. STAT. § 626A.42; UTAH CODE ANN. § 77-23c-102; VA. CODE ANN. § 19.2-70.3.

356. MINN. STAT. § 626A.42(b)(1)-(5).

357. UTAH CODE ANN. § 77-23c-102(2)(a).

358. VA. CODE ANN. § 19.2-70.3(E)(3).

359. WASH. REV. CODE § 9.73.260(6)(a) (West 2015).

360. *Id.*

361. VA. CODE ANN. § 19.2-70.3(E)(4).

evidence collected. Once a judge issues a warrant, both Virginia and Washington limit the tracking period to thirty days, subject to possible extension in additional thirty-day periods.[362]

While the only penalty provided by Washington for violating the statute is a gross misdemeanor charge,[363] California expressly provides for actual damages of no less than $2,500, with potential awards of punitive damages and attorney's fees.[364] Utah, while not providing any specific penalties, does create a safe harbor for phone companies that comply with law enforcement requests.[365]

These differences are likely a byproduct of the drafting process of each statute: while Washington amended its pen register statute to include StingRays, other states appear to have written the statutes anew. But with the exception of these minor differences, the various statutes all provide the same basic requirement of a warrant based upon probable cause.

CONCLUSION

Regardless of which approach states take, they should pass legislation that clarifies law enforcements' burdens before collecting CSLI. Circuit courts' treatment of CSLI, as well as the United States Supreme Court's silence on the issue, creates a need for clarity at the state level. This Note aims to help states determine the proper legislative solution to law enforcement's use of cell site simulators such as StingRays.

Even if a circuit court has held that CSLI is available under the third-party doctrine without a court order or a warrant, state legislatures can still provide enhanced protections by requiring a court order or a warrant. Furthermore, if the United States Supreme Court considers CSLI, the Court will look to existing state laws to inform its analysis of the issues in question. States' adoption of clear and simple rules will promote long-term stability in Fourth Amendment jurisprudence. Whether states require a court order or a warrant, a legislative solution would help resolve the current confusion among states and in circuit courts.

---

362. VA. CODE. ANN. § 19.2-70.3(J).

363. WASH. REV. CODE § 9.73.080 (West 2015).

364. SB 741, 2015 Leg., Reg. Sess. (Ca. 2015), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201520160SB741 [https://perma.cc/4E8S-BLV6].

365. UTAH CODE ANN. § 77-23c-102(3) (West 2016).