Catholic University Law Review

Volume 67
Issue 2 *Spring 2018*

Article 10

5-15-2018

Is Your Smartphone Conversation Private? The StingRay Device's Impact on Privacy in States

Katherine M. Sullivan

Is Your Smartphone Conversation Private? The StingRay Device's Impact on Privacy in States

Cover Page Footnote

I am grateful for the insights and assistance from my mentor, Joe S. Cecil, Senior Research Associate, Federal Judicial Center, Washington, D.C. Your expertise in this area of law was invaluable.

IS YOUR SMARTPHONE CONVERSATION PRIVATE? THE STINGRAY DEVICE'S IMPACT ON PRIVACY IN STATES

Katherine M. Sullivan[+]

The Supreme Court has interpreted the Fourth Amendment to provide that, "subject only to a few, specifically established and well-delineated, exceptions," the search or seizure of a person or place must be supported by a warrant.[1] However, the Twenty-First Century, with its fast-pace, ever-changing technology, has introduced devices that place a strain on the application of this constitutional right. The StingRay device is one such example. The StingRay is a mobile surveillance system that mimics a cell tower so that cell phones and other mobile devices in the vicinity connect to it, thereby revealing the unique identifier and location of those devices.[2]

The StingRay devices are more commonly known as cell-site simulators,[3] but these devices were not originally invented for these purposes. Currently, the devices are used to locate suspects in the United States for alleged crimes, including fraud and drug trafficking.[4] The devices were originally designed for surveillance abroad by entities such as the Central Intelligence Agency (CIA).[5] Due to national security concerns and international challenges, the CIA sought

[+] I am grateful for the insights and assistance from my mentor, Joe S. Cecil, Senior Research Associate, Federal Judicial Center, Washington, D.C. Your expertise in this area of law was invaluable.

1. Katz v. United States, 389 U.S. 347, 357 (1967) ("Searches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few, specifically established and well-delineated, exceptions.").

2. *Stingray Tracking Devices: Who's Got Them?*, AM. CIV. LIBERTIES UNION, https://www.aclu.org/map/stingray-tracking-devices-whos-got-them (last updated Mar. 2018) [hereinafter *Stingray Tracking Devices: Who's Got Them?*]; *see also* Ellen Nakashima, *Justice Department: Agencies Need Warrants to Use Cellphone Trackers*, WASH. POST (Sept. 3, 2015), https://www.washingtonpost.com/world/national-security/justice-department-agencies-will-have-to-obtain-warrant-before-using-cellphone-surveillance-technology/2015/09/03/08e44b70-5255-11e5-933e-7d06c647a395_story.html.

3. *Street-Level Surveillance: Cell-Site Simulators/IMSI Catchers*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/sls/tech/cell-site-simulators/faq (last visited Apr. 18, 2018) [herein after *Street-Level Surveillance*].

4. *Id.*

5. Kim Zetter, *Hacker Lexicon: Stingrays, the Spy Tool the Government Tried, and Failed, to Hide*, WIRED (May 6, 2016, 6:41 PM), https://www.wired.com/2016/05/hacker-lexicon-stingrays-spy-tool-government-tried-failed-hide/ ("Although use of the spy technology goes back at least 20 years . . . their use of it has grown in the last decade as mobile phones and devices have become ubiquitous. Today, they're used by the military and CIA in conflict zones—to prevent adversaries from using a mobile phone to detonate roadside bombs, for example—as well as domestically by federal agencies . . . .").

this technology because it was almost impossible to rely on cooperation from local telephone providers in foreign countries.[6] Thus, these devices were created in the interest of national security and counter-terrorism.[7]

Private manufacturers—after discovering how invaluable and indispensable these devices were—sought to fill the demand.[8] The Harris Corporation, the major manufacturer of the StingRay devices, did exactly that.[9] After many devices were purchased by the federal government, the Harris Corporation sought to expand their market share into law enforcement agencies at both the state and local level.[10] The StingRay market has now expanded into state and local agencies; there are currently "72 agencies identified in 24 states and the District of Columbia that own StingRays."[11]

Judges and defense attorneys were in the dark about these new devices for some time.[12] When judges signed off on warrants, they often did so without knowing what the devices did and the implications from signing the warrant.[13] Often, judges failed to appreciate the degree of invasiveness of the StingRay devices. Other times, the warrant application would deliberately use the vague term of "technology" to encompass devices like the StingRay, leaving the judge unaware of all that would be included under the umbrella of that term.[14]

Historically, judges have been aware of pen registers being used, which only provide specific phone numbers of a cell phone;[15] however, StingRay devices

---

6. Stephanie K. Pell & Christopher Soghoian, *A Lot More than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 146 n.38 (2013).

7. *See Street-Level Surveillance*, *supra* note 3.

8. *See id.*

9. *See* Allison Grande, *Immigration Officials Pushed to Detail Cellphone Tracking*, LAW360 (May 19, 2017, 8:37 PM), https://www.law360.com/articles/926160/immigration-officials-pushed-to-detail-cellphone-tracking (noting that the Harris Corporation uses the "StingRay" label as the now, well-known branding name of the device).

10. Kris Hermes, *Law Enforcement Uses StingRays to Spy on Americans and Lies About It*, HUFFINGTON POST (Sept. 26, 2016, 2:11 PM), https://www.huffingtonpost.com/kris-hermes/law-enforcement-uses-stin_b_12080634.html.

11. *Stingray Tracking Devices: Who's Got Them?*, *supra* note 2.

12. Nathan Freed Wessler, *ACLU-Obtained Documents Reveal Breadth of Secretive Stingray Use in Florida*, AM. CIV. LIBERTIES UNION (Feb. 22, 2015, 5:30 PM), https://www.aclu.org/blog/free-future/aclu-obtained-documents-reveal-breadth-secretive-stingray-use-florida.

13. *Id.*

14. *See* Andrew Hemmer, Note, *Duty of Candor in the Digital Age: The New Heightened Judicial Supervision of Stingray Searches*, 91 CHI. -KENT L. REV. 295, 306–07 (2016) ("Congress enacted the USA PATRIOT Act, and one provision of the Act amended the definition of a 'pen register' to make it more encompassing. Due to this amendment to the Pen Register Statute, law enforcement agencies have been able to convince some magistrates to issue court orders under the statute for the use of Stingrays.").

15. Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) ("A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not

provide much more than a ten-digit phone number, they provide the content of the phone calls and the precise location of the device.[16] Furthermore, defense attorneys rarely know whether StingRay devices were used in obtaining evidence against their clients, which makes it more difficult to defend their clients.[17] Ultimately, an individual's Fourth Amendment right is at risk if state and local law enforcement lack clear guidance to determine when it is appropriate to use a StingRay without a warrant.

This Comment will investigate the impact of the StingRay device on an individual's Fourth Amendment right and how state and local law enforcement will know whether they require a warrant to use the device. Part I explains how the U.S. Supreme Court has adapted to the changes in technology regarding privacy rights, as well as how some states have dealt with this issue. Part II analyzes how smartphones in public and private areas should not factor into the analysis of whether a warrant is valid.

Part III proposes how state legislatures and judges can help protect the privacy rights of the citizens of their states. Part IV concludes that, with regard to smartphones, there is always a reasonable expectation of privacy, which requires a valid warrant before any government intrusion. This Comment advocates that the state legislatures that lack legislation specifically addressing the StingRay device should adopt one to protect its citizens' privacy rights. Moreover, if the state chooses not to adopt such a law, the judiciary must ensure that individual privacy rights remain protected.

I. THE FOURTH AMENDMENT AND ITS ADAPTATION TO ADVANCEMENTS IN TECHNOLOGY

A. The Intention of the Founding Fathers in the Creation of the Fourth Amendment

The Fourth Amendment establishes:

> 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.[18]

---

indicate whether calls are actually completed." (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977))).

16. *See Street-Level Surveillance*, *supra* note 3.

17. *Id.*

18. U.S. CONST. amend. IV. The Fourth Amendment has two clauses, the "reasonableness clause" and the "warrant clause." The former establishes the right to be free from unreasonable searches and seizures of persons, houses, papers and effects. The latter clause sets out the requirements of any valid warrant. There is also a judicial read-in of the Exclusionary Rule. *See*

American citizens have been entitled to this protection since the Fourth Amendment was ratified by the states in 1791.[19] The protection against unreasonable searches and seizures grew from the disdain of the English government's practice of issuing writs of assistance and other general warrants in the colonies.[20] To remedy this perceived injustice, the Founding Fathers carefully sculpted the Fourth Amendment, reasoning that a man's house is his castle and any general authority to search and seize him, his goods, or his papers should not invade the sanctity of his home.[21]

B. When Is a Warrant Required?

Once the Fourth Amendment applies, it is necessary to determine which circumstances require a warrant. A warrant is "a written order issued by a judicial officer or other authorized person commanding a law enforcement officer to perform some act incident to the administration of justice."[22] It is required to search or seize "persons, houses, papers, and effects" of private individuals.[23] The warrant must be sufficiently specific and turns on whether the individual has a reasonable expectation of privacy in the person, place, or thing to be searched or seized.[24]

Through a well-developed body of law, courts have recognized a distinction between a search and a seizure. Specifically, a seizure is a "meaningful interference with an individual's possessory interest,"[25] and a search "occurs when an expectation of privacy that society is prepared to consider reasonable is infringed."[26] Without a valid warrant, searches and seizures performed by government actors are deemed presumptively invalid. Consequently, any

---

Mapp v. Ohio, 367 U.S. 643, 651 (1961) (holding that all evidence obtained by searches and seizures in violation of the Constitution is, by that same authority, inadmissible in state court and federal court).

19. The States ratified the Fourth Amendment on December 15, 1791. U.S. CONST. amend. IV. Furthermore, the Court has interpreted the Fourth Amendment as inapplicable to nonresident aliens briefly in the United States searched by United States agents. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990) ("[I]t suggests that 'the people' protected by the Fourth Amendment . . . refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community.").

20. Boyd v. United States, 116 U.S. 616, 625–26 (1886).

21. *Id.* at 630 ("It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence.").

22. *Warrant*, LEGAL DICTIONARY, http://legal-dictionary.thefreedictionary.com/warrant (last visited Mar. 5, 2017).

23. U.S. CONST. amend. IV.

24. *See* Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring) (incorporating the infamous reasonable expectation of privacy test into the Fourth Amendment).

25. Unites States v. Jacobsen, 466 U.S. 109, 113 (1984).

26. *Id.*

evidence seized without a warrant will be inadmissible at trial unless a court finds that the search was reasonable under the circumstances.[27]

1. Valid Search Warrant

Search warrants may only be issued upon a showing of probable cause.[28] To establish probable cause the search warrant must: be supported by oath or affirmation by an officer;[29] issued by a neutral and detached magistrate;[30] and "contain a particularized description of the place to be searched and persons or things to be seized."[31] The Supreme Court in *Carroll v. United States* stated that probable cause exists when "the facts and circumstances within [the police officer's] knowledge . . . of which they had reasonably trustworthy information were sufficient in themselves to warrant a man of reasonable caution," to believe that a criminal offense has been committed or is about to take place.[32] In *Illinois v. Gates*, the Court held that determining whether probable cause exists requires a totality-of-the-circumstances analysis.[33] As such, the warrant must be sufficiently particular in describing what is to be searched and what is to be seized to permit a proper determination of probable cause.

2. A Warrant Is Not Always Required by Law

Courts have carved out certain exceptions to the warrant requirement,[34] one of which is the "exigent circumstances" exception.[35] Exigent circumstances

27. *Katz*, 389 U.S. at 357 ("[S]earches conducted outside the judicial process, without prior approval by a judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

28. Carroll v. United States, 267 U.S. 132, 155 (1925).

29. The Fourth Amendment provides that warrants must be founded on probable cause and supported by oath or affirmation. Franks v. Delaware, 438 U.S. 154, 155–56 (1978).

30. The magistrate cannot be involved directly with the investigation. *See* Lo-Ji Sales, Inc. v. New York, 442 U.S. 319, 327 (1979) (finding a judge to be the leader of the search party, thus violating this requirement, when he assisted the officers in finding the effects of the warrant, and in some circumstances, deferring to the officers' discretion).

31. United States v. Hazelwood, 412 F. App'x 617, 618 (4th Cir. 2011).

32. *Carroll*, 267 U.S. at 162.

33. Illinois v. Gates, 462 U.S. 213, 230 (1983).

34. These circumstances include the community caretaking exception, the automobile exception, and a search incident to arrest. *See* Fern Lynn Kletter, Annotation, *Necessity of Rendering Medical Assistance as Circumstance Permitting Warrantless Entry or Search of Building or Premises*, 58 A.L.R. 6th 499 Art. 1 § 2 (2008) (noting that the Supreme Court recognized a community caretaking exception to the warrant clause); *accord* United States v. Knotts, 460 U.S. 276, 281 (1983) (recognizing an automobile exception to the warrant clause); Chimel v. California, 395 U.S. 752, 762 (1969) (recognizing the search incident to arrest exception to the warrant clause).

35. *See* Kentucky v. King, 563 U.S. 452, 460 (2011) ("One well-recognized exception applies when 'the exigencies of the situation' make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment." (quoting Mincey v. Arizona, 437 U.S. 385, 394 (1978))).

exist when obtaining a warrant would be impractical under the circumstances. If an officer can show that an "exigent circumstance" exists, the officer may enter a home without violating the individual's constitutional right to be safe from an unreasonable search and seizure.[36]

Application of this principle to the StingRay device is complicated by the fact that the officer never physically enters the home, yet is able to remotely secure information from within the home—such as whether certain individuals are located in the home. Thus, such an invasion by law enforcement generally requires a warrant. However, exigent circumstances may exist if, for example, law enforcement sought to secure an individual's location but securing a warrant would permit the suspect to evade capture.[37] In other words, obtaining the warrant would be impractical under the circumstances.

C. Supreme Court Rulings: Technology and the Fourth Amendment

Proper enquiry into whether an individual's Fourth Amendment right to "be secure in their persons, houses, papers, and effects" was violated must first establish that law enforcement in fact conducted a search.[38] If there is no search, then there is no need to apply the Fourth Amendment. To determine if law enforcement conducted a search, courts ask two questions: (1) whether that person had an actual expectation of privacy, and (2) whether the expectation is one which society recognizes as reasonable.[39]

In *Kyllo v. United States*, an officer suspected that the defendant was growing marijuana in his house.[40] To determine whether the suspicion was correct, the police—located in a public roadway—aimed a thermal-imaging device at the defendant's home.[41] Based on the information provided by the device, the police obtained a search warrant for the home and subsequently found marijuana.[42] The lower court looked at the defendant's subjective and objective expectation

---

36. The Supreme Court has outlined many exigent circumstances including: officers chasing a fleeing suspect in hot pursuit and entering premises in order to prevent the imminent destruction of evidence. *King*, 563 U.S. at 460.

37. United States v. Ellis, No. 13-CR-00818 PJH, 2017 U.S. Dist. LEXIS 136217, at *41 (N.D. Cal. Aug. 24, 2017) (holding that a warrant was not required when using a Stingray to determine a suspect's location when the risk of flight and possession of firearms by the individual constituted an exigent circumstance); *see also* United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016) ("A person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location.").

38. U.S. CONST. amend. IV. Although the Fourth Amendment Right extends to unreasonable searches or seizures by law enforcement, this Comment focuses exclusively on unreasonable searches.

39. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

40. Kyllo v. United States, 533 U.S. 27, 29 (2001).

41. *Id.* at 29.

42. *Id.* at 30.

of privacy.[43] It determined that because the defendant made no effort to hide the heat being emitted from his house, and because the thermal-imaging device did not disclose any personal information about the defendant, the use of the thermal-imaging device by police did not require a warrant.[44] In other words, law enforcement's use of the device did not constitute a Fourth Amendment search.

On appeal, the Supreme Court held that the information obtained by the thermal-imaging machine—the heat signature given off by equipment to grow the marijuana plants—was a search under the Fourth Amendment.[45] The Court reasoned that, without the use of the device, police would only have access to that information by physically intruding into a protected area of the defendant's home; therefore, the use of the device constituted a constitutionally protected search. The Court further reasoned that because the thermal-imaging device was not in "general public use," the search was "presumptively unreasonable without a warrant."[46]

1. Electronic Listening Devices

In *Katz v. United States*, the government sought to introduce evidence obtained by an electronic listening device attached to the exterior of a public telephone booth while the defendant used it.[47] The defendant regularly used the public telephone booth to make calls regarding illicit activity, and the Federal Bureau of Investigations (FBI) had knowledge of this regular occurrence.[48] The Supreme Court, in overruling the Ninth Circuit Court of Appeals, held that once the defendant was in the telephone booth and shut the door, he was guaranteed that the words he spoke in those conversations would remain private.[49] The Court found that the FBI agents ignored the defendant's right under the Fourth Amendment when they obtained the telephone booth conversations without a search warrant.[50]

As technology advanced, the Supreme Court looked at the government's usage of beepers and electronic tracking devices in criminal investigations. In *United States v. Knotts*, the Supreme Court held that there was no Fourth Amendment violation when, without a warrant, law enforcement agents

43. *Id.* at 31.

44. *Id.* at 30–31.

45. *Id.* at 34–35.

46. *Id.* at 40.

47. Katz v. United States, 389 U.S. 347, 348 (1967).

48. *Id.* at 354.

49. *Id.* at 352; *see also* Silverman v. United States, 365 U.S. 505, 511 (1961) (holding that eavesdropping accomplished by mans of an electronic device that penetrated the premises occupied by petitioner was a violation of the Fourth Amendment).

50. *Katz*, 389 U.S. at 350 ("That Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections goes further, and often have nothing to do with privacy at all.").

monitored a beeper that was located in a container of chloroform loaded in a car, as it traveled through public streets and highways.[51] The Court reasoned that the defendant did not have a reasonable expectation of privacy in his car's movements on public roads, and as a result, the monitoring of the beeper by the police did not constitute an unconstitutional search.[52] In other words, the *Knotts* Court found no reasonable expectation of privacy in the monitoring of tracking devices in public areas.[53]

However, the Supreme Court in *United States v. Karo* carved out an exception to its holding in *Knotts*.[54] With a court order, law enforcement agents placed a beeper in a container of ether, which was transported by public roads and ultimately stored in a private home.[55] Due to the storage of the container in the private area, the Court held that the monitoring of the device within a private home violated the Fourth Amendment.[56] Therefore, to determine whether the monitoring of a person violated the Fourth Amendment, the Supreme Court would consider the nature of the place in which the individual was being monitored; that is, whether the area is public or private.[57]

2. Physical Placement of a Tracking Device on Personal Property

In the 2012 case *United States v. Jones*, the Supreme Court considered whether the placement of a tracking device on an automobile triggered Fourth Amendment protections.[58] The defendant in *Jones* was suspected of trafficking drugs. As a result, law enforcement agents sought to monitor Jones's activity, and after obtaining a warrant, installed a tracking device on the bottom of his wife's car while it was parked in a public parking lot.[59]

The warrant only authorized installation of the tracking device in the District of Columbia and was set to expire after ten days.[60] In contradiction of the

51. United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

52. *Id.* at 285.

53. *Id.* at 282. Courts have asked the question of whether the electronic tracking devices provide information that the police could otherwise not have obtained by visual surveillance. If answered in the negative, it is not a search under the Fourth Amendment. *Compare id.* at 285 (finding no search when monitoring a beeper placed on a car on public roads), *with* United States v. Karo, 468 U.S. 705, 714 (1984) (finding that a search occurred when the police monitored a beeper which entered into a home).

54. *Karo*, 468 U.S. at 714.

55. *Id.* at 708.

56. *Id.* at 714. ("[T]he monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.").

57. *Id.* at 714–15.

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

59. *Id.* at 402–03. The warrant was issued by the U.S. District Court for the District of Columbia after the agents lawfully surveilled the suspect.

60. *Id.*

warrant, the agents placed the tracking device on the car on the eleventh day and in Maryland.[61] The Court determined that installing the device constituted a Fourth Amendment search.[62] Justice Scalia, speaking for the majority, held that physical occupation of private property by means of the tracking device violated the Fourth Amendment.[63] He reasoned that because the defendant possessed the vehicle at the time the government attached the device to the car, it violated the defendant's Fourth Amendment rights.[64]

In his concurrence, Justice Alito recognized the changing aspects of technology and focused more on the scope and duration of the government's use of the device.[65] Justice Alito believed the proper inquiry to the issue was "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove," notwithstanding the public character of the car's movements.[66]

3. Possession of a Defendant's Cell Phone

The Supreme Court's 2014 decision in *Riley v. California*[67] addressed the issue of "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[68] The defendant in *Riley* was a gang member who was arrested for possession of concealed and loaded firearms following a traffic stop. Incident to his arrest, law enforcement subsequently seized and searched his mobile phone.[69]

The specific facts of the case are as follows. Riley was driving on expired registration tags and a suspended driver's license when he was pulled over by the police. Pursuant to department policy, the police were allowed to impound the car and conduct an inventory search.[70] During this search, police found photographs of the defendant standing in front of a car suspected to have been

61. *Id.* at 403.

62. *Id.* at 404.

63. Justice Scalia reasoned that because the government "physically occupied private property for the purpose of obtaining information," it would have been considered a "physical intrusion" and search "within the meaning of the Fourth Amendment when it was adopted." *Id.* at 404–05.

64. *Id.* at 404. The ruling in *Jones* caused a "sea change" inside the U.S. Department of Justice. Speaking after the decision, FBI General Counsel Andrew Weissmann noted that it prompted the FBI to turn off about 3,000 GPS tracking devices that were in use. *See* Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, WALL ST. J. (Feb. 25, 2012, 3:36 PM), https://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling.

65. *Jones*, 565 U.S. at 419.

66. *Id.*

67. 134 S. Ct. 2473, 2480 (2014).

68. *Id.* at 2480.

69. The phone, a smartphone, was seized from the defendant's pants pocket and was searched by the police because "gang members will often video themselves with guns or take pictures of themselves with the guns." *Id.* at 2480–81.

70. *Id.* at 2480.

involved in a shooting weeks earlier.[71] Ultimately, the defendant was charged with attempted murder, firing at an occupied vehicle, and assault with a semiautomatic weapon in connection with that shooting. At trial, Riley unsuccessfully sought to suppress the evidence acquired during this search.[72]

The Supreme Court found that the evidence from his cell phone used at trial was discovered through an unreasonable search under the Fourth Amendment.[73] The Court considered whether the government had a legitimate interest in assessing the material on the phone without a warrant.[74] The Court found that the search was unnecessary for the protection of the officers and held that the search incident to arrest exception to the warrant requirement did not apply.[75] The Court reasoned that since "[d]igital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer," the search incident to arrest exception did not apply.[76] Furthermore, the Court found the governmental interests were minimal compared to the degree of intrusion against the defendant, and therefore, triggering the warrant requirement to access the contents of the phone.[77]

Although Riley was in custody and, as such, had reduced privacy interests, they did not disappear entirely.[78] The Court specifically rejected the government's argument that the "officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart."[79]

---

71. *Id.* at 2481.

72. *Id.*

73. *Id.* at 2495.

74. *Id.* at 2484.

75. *Id.* at 2485. Generally, the search incident to arrest exception allows the officer to search an arrestee's person and the immediate area in order to find weapons that may be used against him or would allow the arrestee "to resist arrest or effect his escape." *Id.* at 2486 (quoting Chimel v. California, 395 U.S. 752, 763 (1969)).

76. Interestingly, the Court left open the possibility for law enforcement to search the "*physical aspects* of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case." *Id.* at 2485 (emphasis added). However, as discussed, this search involved data, not razor blades. The Court also addressed another warrant exception: the prevention of destruction of evidence. To this point, the Court ruled that under these circumstances, where the defendant's phone was already secured, "there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone." *Id.* at 2486. Moreover, the Court discussed the possibility of remote wiping, and noted that the officers could do two things to prevent this: (1) "turn the phone off or remove its battery"; or (2) "leave [the] phone powered on and place it in an enclosure that isolates the phone from radio waves." These enclosures are commonly called "Faraday bags." *Id.* at 2487.

77. *Id.* at 2495.

78. *Id.* at 2488.

79. *Id.* at 2493. To illustrate the Chief Justice's point, "the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery." *Id.* Similarly, "the fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years." *Id.* The Court here was clearly worried about the degree of intrusion and quantity of data acquired

Because the amount of digital data that can be stored on a phone is far greater than what one single person can put in their pockets, the Court concluded:

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life." The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our 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.[80]

D. The Department of Justice Policy Regarding StingRay Devices

1. Federal Government Addressing the Issue

On September 3, 2015, about a year after the *Riley* decision, the Department of Justice (DOJ) instituted a new policy requiring the FBI and other federal agencies to obtain a search warrant before using the StingRay device.[81] In the application for a warrant, the new policy requires DOJ officials to specifically disclose to judges that a cell-site simulator will be used and "describe in general terms the technique to be employed."[82] The DOJ's policy allows for exempted circumstances that would permit law enforcement agents to use the device without first obtaining a search warrant.[83] It is important to note that this policy applies in all instances involving the DOJ's use of StingRay devices "in support of other Federal agencies and/or State and Local law enforcement agencies."[84]

2. Where Do States Stand on the Issue?

Even though the DOJ policy applies when the federal government uses the device to assist state and local law enforcement, it fails to extend to scenarios

---

in these searches when compared to singular, individual documents discoverable in the pre-digital world.

80. *Id.* at 2494–95 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

81. Press Release, No. 15-1084, U.S. Dep't of Justice, Office of Pub. Affairs, 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 [hereinafter DOJ Press Release].

82. *Id.*

83. Exigent circumstances would be included in the exception to the warrant requirement. The exigent circumstances described are those very same exceptions in the non-digital world: "These include the need to protect human life or a very serious injury; the prevention of the imminent destruction of evidence; the hot pursuit of a fleeing felon; or the prevention of escape by a suspect or convicted fugitive from justice." *Id.* Other circumstances excluded from the warrant requirement involve situations in which obtaining a search warrant is "impracticable." However, the Department expects these circumstances "to be very limited" and requires executive level approval of a warrantless search. *Id.*

84. *Id.*

where state and local governments act on their own. Former Representative Jason Chaffetz, a Republican from Utah, introduced the Cell-Site Simulator Act of 2015, also known as the Stingray Privacy Act to the House of Representatives in November of 2015 to address that concern.[85] The new bill would require state and local law enforcement agencies to obtain a warrant before they could use cell-cite simulator devices in pursuit of charges under Title 18 of the United States Code.[86] However, the bill as introduced by Representative Chaffetz never made it out of committee; this left state and local authorities in the same position: warrant limbo.

The following chart illustrates the use of cell-site simulators at the state and local law enforcement level.[87]

States that currently have local police using cell-site simulators	Washington Nevada Arizona New Mexico Missouri Georgia Massachusetts Alaska
States that currently have state police using cell-site simulators	Oklahoma Louisiana Delaware Pennsylvania
States that currently have both local and state police using cell-site simulators	California Texas Virginia North Carolina Maryland New York Florida Michigan Indiana Illinois Wisconsin Minnesota Tennessee

85. Stingray Privacy Act of 2015, H.R. 3871, 114th Cong. (2015).
86. *Id.* § 2(a).
87. *Stingray Tracking Devices: Who's Got Them?*, *supra* note 2.

Although the extent of the use of cell-site simulators in the states not listed above is unknown, the American Civil Liberties Union has identified seventy-two law enforcement agencies in twenty-four states and the District of Columbia that own StingRay devices.[88] Notably, however, some of these state legislatures have enacted laws to protect their residents against unreasonable use of these. The following table is illustrative:[89]

California	Enacted in 2015	Requires warrant for both historical and real-time location data
Colorado	Enacted in 2014	Requires warrant for location data obtained from devices but not from service providers
Illinois	Enacted in 2014	Protects only real-time location data
Indiana	Enacted in 2014	Protects only real-time location data, but also requires warrant for drone use and for electronic device searches
Iowa	Enacted in 2014	Applies only to Global Positioning System (GPS) tracking devices
Maine	Enacted in 2013	Requires warrant for both historical and real-time location data
Maryland	Enacted in 2014	Applies only real-time location data
Minnesota	Enacted in 2014	Requires warrant for both historical and real-time location data
Montana	Enacted in 2013	Requires warrant for both historical and real-time location data
New Hampshire	Enacted in 2015	Requires warrant for both historical and real-time location data

88. *Id.*

89. Peter Cihon, *Status of Location Privacy Legislation in the States: 2015*, AM. CIV. LIBERTIES UNION (Aug. 26, 2015, 1:15 PM), https://www.aclu.org/blog/free-future/status-location-privacy-legislation-states-2015.

Tennessee	Enacted in 2014	Amended to undermine all protections
Utah	Enacted in 2014	Requires warrant for both historical and real-time location data, as well as electronic communications content
Virginia	Enacted in 2015	Requires warrant for use of StingRay devices
Washington	Enacted in 2015	Requires warrant for use of StingRay devices
Wisconsin	Enacted in 2014	Permits location tracking under a less protective legal standard

As demonstrated in the above table, these fifteen states have enacted a law addressing warrants and the use of cell-site stimulators. The protections vary from either requiring a warrant for historical information, real-time location, or a hybrid of both.

Even though some states have not passed legislation on the matter, they have been subjected to limitations by their own judiciary. For example, in *Tracey v. State*, the Florida Supreme Court required a warrant for real-time location information that would be obtained through use of the StingRay device.[90] In attempting to develop a workable framework, the Florida Supreme Court rejected the application of the mosaic theory to the Fourth Amendment search analysis.

The mosaic theory stands for the proposition that "discrete acts of surveillance by law enforcement may be lawful in isolation, but may otherwise infringe on reasonable expectations of privacy in the aggregate because they 'paint an intimate picture of a defendant's life.'"[91] However, the court noted that applying the theory was "problematic where traditional surveillance becomes a search only after some specified period of time."[92] It concluded "that basing the

90. Tracey v. State, 152 So. 3d 504, 526 (Fla. 2014) ("Therefore, we hold that regardless of Tracey's location on public roads, the use of his cell site location information emanating from his cell phone in order to track him in real time was a search within the purview of the Fourth Amendment for which probable cause was required.").

91. *Id.* at 520 (quoting United States v. Wilford, 961 F. Supp. 2d 740, 771 (D. Md. 2013)).

92. *Id.*

determination as to whether warrantless real time cell-site location tracking violates the Fourth Amendment on the length of time the cell phone is monitored is not a workable analysis."[93] Thus, every decision would need to be made on a case-by-case basis.[94]

Ultimately, the Florida Supreme Court concluded that the defendant had a subjective expectation of privacy that society was now prepared to recognize as reasonable, thereby requiring a warrant. This rang true even when the defendant was on a public road and did not voluntarily convey his whereabouts to the service provider "for any purpose other than to enable use of his cell phone for its intended purpose."[95]

In *State v. Earls*, the Supreme Court of New Jersey confronted the issue of whether the warrant requirement applied when police obtain a defendant's cell phone location information from a cell phone service provider.[96] Phrased another way, the New Jersey Supreme Court "consider[ed] whether people have a constitutional right of privacy in cell-phone location information."[97] The facts of *Earls* stemmed from the investigation of a series of residential burglaries in the Middletown Township. The police obtained a court order to trace a cell phone stolen in one of the burglaries. The trace led police to a man in possession of the stolen phone who reported purchasing the phone from his cousin—defendant Thomas Earls.[98]

After obtaining assistance from Earls' former girlfriend, police located the stolen material in a storage unit belonging to the former girlfriend. The next day, the girlfriend's relative contacted police to report that Earls learned of her cooperation with police and threatened to harm her in retaliation. Immediately, police obtained an arrest warrant for Earls and initiated an aggressive attempt to locate Earls and his potential hostage.[99] To locate them, police contacted his mobile service provider without seeking a court order or warrant to obtain his cell phone location information.[100] After three separate cell phone location tracings and with the assistance of a neighboring police department, police located and arrested Earls.[101]

---

93. *Id.*

94. *Id.* ("It requires case-by-case, after-the-fact, ad hoc determinations whether the length of the monitoring crossed the threshold of the Fourth Amendment in each case challenged.").

95. *Id.* at 525.

96. State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

97. *Id.*

98. Earls' cousin further alleged that Earls "had been involved in residential burglaries and kept the proceeds in a storage unit that either defendant or his former girlfriend, Desiree Gates, had rented." *Id.* at 633. After police contacted Gates, she agreed to assist police in the investigation and led police to the location of the storage unit where they found the stolen material. *Id.*

99. *Id.*

100. *Id.* at 633–34.

101. *Id.* at 634.

Based on state constitutional grounds, the New Jersey Supreme Court found that an individual's privacy interests extended to the location of his or her cell phone.[102] The court held that the police must "obtain a warrant based on a showing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information through the use of a cell phone."[103] Today, New Jersey lacks legislation mandating that law enforcement obtain a warrant to access cell phone location information, but the basis for this protection rests on their state constitutional jurisprudence.[104]

For the states that lack either legislative or judicial safeguards against government use of cell phone location data, the question remains: How will individuals' Fourth Amendment rights remain protected?

II. CONSIDER THE SMARTPHONE AN EXTENSION OF YOUR HOME

Before the first smartphone came out, an individual carried the basic cell phone that was used solely to connect through voice and text communication. Now it is impossible to walk down the street without someone bumping into you as they scroll the Internet in the palm of their hand. Smartphones expand to each corner of an individual's life: one can now pay for things; store airplane boarding passes; lock one's home; and navigate their way across any distance in real time with extreme precision. Indeed, many consider the smartphone an extension of an individual's home—just like wallets, car keys, and wedding rings, one never leaves home without it. The inherent danger in that, however, is that such technological advances are equally as accessible to state and local law enforcement.

A. How Smartphones Function Versus Old Technology

There is a big difference between a cell phone and a smartphone, the former is only used to communicate by text and call, while the latter, in addition to these

102. *Id.* at 632.

103. *Id.* at 644. Interestingly, even though the New Jersey Supreme Court held that a warrant was required, it remanded the case to the Appellate Division "to determine whether the emergency aid doctrine applies to the facts of this case under the newly restated test." *Id.* at 646.

104. *Id.* at 632.

functions can access the internet, which includes location or GPS services.[105] Currently, there are more gadgets than people in the world.[106]

1. StingRays Versus Pen Registers

In its 2015 policy, the DOJ required that cell-site simulators must be configured in a "manner that is consistent with" the Pen Register Statute.[107] Pen Registers are similar to StingRays in that some information from a cell phone can be obtained. The major difference lies, however, in the vast quantity and more intrusive degree of information that can be obtained using the StingRay.

Pen Registers are defined under the Electronic Communications Privacy Act of 1986, as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication."[108] Simply stated, Pen Registers only document the phone numbers called and received on a particular phone. On the other hand, the more intrusive StingRay device is much more advanced.[109] The devices have been described as "portable spy device[s] able to track cell phone signals inside vehicles, homes and insulated buildings."[110]

One major difference the smartphone introduces into this analysis is the amount of time and resources expended by law enforcement when attempting to locate a suspect. In cases like *Knotts*, the government needed to *physically place a beeper* on the individual's person while it was limited in range.[111] With the

105. *See* Jason Gordon, *How Does GPS Work on Cell Phones?*, USA TODAY, http://travel tips.usatoday.com/gps-work-cell-phones-21574.html (last updated Sept. 12, 2017) ("Cell phones with GPS receivers communicate with units from among the 30 global positioning satellites in the GPS system. The built-in receiver trilaterates your position using data from at least three GPS satellites and the receiver. GPS can determine your location by performing a calculation based on the intersection point of overlapping spheres determined by the satellites and your phone's GPS receiver. In simple terms, trilateration uses the distance between the satellites and the receiver to create overlapping 'spheres' that intersect in a circle. The intersection is your location on the ground.").

106. Zachary Davies Boren, *There Are Officially More Mobile Devices than People in the World*, INDEPENDENT (Oct. 7, 2014, 3:30 PM), http://www.independent.co.uk/life-style/gadgets-and-tech/news/there-are-officially-more-mobile-devices-than-people-in-the-world-9780518.html.

107. DOJ Press Release, *supra* note 81 (citing 18 U.S.C. § 3125 (2012)).

108. 18 U.S.C. § 3127(3). Interestingly, the Supreme Court in *Smith v. Maryland* relied on a different definition than is found in the statute, as this case predated the enactment of this statute. *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (defining a pen register as "a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released").

109. *See generally* Clarence Walker, *New Hi-Tech Police Surveillance: The "Stingray" Cell Phone Spying Device*, GLOBAL RES. (May 19, 2015), http://www.globalresearch.ca/new-hi-tech-police-surveillance-the-stingray-cell-phone-spying-device/5331165.

110. *Id.*

111. United States v. Knotts, 460 U.S. 276, 277 (1983).

smartphone, the government can track the device's location remotely and in real time, as long as it is turned on and registering with a cell tower.[112]

The type of information StingRays collect is called metadata. Metadata is the "data about the communication that allows the communication to successfully reach its intended recipient."[113] It includes: the location that the message originated from; the device that sent or made the communication; the times at which the message was made and sent; and the length or duration of the message.[114] Without having proper protections on metadata, individuals can be tracked and followed continuously and without warning. Metadata reveals a lot about the individual and, when in the wrong hands, can identify and outline many personal details about the individual.

There is also a difference between private and governmental uses of metadata. Companies want metadata because they can capitalize on a target audience for marketing purposes—as they could learn the likes and dislikes of the individual consumer. But when the government collects metadata, it could build a profile of any individual for a myriad of reasons. Individuals often willingly allow companies like Facebook to collect metadata, which is how many tech companies survive. However, when it comes to the government's use of metadata, individuals are being tracked unwittingly.

2. Public Versus Private Areas

Another issue to consider is whether the cell phone's location matters. For example, as a person travels home, would she reasonably expect that the government could track her because she was using her mobile phone to get there? Law abiding citizen or not, one should not feel threatened by the government's unreasonable conduct.

Applying the Supreme Court precedent in *Kyllo* to the StingRay device, it is clear that the use of the device without a warrant to monitor the movements of an individual inside her own home would constitute an unconstitutional search because "the Fourth Amendment draws 'a firm line at the entrance to the house.'"[115] Using the precedent established in *Katz*, just as the Fourth Amendment protected the privacy of the defendant's conversation in a public telephone booth, it should also protect an individual's cell phone conversation

---

112. *See* Gordon, *supra* note 105 ("Even the cell phones that don't have GPS can use cell tower position and distance to calculate your location. Cell phones function by communicating with towers connected to a base station in a configuration called a 'cell.' As you move through the cell, the base station monitors your cell phone's signal and transfers it to the nearest tower.").

113. *Metadata*, PRIVACY INT'L, https://www.privacyinternational.org/node/53 (last visited Nov. 28, 2016).

114. *Id.*

115. Kyllo v. United States, 533 U.S. 27, 40 (2001).

in her car or other visible public locations from being "broadcast[ed] to the world."[116]

Unlike the situation in *Knotts*, but like the circumstances in *Karo*, an individual almost certainly would have a reasonable expectation of privacy in his phone's movement on public roads. The mobile phone is an extension of the "firm line" of the home and may be properly characterized as part of the private residence, the Supreme Court should come to a conclusion that a warrantless monitoring of a cell phone, which "reveal[ed] no information that could not have been obtained through visual surveillance," was an unreasonable search in violation of the Fourth Amendment.[117]

Using Justice Scalia's rationale in *Jones*, the government would "physically occup[y] private property for the purpose of obtaining information," as soon as it begins using the StingRay device and, therefore, would violate the Fourth Amendment.[118] The Supreme Court, through these decisions, requires that law enforcement agencies act reasonably and with care when it comes to an individual's privacy rights.[119] The best way to handle this issue is to follow the example of the DOJ guidelines and those states with legislation requiring law enforcement officials to obtain a warrant before using cell-site simulators.

B. The Individual's Reasonable Expectation of Privacy

Importantly, in today's technological age, information "disclos[ed] to a third-party [service] provider, as an essential step to obtaining service altogether, does not upend the privacy interest at stake."[120] It is almost impossible in our society to *not* have a smartphone—individuals receive news updates, banking information, texts, phone calls, and read books, all from one device, on the go, instantaneously. Individuals do not waive their right to privacy by purchasing the device that allows a carrier to obtain one's location automatically. A bank does not broadcast to the world an account holder's routing number just because it has the information readily available. That information is sacred, and cell phone data is no different.

Society shapes the behaviors individuals think and believe to be acceptable based on social norms. Society, as it stands today, would not reasonably expect

---

116. Katz v. United States, 389 U.S. 347, 352 (1967) ("No less than an individual in a business office, in a friend's apartment, or in a taxicab, a person in a telephone booth may rely upon the protection of the Fourth Amendment.").

117. United States v. Karo, 468 U.S. 705, 714 (1984) ("The monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence.").

118. United States v. Jones, 565 U.S. 404 (2012).

119. Even in some cases where the police act reasonably but without a warrant, nevertheless a court will find the Fourth Amendment to be violated. *See* State v. Earls, 70 A.3d 630, 633 (N.J. 2013) (finding that the defendant's Fourth Amendment right was violated even though he police thought he took a hostage).

120. State v. Reid, 945 A.2d 26, 33 (N.J. 2008) (holding limited to New Jersey law).

that *any* information turned over to a service carrier dissolves her privacy expectations.[121] In addition, it would be unreasonable to think that this information should be used against her in a criminal trial without constitutional authority to actually obtain that information.[122]

III. STATE LEGISLATURE'S ROLE

As explained above, many states have adopted laws requiring local and state law enforcement obtain a warrant before gathering data from smartphones. Many states encompass the requirement of obtaining warrants for historical locations, real-time location, phone records, content of electronic communications, cell phone and internet service provider records, GPS tracking, and StingRay tracking. But no state has passed legislation that encompasses all these components.

It is well known that the law has and will always struggle to match pace with technology.[123] But the problem herein arises when legislation fails to encompass all the protections it should, which forces law enforcement agencies to determine when a warrant is necessary. Of course, there will be cases where obtaining a warrant is impracticable, and in those instances, the warrantless search would not violate the Fourth Amendment. Nonetheless, effective legislation would address situations where law enforcement had time to get a warrant but failed to do so, impermissibly yielding the protected information from a StingRay search.

A. The Ideal State Law for Privacy Rights

The legislation this Comment proposes has yet to be enacted by any state, but seeks to assist states that are looking to address these concerns. The law this Comment recommends is one that requires a warrant for *all* information that can be obtained off a smartphone from a StingRay: historical location, real-time location, phone records, content of electronic communications, cell phone and internet service provider records. However, the law must recognize legitimate, practical concerns for law enforcement and should only apply if the government has a reasonable amount of time to obtain a warrant and no one's life is endanger. This Comment is not advocating that local and state law enforcement agencies should never be able to obtain this information, but to obtain the information, the agencies must do so with a valid warrant.

By adopting this proposed law, legislatures would be holding local and state law enforcement agencies accountable, while simultaneously protecting the individual rights of its citizens. In passing this law, the legislatures would save time and money for themselves, state and local police departments, and state

---

121. *See id.*

122. *See* Wong Sun v. United States, 371 U.S. 471, 484–85 (1963).

123. *See* United States v. Gomez, 807 F. Supp. 2d 1134, 1150 n.16 (S.D. Fla. 2011) (explaining Moore's law as "the computing power of today's cell phone, tablet PC, laptop, etc., is likely to be, at least, twice as powerful in two years").

courts. Perhaps the most important factor to consider is that through effective legislation, instances where police failure to secure a warrant leads to the release of potentially dangerous individuals would be diminished.

It is in the best interest of the public to keep dangerous criminals from walking the streets. If they break the law, and if they participate in illegal activities, they should be arrested and prosecuted by the government. But the government must do so in a manner consistent with the protection of the Constitution, by obtaining a warrant.

B. Role of the Judiciary

The judiciary is at the front lines of protecting individual's reasonable expectation of privacy.[124] It is the first to see the warrant, and by the stroke of a pen, judges enable or disable law enforcement to act on the warrant and conduct a search. Judges should ask pressing questions of law enforcement personnel who apply for warrants; they should ask about who the person of interest is, why the department believes there is probable cause, and whether there are other available means to figure out where the person of interest is without using the StingRay device.[125] These questions would help inform the judge to make the proper decision.

Giving judges the opportunity to receive proper training and education about what the StingRay devices are, what they really do, and how intrusive they can be to an individual are vital to the privacy interests at stake. With this training, judges will be able to fully realize the implications of each StingRay warrant. And with each new development in technology, judges will continue to be faced with the StingRay and other similar devices as time goes on. For judges to be fully knowledgeable in this area of the law will allow every state to better efficiently and effectively pursue justice.

IV. CONCLUSION

Overall, state legislatures that do not have a law addressing the StingRay device should adopt one, as it would strike a more equitable balance between individual privacy rights and the government's interests in enforcing its laws. Technology is a great tool, especially with regard to law enforcement's interest

---

124. Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 899 (2014) ("Because courts are best positioned to extract details about hidden investigative techniques when defendants are kept entirely in the dark, judges sitting in surveillance cases should press the government for those details sua sponte . . . .").

125. *See* Michele Adelman & Erik Schulwolf, *IPhone Access Gets Attention, "Stingrays" Fly Under the Radar*, LAW360 (Apr. 5, 2016, 10:50 PM), https://www.law360.com/articles/779899/iphone-access-gets-attention-stingrays-fly-under-the-radar ("While it is not clear to what extent there is—or will be—large-scale civilian use of Stingrays, the threat of such use underscores the need for the general public to be aware of the potential danger posed by Stingray-like devices, and for cellphone makers, cellular network providers, and governments to work to mitigate it.").

in public safety, and should not be viewed negatively. However, there needs to be a balance between using advanced technology to excel society and upholding the Framers' intention behind the Fourth Amendment.