Washington and Lee Journal of Civil Rights and Social Justice

Volume 24 | Issue 1 Article 7

9-1-2018

Out of the "Serbonian Bog"1 Surrounding Government Acquisition of Third-Party Cell Site Location Information: "Get a Warrant" †

Glenn Williams
Washington and Lee University School of Law

Out of the "Serbonian Bog"[1] Surrounding Government Acquisition of Third-Party Cell Site Location Information: "Get a Warrant" †

*Glenn Williams**

Table of Contents

1. United States v. Lambis, 197 F. Supp. 3d 606, 610 (S.D.N.Y. 2016).

† 2017 Louise A. Halper Award for Best Student Note, Washington and Lee University School of Law, Journal of Civil Rights and Social Justice Student Note.

* Candidate for Juris Doctor, Washington and Lee University School of Law, 2018; Bachelor of Arts, The College of William and Mary, 2013. I would like to thank the Journal of Civil Rights & Social Justice at Washington and Lee University School of Law, Professor Joshua Fairfield, Professor Timothy Keefer, Professor Timothy MacDonnell, and Professor Brian Murchison. I sincerely appreciate their time and encouragement.

Introduction

> 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 . . . .[2]

One evening, you are on your way home from work. You make your normal drive from your office to your house without any stops. A few days later, you receive a certified letter from the local police department informing you that you are a "person of interest" in a homicide investigation. The police request you to come to the station to be interviewed. The letter explains that law enforcement obtained your cell phone's site location information (CSLI)[3] from your cellular provider. Using your CSLI, as well as CSLI from other "persons of interest," your phone's data shows that you were in the vicinity of the homicide at the time it occurred.[4] The letter

---

2. Boyd v. United States, 116 U.S. 616, 630 (1886).

3. *See* Case Comment, United States v. Graham: *Fourth Circuit Holds That Acquisition of Historical Cell-Site Location Information Is Not a Search*, 130 HARV. L. REV. 1273, 1273 (2017) [hereinafter *Acquisition*] (explaining that CSLI is "a carrier's records of the cell tower used to route a user's calls and messages" usually to the closest tower (citing United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015))); s*ee also* Alexander Porter, *"Time Works Changes": Modernizing Fourth Amendment Law To Protect Cell Site Location Information*, 57 B.C. L. REV. 1781, 1798 (2016) ("Historical CSLI is data that the cellular service provider creates and keeps about the communication between an individual cell phone and the cellular network." (citing 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, 574–75 (2012))).

4. *See* Riley v. California, 134 S. Ct. 2473, 2490 (2014) (explaining that law enforcement can use CSLI to "reconstruct someone's specific movements down to

also claims that by signing up and using your cell phone provider's service, you *voluntarily* consented to your provider releasing your cell phone tracking information to law enforcement. The police have conducted warrantless surveillance with no reasonable cause.

The hypothetical above should frighten every smartphone user in the United States. It is estimated that in 2017, there are approximately 224,300,000 people using smartphones in the United States.[5] Given the current state of technology and the law, the hypothetical could become a reality. Advances in technology allow smartphone location data to be determined more precisely.[6] Smartphones hold increasingly personalized and revealing information about their owners.[7] Law enforcement also has access to increasingly sophisticated methods to acquire CSLI.[8] Meanwhile, the law has not kept up with technology or society's

---

the minute, not only around town but also within a particular building" with increasing accuracy (citing United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring))).

5. *See Number of smartphone users in the United States from 2010 to 2022 (in millions)*, STATISTA (2017), https://www.statista.com/statistics/201182/forecast-of-smartphone-users-in-the-us/ (displaying the number of smartphone users in the United States from data gathered between 2010 and 2016 and projecting that consumer smartphone use in the United States will continue to increase) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also Riley*, 134 S. Ct. at 2490 ("[M]any of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate." (citing City of Ontario v. Quon, 560 U. S. 746, 760 (2010))); *see also* Jacob Poushter, *Smartphone Ownership and Internet Usage Continues to Climb in Emerging Economies*, PEW RES. CTR. (Feb. 22, 2016), http://www.pewglobal.org/2016/02/22/smartphone-ownership-and-internet-usage-continues-to-in-emerging-economies/ (stating that 2015 research indicates 72% of people over eighteen years of age in the United States own a smartphone) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

6. *See* Craig Silliman, *Technology and Shifting Privacy Expectations (Perspective)*, BLOOMBERG (Oct. 7, 2016), https://bol.bna.com/technology-and-shifting-privacy-expectations-perspective/ ("[C]hanges—particularly, the surge in our customers' use of data and the fact that many of today's cell sites have smaller ranges—mean that our network now collects more voluminous and more precise location information . . . .") (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

7. See *id.* (explaining how the current technological capabilities of everyday technology such as a cell phone create Fourth Amendment concerns).

8. *See id.* (describing the process used by wireless networks to capture CSLI).

reasonable expectations of privacy.[9] The legal standards for the government to obtain cell phone tracking data are inconsistent and often unclear.[10] The ability of law enforcement agencies to obtain this type of personal information often without a warrant impacts all smartphone users and raises serious Fourth Amendment privacy concerns.[11]

In some jurisdictions, real-time tracking of a cell phone's location does require a warrant.[12] As of February of 2017, however, several federal circuit courts have held that law enforcement may routinely obtain CSLI without a probable cause warrant.[13] The

9. *See id.* (suggesting that U.S. Supreme Court precedent from the 1970s may not be applicable today "when [a customer] reveal[s] location information to [the] carrier simply because [the] device is connected to its network").

10. *See id.* (noting that while some jurisdictions require law enforcement to obtain historical location information through a probable cause warrant, which imposes a significant burden on the government, "[m]ost courts have held that a court order is sufficient").

11. *See id.* (describing how courts struggle when applying the third-party doctrine to advancing technology).

12. *See* Robinson Meyer, *This Very Common Cellphone Surveillance Still Doesn't Require a Warrant*, ATLANTIC (Apr. 14, 2016), https://www.theatlantic.com/technology/archive/2016/04/sixth-circuit-cellphone-tracking-csli-warrant/478197/ (discussing different warrant requirements between real-time CSLI and historic CSLI) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also* VA. CODE ANN. § 19.2-70.3 (2015) (enacted as a companion statute to the Stored Communications Act 18 U.S.C.A. § 2703(d) (1986) and requiring the government to obtain real-time CSLI).

13. *See* Porter, *supra* note 3, at 1782 (explaining that "[f]ive Federal Courts of Appeals covering more than 155 million Americans have approved the acquisition of historical CSLI by law enforcement" on less than probable cause, using instead a "specific and articulable facts standard"). However, many scholars argue that for cases involving historical CSLI, the government should be required to meet a higher standard that requires a probable cause warrant. *See* Brian L. Owsley, *The Fourth Amendment Implications of the Government's Use of Cell Tower Dumps in Its Electronic Surveillance*, 16 U. PA. J. CONST. L. 1, 37–38 (2013) (referencing court opinions that support the application of a probable cause standard due to the breadth and intrusiveness of electronic surveillance using cell-site-location records); *see also* Patrick T. Chamberlain, Note, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1751 (2009) (arguing that a probable cause standard should govern disclosure of historical CSLI, and not "some lesser standard," because it will likely be obtained more frequently by federal agents than real-time CSLI); *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 742–43 (2011) (stating that "acquisition [of historical CSLI] by law enforcement should proceed only after agents obtain a warrant based on probable cause" because "its acquisition implicates a reasonable expectation of privacy").

legal doctrine used to justify these warrantless searches is known as the "third-party doctrine."[14]

Like our hypothetical, the third-party doctrine justifies warrantless searches of a consumer's historical CSLI under the theory that the consumer has "voluntarily" given consent to his carrier to disclose cell phone tracking information to third parties.[15] The logic behind the doctrine is that since the consumer has consented in the agreement with the provider, the consumer lacks a reasonable expectation of privacy of the CSLI regardless how much or what type of information is revealed.[16] The doctrine was first established in the 1970's when particular technology involving the spread of consumer-based microprocessors and sensors was much less ubiquitous than it is in 2017.[17] As a result, consumers' expectations of privacy have likely changed dramatically.[18] Therefore, the third-party doctrine "does not accurately estimate what society today would consider reasonable."[19]

Courts have struggled to apply this dated and static doctrine in a world of ever-changing technology.[20] This struggle will only become more difficult as technology continues to evolve.[21] Several

---

14. *See* Monu Bedi, *The Curious Case of Cell Phone Location Data: Fourth Amendment Doctrine Mash-Up*, 110 NW. U. L. REV. 507, 511 (2016) (describing the Fourth Amendment roots of the third-party doctrine and the problems this doctrine creates as technology evolves).

15. *See* 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) (discussing how the element of voluntary disclosure in the third-party doctrine precludes a court from characterizing the government's acquisition of such disclosed information as a "search").

16. *See* Silliman, *supra* note 6 (stating that new technology may change society's reasonable expectation of privacy).

17. *See* David Oscar Markus & Nathan Freed Wessler, *That '70s Show: Why the 11th Circuit Was Wrong to Rely on Cases from the 1970s to Decide a Cell-Phone Tracking Case*, 70 U. MIAMI L. REV. 1179, 1181 (2016) (discussing how courts should not apply old privacy doctrines to modern technology).

18. *See id.* at 1205 ("Recent data shows that more than 80 percent of people consider '[d]etails of [their] physical location over time' to be 'sensitive'--evincing greater concern for this data . . . .").

19. *Acquisition*, *supra* note 3, at 1273.

20. *See* Silliman, *supra* note 6 (explaining that courts are struggling to apply static law to rapidly advancing technology in Fourth Amendment cases).

21. *See* Markus & Wessler, *supra* note 17, at 1193–94 (2016) (analyzing how courts rely on old pre-digital precedent to reach different conclusions).

recent United States Supreme Court cases suggest that the third-party doctrine should be modernized.[22] Questions remain about how the doctrine should be updated and whether the courts or the legislature should decide this issue.

This Note is divided into three parts. Part I describes the birth and evolution of the third-party doctrine including informants, controversial pen registers, and the current complexity of location-based tracking technology. Part II examines the current conflict between courts' application of the third-party doctrine and citizens' reasonable expectations of privacy. Finally, Part III considers possible solutions to the third-party doctrine quagmire. Ultimately, this Note proposes that the current third-party doctrine should be interpreted to require the government to obtain a probable cause warrant to collect real-time and historical CSLI.

I. The Evolution of the Third-Party Doctrine: From Informants to Modern Cell Phone Tracking

In 1942, United States Supreme Court Justice Murphy opined that "science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears . . . ."[23] A brief history of Fourth Amendment protections involving advancing technology is essential to understand the current state of the third-party doctrine.

---

22. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J. concurring) ("[The third-party doctrine] is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."); *see also* Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("Our answer to the question of what police must do before searching [information on] a cell phone seized incident to an arrest is accordingly simple—get a warrant."); *see also* United States v. Graham, 824 F.3d 421, 437 (4th Cir. 2016) ("A per se rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy.").

23. Goldman v. United States, 316 U.S. 129, 139 (1942) (Murphy, J., dissenting).

A. Fourth Amendment Protections

1. Wiretapping

The Fourth Amendment states:

> 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.[24]

Since 1877, the United States Supreme Court has recognized this protection and has applied it to privacy matters.[25] The notion of privacy has evolved considerably since 1877. As Michael Price explains, the Supreme Court "could afford to be technology-blind"[26] until 1928 when it heard the case of *Olmstead v. United States*.[27] In *Olmstead*, Chief Justice Taft explained that in attempting to gather evidence of a conspiracy, law enforcement inserted wires in telephone lines "without trespass[ing] upon any property of the defendants."[28] Collecting evidence through these wiretaps "continued for many months."[29]

Analyzing wiretapping in the light of Fourth Amendment privacy concerns, the Court explained that Fourth Amendment protections are only implicated by an "official search and seizure of his [a defendant's] person, or such a seizure of his papers or his

---

24. U.S. CONST. amend IV.

25. *See* Ex parte Jackson, 96 U.S. 727, 735 (1877) (explaining that the Fourth Amendment protects privacy rights by requiring a warrant to open letters and sealed postal packages); *see also* Katz v. United States, 389 U.S. 347, 356 (1967) (stating that the Constitution protects a citizen's reasonable expectation of privacy).

26. *See* Michael W. Price, *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine*, 8 J. NAT'L SECURITY L. & POL'Y 247, 259 (2016) (detailing the evolution of the Supreme Court's reasoning in Fourth Amendment privacy cases).

27. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that wiretapping "did not amount to a search or seizure within the meaning of the Fourth Amendment").

28. *See id.* at 457 (describing how federal prohibition officers seized information about the defendants' conspiracy "by intercepting messages on the telephones of the conspirators" without physically invading their property).

29. *Id.*

tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[30] Under the Court's Fourth Amendment analysis, the Court held that warrantless wiretapping was constitutional.[31]

Price explains that because the Court in *Olmstead* relied on property law, it did not focus on the role technology played in society.[32] Illustrating Price's criticism, Justice Taft stated that in the context of wiretapping, "intervening wires are not part of his house or office any more than they are the highways along which they are stretched."[33] Notably, Justice Brandeis offered a dissent stating:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[34]

Extending its reasoning from *Olmstead*, the Court held in the 1942 case of *United States v. Goldman*[35] that federal agents using a "detectaphone" placed on the side of a wall to hear and transcribe a conversation between defendants was "not a violation of the Fourth Amendment."[36]

Both *Olmsted* and *Goldman* "were products of the Court's failure to give weight to new technology and the way it functions in society."[37] Even with the spread of and reliance on technology in society, the Supreme Court continued to emphasize that the

---

30. *See id.* at 467 (explaining the circumstances necessary to invoke the protections offered by the Fourth Amendment).

31. *See id.* at 466 (determining that the government's wiretapping did not give rise to Fourth Amendment protections for the defendants).

32. *See* Price, *supra* note 26, at 267 (examining how the Supreme Court initially analyzed Fourth Amendment concerns about new technology in society).

33. *See* Olmstead v. United States, 277 U.S. 438, 465 (1928).

34. *Id.* at 474.

35. Goldman v. United States, 316 U.S. 129 (1942).

36. *See id.* at 131 (explaining that a detectaphone is a "listening apparatus" with earphones that allow law enforcement officers to hear the defendant through the wall).

37. Price, *supra* note 26, at 260.

Fourth Amendment's protection extends primarily to physical trespasses.[38] While the development of privacy protections under the Fourth Amendment continued, the Court was slow to depart from this trespass analysis.[39]

2. Informants and "False Friends"

In addition to analyzing Fourth Amendment cases through the lens of a physical trespass requirement, the Court also emphasized that generally, information revealed to third parties lacked sufficient Fourth Amendment protections.[40] In the 1952 case, *On Lee v. United States*,[41] the Court famously allowed law enforcement to submit evidence obtained from "informers, accessories, accomplices, [and] false friends" without violating the Fourth Amendment.[42] The Court explained that a defendant may still be implicated in a crime when she discusses her involvement in or knowledge of criminal activity with a government informant.[43] The fact that the defendant does not know the identity of the informant does not shield the defendant from liability.[44]

---

38. *See id.* (noting that following *Goldman* in 1942, the Supreme Court did not make a "shift away from the traditional concepts of property and trespass that had long dominated its jurisprudence" until 1967, when the Court "declar[ed] that the Fourth Amendment 'protects people, not places'" (citing Katz v. United States, 389 U.S. 347, 351 (1967))).

39. *See* Ryan Merkel, *Playing Hide and Seek with Big Brother: Law Enforcement's Use of Historical and Real Time Mobile Device Data*, 35 N. ILL. U. L. REV. 429, 439–40 (noting the Supreme Court's discussion of the trespass doctrine in recent location tracking technology cases).

40. *See* Rothstein, *supra* note 15, at 506–11 (discussing the Fourth Amendment search cases that helped establish the third-party doctrine).

41. *See* On Lee v. United States, 343 U.S. 747, 751 (1952) (finding no violation of the Fourth Amendment where an undercover federal agent entered the defendant's place of business with consent and used a radio to transmit self-incriminating statements made by the defendant to another federal agent who was stationed outside the defendant's place of business).

42. *See id.* at 757 ("We cannot say that testimony such as this shall, as a matter of law, be refused all hearing.").

43. *See id.* at 757–58 (stating that the informant's credibility may be attacked in court, but the court should admit evidence of the defendant's conversation with the informant).

44. *See id.* (suggesting that courts should not exclude testimony of "informers" or "false friends").

To do otherwise would "arbitrarily" penalize the government's case, because of the "low morals of its informers."[45] Continuing its analysis, the Court explained that while an informant's credibility may be attacked and questioned in court, evidence obtained from an informant should not be excluded.[46] The *On Lee* Court further reasoned that revealing information to individuals contains a risk that the receiver of the information may go to the police.[47]

3. Katz *and the Legal Framework for the Third-Party Doctrine*

As the Court continued to use the 1952 reasoning of *On Lee* to justify informant evidence, technology continued to advance. Finally, in 1967, the Court appeared to embrace Justice Brandeis's *Olmstead* dissent.[48] In the case of *Katz v. United States*,[49] the Court departed from the traditional application of the Fourth Amendment search analysis which had focused on the notion of physical trespass. *Katz* helped established the framework for the third-party doctrine.[50] The Court seemed to acknowledge emerging technology and society's expectation of privacy.[51]

In *Katz*,[52] the defendant was convicted of transmitting "wagering information" over a telephone from Los Angeles to

---

45. *Id.*

46. *See id.* (asserting that the testimony of government informants should be challenged using the traditional evidentiary canons such as relevance and credibility and should not be automatically excluded from trial).

47. *See* Price, *supra* note 26, at 266–67 (explaining how courts use assumption of the risk analysis in Fourth Amendment privacy cases).

48. *See* Olmstead v. United States, 277 U.S. 438, 468 (1928) (Brandeis, J., dissenting) ("Decency, security, and liberty alike demand that government officials shall be subjected to the same rules of conduct that are commands to the citizen.").

49. *See* Katz v. United States, 389 U.S. 347 (1967) (shifting from the traditional Fourth Amendment search analysis which had focused on physical trespass).

50. *See id.* at 353 (refusing to follow previous precedent which emphasized physical trespass to establish Fourth Amendment protections).

51. *See id.* (concluding that "[t]he [g]overnment's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth").

52. *Id.*

Miami and Boston.[53] Katz argued that the government violated his Fourth Amendment protections because FBI agents "attached an electronic listening and recording device to the outside of the public telephone booth from which he [Katz] had placed his calls" to conduct his wagering business.[54] Initially, the Court of Appeals for the Ninth Circuit continued the traditional analytical framework by emphasizing that there should be a trespass and physical seizure before recognizing a Fourth Amendment violation.[55] As a result, the Court of Appeals affirmed Katz's conviction and stated that his Constitutional protections were not violated.[56]

On appeal, the Supreme Court modified its traditional Fourth Amendment analytical emphasis on whether there was a physical trespass.[57] Instead, the Court acknowledged that:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[58]

Reversing Katz's conviction, the Supreme Court reasoned that the Constitution protects "people, not places."[59] The Court stated that the Fourth Amendment does not require a "technical trespass under . . . property law" before a Constitutional protection can be violated.[60] Distinguishing *Olmstead*, which relied on the need for a physical trespass and seizure of material before Fourth Amendment protections were violated, the Court stated that "we have since departed from the narrow view on which that decision

---

53. *Id.* at 348.

54. *Id.*

55. *See id.* (using precedent based on property law to determine if there was a Fourth Amendment violation).

56. *See* Katz v. United States, 369 F.2d 130, 134–35 (9th Cir. 1966) (affirming defendant's conviction primarily because there was no "physical entrance into the area occupied" by the defendant).

57. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (refusing to follow previous precedent which emphasized physical trespass to establish Fourth Amendment protections).

58. *Id.* at 351 (citing Lewis v. United States, 385 U.S. 206, 210 (1966); United States v. Lee, 274 U.S. 559, 563 (1927); Rios v. United States, 364 U.S. 253 (1960); Ex parte Jackson, 96 U.S. 727, 733 (1877)).

59. *Id.*

60. *Id.* at 353 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

[*Olmstead*] rested."[61] As a result, the Court altered its previous jurisprudential reliance on trespass law and held that the Fourth Amendment privacy protections against unreasonable searches and seizures applied in a case involving the use of a telephone booth.[62]

As Justice Harlan noted in his concurring opinion, a question remained: if the Constitution protects people and not physical places, how will the Court analyze this protection?[63] Justice Harlan outlined what became known as the *Katz* two-prong privacy test: first, whether "a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable."[64] Under the *Katz* test, Justice Harlan stated that the defendant had a "constitutionally protected reasonable expectation of privacy" inside the telephone booth, and law enforcement violated this expectation.[65]

4. Bank Records in United States v. Miller *and Pen Registers in* Smith v. Maryland

After Justice Harlan's *Katz* test, the Supreme Court considered two cases in the 1970's that were essential to establishing the third-party doctrine.[66] In 1976, the Supreme Court examined how the Fourth Amendment's privacy protections applied to a customer's bank deposit slips, checks, and financial records in the case of *United States v. Miller*.[67] While Miller

---

61. *Id.* at 353.

62. *See id.* at 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

63. *See id.* at 361–62 (Harlan, J., concurring) (suggesting that courts may need more of a clear standard to analyze Fourth Amendment claims with new technology).

64. *Id.*

65. *Id.* at 360–61.

66. *See* Markus & Wessler, *supra* note 17, at 1180–81 (explaining that the modern-day test courts use to evaluate Fourth Amendment privacy claims was created primarily in the 1970's).

67. *See* United States v. Miller, 425 U.S. 435, 436–38 (1976) (explaining that the bank ordering employees to make defendant's bank records available to police did not constitute a Fourth Amendment violation).

claimed that he disclosed the bank records to his bank "for a limited purpose" and therefore he retained an expectation of privacy under the first prong of the *Katz* test, the Court rejected his assertion.[68] Instead, the Court stated that "[w]e must examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents."[69]

Examining Miller's deposit slips, checks, and financial documents, the Court concluded that there was "no legitimate 'expectation of privacy'" because all the documents were either "not confidential communications but negotiable instruments to be used in commercial transactions" or "contain[ed] only information voluntarily conveyed to the banks" in the ordinary course of business.[70]

Interestingly, some scholars suggest that the nature of the documents played a role in the Court's analysis,[71] as follows:

> The Court found it significant that the documents in question were not sensitive in nature or shared with the intent that they stay private; rather, they were commercial instruments any employee could see. That, rather than their third-party nature, was why Miller—and by extension society—could not legitimately expect privacy in them.[72]

Furthermore, the Court explained that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[73]

---

68. *See id.* at 442–43 (stating that Court has examined the nature of the documents and acknowledged that the depositor assumes the risk that this information may be revealed to police).

69. *See id.* at 442 (affirming the defendant's conviction by using information about the defendant that the police obtained from the bank (citing Couch v. United States, 409 U.S. 322, 335 (1973))).

70. *Id.*

71. *See Acquisition*, *supra* note 3, at 1277; *see generally* Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1230–31 (2016) (discussing the modern version of this analysis and the interaction between informational fiduciaries and the Fourth Amendment).

72. *Id.* at 1277.

73. United States v. Miller, 425 U.S. 443 (1976) (citing United States v. White, 401 U.S. 745, 751–52 (1971)).

Not all the Justices in *Miller* agreed.[74] Foreshadowing the same issue that would arise when modern-day consumers sign up for cell phone service, Justice Brennan noted that the disclosure of information to a bank is "not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[75] Critically, he warned that the majority's reasoning and decision to allow third parties access to a citizen's sensitive and personal information without a search warrant may create serious Fourth Amendment concerns.[76] As Justice Brennan noted:

> To permit a police officer access to these records merely upon his request, without any judicial control as to relevancy or other traditional requirements of legal process, and to allow the evidence to be used in any subsequent criminal prosecution against a defendant, opens the door to a vast and unlimited range of very real abuses of police power.[77]

Three years after *Miller*, the Supreme Court examined whether law enforcement violated a defendant's Fourth Amendment protections by installing, without a warrant, a "pen register"[78] at a telephone company to determine which numbers a defendant was dialing from his private telephone line.[79] In *Smith v. Maryland*[80] the Court concluded that "no warrant was required."[81] The Court explained that Smith used the phone and "voluntarily conveyed" his information to the phone company.[82] As a result, he "assumed the risk" that his information would be revealed to police.[83]Furthermore, the Court explained that Miller

---

74. *See id.* at 455 (Marshall, J., dissenting) ("I wash my hands of today's extended redundancy by the Court.").

75. *Id.* at 451 (Brennan, J., dissenting).

76. *Id.*

77. *Id.*

78. *See* Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (explaining that a pen register is a mechanical device that records the telephone numbers dialed from the petitioner's home without overhearing the conversations).

79. *See id.* at 736 ("This case presents the question whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment . . . .").

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

81. *Id.* at 746.

82. *Id.* at 744.

83. *Id.*

had "no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"[84] The Court also emphasized that this expectation was "not one that society [was] prepared to recognize as 'reasonable.'"[85] Finally, the majority opinion stated that these pen registers "do not acquire contents of communication."[86]

Again, the Court was split.[87] Justices Brennan, Stewart, and Marshall dissented.[88] Justice Marshall and Justice Brennan recognized a principle that would apply to future cell phone customers, explaining that "it is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative" to using the technology in question.[89] Recognizing the prevalence of technology in society in 1979, the dissent stated that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[90]

Importantly, Justice Stewart's dissent suggested that although the phone numbers dialed from a private line may be more "prosaic" than the actual phone conversation, they are "not without content."[91] Justice Marshall's dissent noted that, without a search warrant, innocent people with nothing to hide could be negatively affected.[92] For example, "[m]any individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts."[93] The dissent explained that to allow:

---

84. *Id.* at 745.

85. *See id.* at 743–46 (explaining that society did not have this expectation of privacy (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring))).

86. *Id.* at 741.

87. *See id.* at 736–52 (demonstrating the divergence of views on this point).

88. *Id.* at 746–52.

89. *Id.* at 750 (Marshall, J., dissenting).

90. *Id.* at 750 (citing Lopez v. United States, 373 U.S. 427, 465–66 (1963)).

91. *Id.* at 748 (Stewart, J., dissenting).

92. *See id.* at 751–52 (warning that government intrusion into personal information without a probable cause warrant may raise significant and unintended Fourth Amendment concerns).

93. *Id.* (citing NAACP v. Alabama, 357 U.S. 449, 463 (1958); Branzburg v. Hayes, 408 U.S. 665, 695 (1972)).

> [G]overnmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I [Justice Marshall and Justice Brennan] am unwilling to insulate use of pen registers from independent judicial review.[94]

Because these privacy interests are significant, the dissent argued that law enforcement should be "require[d]" to obtain a warrant before seeking customers' information from the telephone companies .[95]

B. Fourth Amendment Privacy Issues and Modern Technology

These two cases from the 1970's, *Miller* and *Smith*,[96] helped create the framework for Fourth Amendment privacy analysis that courts still apply today.[97] While the legal analysis has not changed, technology has. As modern cell phones and other technologies have evolved, lower courts have struggled with the application of the third-party doctrine and the Supreme Court has generally "stayed out" of modern electronic surveillance.[98] Noting this dichotomy between the older legal doctrine and modern technology, the Supreme Court has issued several recent decisions that suggest a "new way forward."[99]

1. GPS in United States v. Jones

In 2012, the United States Supreme Court signaled that courts may need guidance in applying the third-party doctrine to new

---

94. *Id.* at 751 (Marshall, J., dissenting).

95. *Id.* at 752 (Marshall, J., dissenting).

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

97. *See* Markus & Wessler, *supra* note 17, at 1181 (discussing the current technologies available when the third-party doctrine originated).

98. Susan Freiwald, *First Principles of Communication Privacy*, 2007 STAN. TECH. L. REV. 3 (2007).

99. *See* Price, *supra* note 26, at 247 (citing Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945 (2012)).

technology, especially with regard to society's reasonable expectation of privacy.[100] In *United States v. Jones*,[101] government officials obtained a warrant to install a GPS tracking device under the defendant's car within ten days inside of the District of Columbia. Eleven days after the issuance of the warrant, officers installed the GPS device on Jones' car while in a parking lot in Maryland.[102] Law enforcement tracked "the vehicle's movements for 28 days."[103] The Court unanimously held, with two concurrences, that the tracking was an unlawful trespass and constituted a prohibited Fourth Amendment search.[104]

While *Jones* did not involve a third-party dispute such as those in *Miller* and *Smith*,[105] the two concurrences in *Jones* offer significant insights into possible ways of modernizing the third-party doctrine.[106] In her concurrence, believing that trespass could serve as a floor instead of a ceiling for privacy interests, Justice Sotomayor backed Justice Scalia and asserted that the *Jones* case demonstrated the need to consider society's reasonable expectation of privacy in the government's use of location-based tracking technology.[107] Justice Sotomayor stated that a "Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[108] She warned that "[w]ith increasing regularity, the government will be capable of duplicating the monitoring

---

100. *See generally* United States v. Jones, 132 S. Ct. 945 (2012).

101. *Id.*

102. *See id.* at 948 ("On the 11th day, and not in the District of Columbia but in Maryland, agents installed a GPS tracking device on the undercarriage of the Jeep while it was parked in a public parking lot.").

103. *Id.* at 946.

104. *See id.* at 947 (discussing the history of Fourth Amendment violations and emphasizing the trespass doctrine).

105. *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that a phone company's use of a pen register to record phone numbers dialed from the suspect's home upon police request did not constitute a "search" requiring a warrant under the Fourth Amendment); *see also* United States v. Miller, 425 U.S. 435 (1976) (expressing the view that the Fourth Amendment does not bar the acquisition of information provided to a third-party by subpoena).

106. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (emphasizing the privacy implications associated with Fourth Amendment searches).

107. *Id.*

108. *Id.* at 954–55.

undertaken in this case by enlisting factory or owner-installed vehicle tracking devices or GPS-enabled smartphones."[109] Knowledge of such GPS tracking "chills associational and expressive freedoms."[110]

While Justice Sotomayor's statements are arguably dicta, her recognition of the speed with which technology is changing and society's increasing expectations of privacy are directly relevant to the need for an updated analysis of the third-party doctrine in the context of obtaining cell phone location data.[111] While *Jones* was not a *per se* third-party doctrine case, Justice Sotomayor's five-page concurrence discussing the need for change to the third-party doctrine is significant. Her concurrence may mean the Supreme Court is willing to consider updating the doctrine in the appropriate case. Justice Sotomayor even seemed to signal that change could be imminent, writing, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[112]

Similarly, Justice Alito filed a concurrence which Justice Ginsburg, Justice Breyer, and Justice Kagan joined.[113] Justice Alito opined that the majority's opinion was "highly artificial" because it relies on eighteenth century tort law.[114] Instead, *Jones* presented the question of "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[115] Justice Alito accepted the *US v. Knotts*[116] decision, which stated that a beeper placed in a container to track the defendant's movements was constitutional because the defendant was traveling on public roads.[117] Justice

109. *See id.* at 955 (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1125 (9th Cir. 2010) (Kozinski, J., dissenting)).

110. *Id.* at 956.

111. *Id.* at 957.

112. *Id.* (citing Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976)).

113. *See id.* at 964 ("I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.").

114. *Id.* at 958.

115. *Id.* at 957–58.

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

117. *See id.* at 282 (discussing how traveling on public roads impacts certain

Alito also noted that monitoring a defendant without a warrant should be limited.[118] While *Jones* held that monitoring the defendant's movements for four weeks was considered a Fourth Amendment search, Justice Alito suggested:

> The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated. Under this approach, relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable.[119]

Justice Alito's approach also suggests that "the *Katz* test rests on the assumption that the hypothetical reasonable person has a well-developed and stable set of privacy expectations."[120] A person may have "a well-developed and stable set of privacy expectations. But technology can change those expectations."[121] As a result, he appears to suggest use of a balancing test, developed by the legislature, which would weigh the public interest against privacy concerns.[122]

In support of his suggestion, Alito notes that after *Katz*, instead of leaving the complex issue of wiretapping to the courts, Congress passed a federal wiretapping statute, 18 U.S.C.S. § 2510.[123] As with wiretapping, GPS tracking technology can also be intrusive and presents significant privacy concerns. Like cell phone tracking, GPS tracking can create an accurate and detailed

---

Fourth Amendment protection analysis).

118. *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (explaining the precision of advanced location tracking technology and arguing that "lengthy monitoring" of defendant's movements through GPS technology implicates Fourth Amendment protections).

119. *Id.* at 964 (citing United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

120. *Id.*

121. *Id.*

122. *See id.* (stating that perhaps the Fourth Amendment protections could be safeguarded while allowing police to use this advanced technology by balancing the public safety with the individual's privacy).

123. *See id.* at 963 ("After *Katz*, Congress did not leave it to the courts to develop a body of Fourth Amendment case law governing that complex subject. Instead, Congress promptly enacted a comprehensive statute . . . since that time, the regulation of wiretapping has been governed primarily by statute.").

record of a person's daily activities and impact privacy expectations:

> On toll roads, automatic toll collection systems create a precise record of the movements of motorists who choose to make use of that convenience. Many motorists purchase cars that are equipped with devices that permit a central station to ascertain the car's location at any time so that roadside assistance may be provided if needed and the car may be found if it is stolen.[124]

Obtaining tracking information through toll road collection systems or new car location devices, can "shape the average person's expectations"[125] of privacy. Thus, Justice Alito warned that the use of longer-term tracking "impinges on the expectation of privacy"[126] in society.

While the *Jones* Court concluded that the government's actions constituted a Fourth Amendment search, the Court did not define a bright-line test for determining an appropriate amount of time a defendant may be monitored without implicating constitutional protections.[127] Justice Alito's concurrence, which stated that only "relatively short-term monitoring"[128] may not constitute a search, provides guidance for determining if a Fourth Amendment violation has occurred in situations involving the latest technology.[129]

2. Cell Phones in Riley v. California

In the 2014 case of *Riley v. California*,[130] the Supreme Court required police to obtain a detailed search warrant specifying which parts of a cell phone they intended to search.[131] The Court

---

124. *Id.* at 963.

125. *Id.*

126. *Id.* at 964.

127. *See id.* at 950 (describing when a citizen's reasonable expectation of privacy is violated but not listing a definitive test applicable to this new technology).

128. *Id.* at 964.

129. *See id.* at 963 (stating that lengthy monitoring may conflict with modern notions of privacy because of the relative ease and breadth of technological snooping).

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

131. *See id.* at 2478 (discussing the risks associated with allowing police to

explained that a heightened expectation of privacy was applicable because of the personalized nature of cell phones.[132] Cell phones are "minicomputers" because of the amount and detailed information they contain.[133] Modern cell phones, the Court stated, "could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers."[134] Because cell phones can store and reveal highly personal information, the Court reasoned that "officers must generally secure a warrant" before searching the digital contents of a cell phone, even when a phone is seized incident to an arrest.[135]

Significantly, the *Riley* Court recognized that smartphones have the ability to "reconstruct someone's specific movements down to the minute, not only around town but also within a particular building."[136] While *Riley* was not a *per se* third-party information case, it implicated third-party doctrine concerns. Specifically, the Court expressed concern about the amount of data accessible through the device as well as its geo-tracking capabilities.[137] While the government argued that procedures can be established to protect citizens from the intrusive nature of these technologies, the Court emphatically noted that "the Founders did not fight a revolution to gain the right to government agency protocols."[138] As a result, the privacy concern helped the Court

---

obtain certain data without a warrant).

132. *See id.* at 2479 (articulating that "today [2014] many of the more than 90% of American adults who own cell phones keep on their person a digital record of nearly every aspect of their lives").

133. *See id.* at 2489 (describing that cell phones are like minicomputers because of their immense storage capacity).

134. *Id.*

135. *See id.* at 2485 (explaining that warrants would help protect Fourth Amendment concerns involved with this highly revealing technology).

136. *See id.* at 2490 (describing how different technologies can reveal a significant amount of information).

137. *See id.* ("Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

138. *Id.* at 2491.

conclude that law enforcement should seek a specified warrant before obtaining a smartphone user's personalized information.[139]

3. CSLI in United States v. Graham

Justice Alito's concurrence in *Jones* and the Court's reasoning in *Riley* suggest that changes to the third-party doctrine are necessary and imminent. As technology continues to advance, and time-specific location information becomes more accurate, courts are struggling to keep pace.[140]

A more recent Fourth Circuit case illustrates the current disagreement over applying the third-party doctrine. *United States v. Graham*[141] involved a report of several armed robberies over the course of a few weeks.[142] Investigating this report, police stopped Aaron Graham's car with passenger Eric Jordon because the car and defendants matched witness descriptions from a recent robbery.[143] The police found a gun in the car. Both Graham and Jordan provided police their cell phone numbers.[144] Police then sought a court order under the Stored Communication Act (SCA), which was granted based on "specific and articulable facts"[145] instead of a probable cause warrant. The government wanted to use the defendants' cell phone location information to "more conclusively link the [d]efendants"[146] to the robberies.

---

139. *See id.* at 2494–95 (stating that the "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").

140. *See* Silliman, *supra* note 6 (emphasizing that technology continues to rapidly advance and courts cannot keep applying old law to current technology).

141. *See* United States v. Graham, 796 F.3d 332, 338 (4th Cir. 2015) (illustrating how the third-party doctrine applied in a case with robberies).

142. *See id.* (stating that this "prosecution arose from a series of six armed robberies of several business establishments" occurring from January 17, 2011 to February 5, 2011).

143. *See id.* at 339–41 (stating that the car and clothing of the defendants matched witness descriptions of the robbers).

144. *See id.* at 340 (explaining the factual circumstances in which the defendants were stopped by police).

145. *See id.* at 387 (discussing the police procedure and reasons for applying the court order).

146. *See id.* at 386 (showing the government's motive for using the defendants' cell phone location information).

Moving to suppress the cell location information evidence, the defendants did not allege that the SCA is *prima facie* unconstitutional, but argued instead that the SCA as applied to their circumstances violated the Fourth Amendment.[147] They stated that the length of time and extent of monitoring without a probable cause warrant violated the defendants' reasonable expectation of privacy and should be deemed unconstitutional.[148] By use of a court order, without a probable cause warrant, police were able to collect "two hundred and twenty-one days and 20,235 individual cell site location data points" from the defendants' cell phone location data.[149] With this information, the government was then able to "place [the defendants] in the vicinity of the armed robberies when the robberies had occurred."[150]

The government argued that "by using their cellular phones, and thereby voluntarily conveying their approximate location to their service provider, the Defendants can claim no legitimate expectation of privacy in that data—in other words, the Fourth Amendment simply does not apply."[151] The lower court held that the defendants' rights were not violated because the SCA[152]

---

147. *See id.* at 342 ("Appellants filed a motion to suppress use of the CSLI at trial, arguing that the government's acquisition of the records without a warrant based on probable cause was an unreasonable search in violation of the Fourth Amendment.").

148. *See id.* at 407 (describing the defendants' challenge that the government's use of their CSLI violated their Fourth Amendment protections).

149. *Id.* at 387.

150. *See id.* at 424 (showing how the government placed the defendants in the vicinity of the armed robbery).

151. *See* United States v. Graham, 846 F. Supp. 2d 384, 388 (2012) (describing why the Fourth Amendment does not apply in this case).

152. *See* 18 U.S.C. § 2703(d) (1986) (explaining when a court can issue orders which allow government entities to receive information from cell phone providers). The statute states:

> [A] court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature

allowed the government to obtain records from the cell providers that were kept "in the ordinary course of business."[153]

On appeal, the Fourth Circuit "declined to apply the third-party doctrine" and held that the appellants "have a reasonable expectation of privacy in their long-term CSLI."[154] The Court "conclude[d] that the government's procurement and inspection of Appellants' historical CSLI was a search, and the government violated Appellants' Fourth Amendment rights by engaging in this search without first securing a judicial warrant based on probable cause."[155] Although the Court found a Fourth Amendment violation, the Court also ruled that the CSLI "records were not subject to suppression" because the government acted in "good faith" applying for "court orders issued under the SCA."[156]

Rehearing the case en banc in 2016, the Fourth Circuit applied the third-party doctrine and held that defendants' Fourth Amendment protections were not violated because the "Government legally acquired those records."[157] The majority opinion seemed to invite the Supreme Court or Congress to change the current third-party doctrine as follows:

> The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI cell-site location information. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case.[158]

The Fourth Circuit in *Graham* went on to state that "Supreme Court precedent mandates this conclusion."[159] The Supreme

---

> or compliance with such order otherwise would cause an undue burden on such provider.

Id.

153. *See Graham*, 846 F. Supp. 2d at 388–90 (articulating that a Fourth Amendment violation had not occurred because the information obtained by police was voluntarily submitted to the third parties and held in the ordinary course of business).

154. *See* United States v. Graham, 796 F.3d 332, 360 (4th Cir. 2015) (discussing the Fourth Circuit's holding on appeal).

155. *Id.*

156. *Id.*

157. *See* United States v. Graham, 824 F.3d 421, 438 (4th Cir., 2016) (explaining the Fourth Circuit's holding when rehearing the case en banc).

158. *Id.* at 425.

159. *Id.*

Court's mandate, however, may not be so clear. As noted in Part II below, there is disagreement in the lower courts as to the exact nature of the Supreme Court's guidance regarding cell phone tracking technology and the third-party doctrine.

Under the SCA, the government must prove "specific and articulable facts"[160] instead of probable cause to obtain a cell phone's location information. This "specific and articulable facts" standard has been criticized by scholars for not being a sufficient standard to protect privacy rights.[161] Demonstrating the need for clarity, several judges in *Graham* concurred and dissented. In Judge Wilkerson's concurrence, he stated the warrant requirement should be considered by Congress.[162] Judge Winn dissented and Judge Floyd and Judge Thacker dissented in part and concurred in part. Judge Winn expressed the following concern:

> A customer buys a cell phone. She turns it on and puts it in her pocket. With those acts, says the majority, she has "voluntarily conveyed" an unbounded set of personal location data to her service provider, all of which is unprotected by the Fourth Amendment.[163]

Some scholars claim that the basis for Judge Winn's statement is, "[c]ell phone users do not know about the CSLI shared by their phones, and they take no discrete action in order to convey it (aside from mere use)."[164] As a result, it appears that the *Graham* decision "shows the third-party doctrine's flaw: in its focus on categorizing behavior, it does not accurately estimate what society today would consider reasonable."[165] *Graham* needs to be updated to "reflect our [society's] complex and changing relationship with

---

160. *See id.* at 426 (discussing what the government must prove under the SCA).

161. *See* Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1750–52 (2009) (arguing that courts should be required to use a probable cause standard instead of a "specific and articulable facts" standard before allowing either historical or real-time CSLI to be disclosed).

162. *See Graham*, 824 F.3d at 435, 438–39 (Wilkerson, J., concurring) (stating Congress is better adept to deal with CSLI privacy concerns).

163. *See id.* at 441 (Wynn, J., dissenting) (stating that consumers do not voluntarily convey privacy information when they purchase a phone).

164. *See Acquisition*, *supra* note 3, at 1276 (stating the basis for Judge Winn's statement).

165. *Id.* at 1273.

technology."[166] Illustrating this need, courts have reached varying conclusions when applying the third-party doctrine.

II. Into the Bog: Confusion in the Courts

Many courts have applied the third-party doctrine to similar factual circumstances, but have reached different legal conclusions. The courts are in a "Serbonian Bog" of confusion.[167] National research conducted by the American Civil Liberties Union (ACLU) displayed on the map below illustrates how different courts have reached different conclusions and demonstrates that the precedent is not as established as the Fourth Circuit stated in *Graham*.[168] The courts need clear guidance when addressing the government's use of CSLI.

166. *Id.*

167. *See* United States v. Lambis, 197 F. Supp. 3d 606, 614 (S.D.N.Y. 2016) (showing how different courts apply the third-party doctrine to similar factual circumstances).

168. *See* United States v. Graham, 824 F.3d 421, 425 (4th Cir. 2016) (illustrating the wide variety of third-party doctrine interpretation).

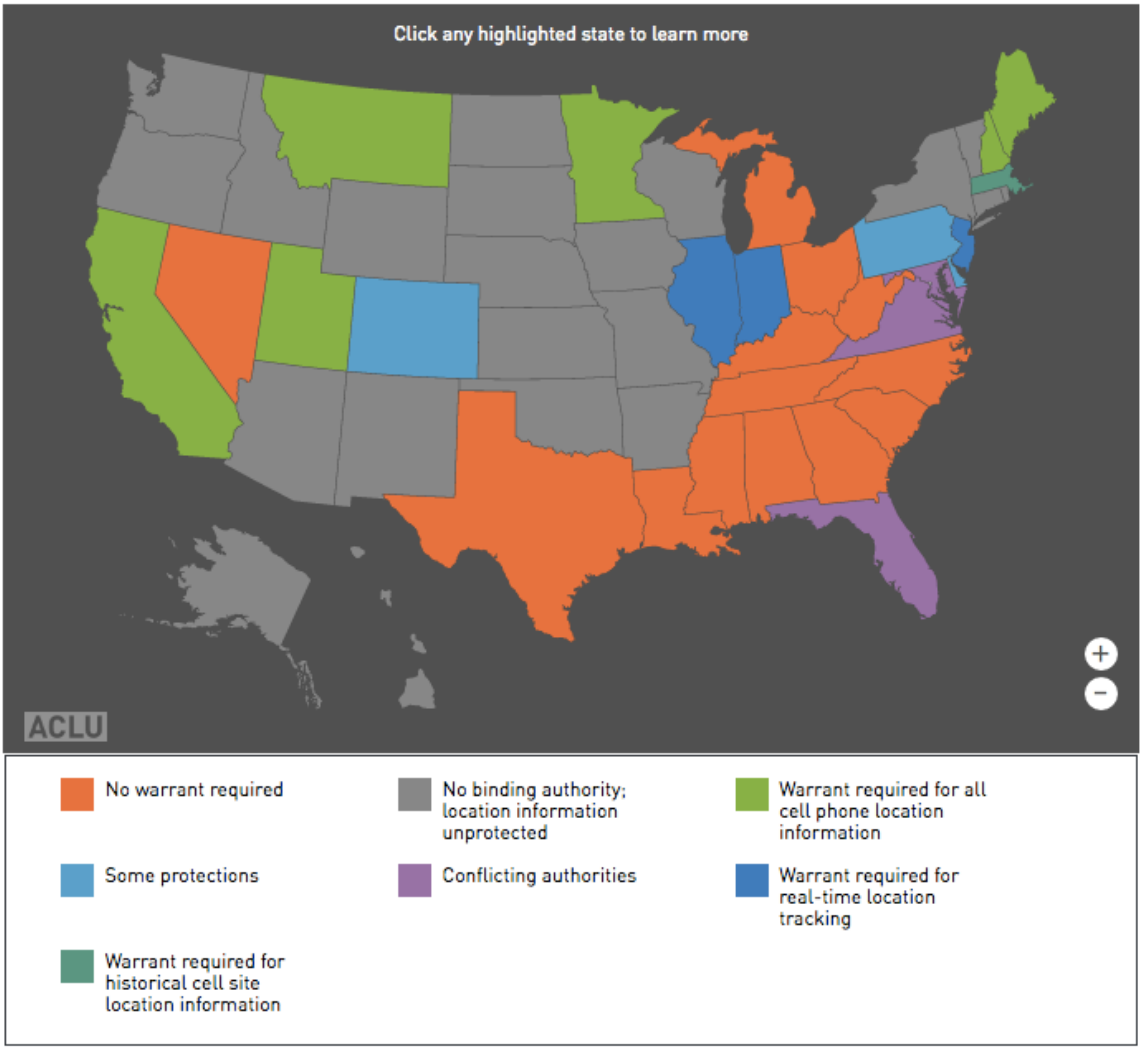

Figure 1[169]

169. *See Cell Phone Location Tracking Lawsby State*, AM. C.L. UNION, https://www.aclu.org/map/cell-phone-location-tracking-laws-state (last visited Nov. 29, 2017) (displaying various applications of the warrant requirement under the third-party doctrine) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

A. Distinguishing Between Type of Data and Technology

Courts disagree about whether a warrant is required for real-time CSLI. Scholar Teresa Reed explains "the Florida Supreme Court ruled in *Tracey v. State* that the warrantless use of cell site location information to track an individual during the course of a single day's car trip violated the Fourth Amendment."[170] Displaying the contradictory nature of this doctrine, not all courts reach the same result. Examining these different conclusions, scholars David Oscar Markus and Nathan Freed Wessler explain that in one 2012 Sixth Circuit case, the Court held that "the Fourth Amendment does not apply to shorter-term real-time tracking of a cell phone user's location during a single three-day multi-state trip on public highways."[171] Therefore, it is apparent that courts apply varying analyses to reach these difficult decisions involving technology and privacy.

Recently, courts have distinguished between the different types of content. For example, several courts have held that reading email content qualifies as a Fourth Amendment search requiring a warrant.[172] The Sixth Circuit has stated that even though email subscribers voluntarily submit this information to third-party internet providers, their reasonable expectation of privacy requires the government to get a warrant before obtaining this information.[173] The Ninth Circuit, however, has held that obtaining email address information, IP addresses, and email data, does not qualify as a Fourth Amendment search and does not require a warrant.[174]

---

170. Teresa Reed, *Digital Privacy in the Post-Riley World*, Outline, STAN. L. SCH. 1–11, 2 (2015).

171. *See* Markus & Wessler, *supra* note 17, at 1197 n.90 ("The court reserved decision about 'situations where police, using otherwise legal methods, so comprehensively track a person's activities that the very comprehensiveness of the tracking is unreasonable for Fourth Amendment purposes.'" (quoting United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012))).

172. *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (stating that the privacy interests associated with this technology were violated when the government compelled the production of emails without first obtaining a warrant based on probable cause).

173. *See id.* at 287–88 (describing the difference between content and non-content privacy concerns with emails).

174. *See* United States v. Forrester, 512 F.3d 500, 504 (9th Cir. 2008) (stating that Fourth Amendment privacy interests were not violated because the manner

In *United States v. Forrester*,[175] in the Ninth Circuit, the Court noted that "the techniques the government used to monitor the defendant's "email and internet activity," including IP addresses and amount of data transmitted does violate the defendant's Fourth Amendment protections.[176] Differentiating between the privacy expectations in the use of these different and evolving modern technologies may be difficult because the third-party doctrine has remained static.[177]

B. Federal Magistrate Discretion

As a result of different courts reaching different conclusions and attempting to distinguish between technologies, one federal circuit reasoned that federal magistrate judges should have discretion to decide whether a warrant is required on a case-by-case basis for CSLI requests.[178] The Third Circuit has stated that magistrates have the discretion to issue these court orders on a "lesser"[179] standard than probable cause, but can also "require a warrant showing probable cause."[180] The Third Circuit stated that this power should be used "sparingly."[181] As a result, courts often employ the reasonable expectation of privacy analysis which leads to differing results.[182] As noted, the reasonable expectation of

---

in which the information was revealed was similar to the use of a pen register).

175. United States v. Forrester, 512 F.3d 500 (9th Cir. 2008).

176. *Id.* at 510–13.

177. *See* Orin S. Kerr, *The Mosaic Theory of The Fourth Amendment*, 111 MICH. L. REV. 311, 311–12 (2011) (emphasizing that Fourth Amendment issues continue to confuse courts as technology develops).

178. *See* Markus & Wessler, *supra* note 17, at 1198 (discussing the various approaches different circuits use when evaluating the constitutionality of CSLI searches (citing In re United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010))).

179. In re United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010).

180. *Id.* at 318.

181. *Id.*

182. *See* Markus & Wessler, *supra* note 17, at 1202 (arguing that more courts should use the reasonable expectation of privacy analysis when determining if the Fourth Amendment requires the government to obtain a search warrant before obtaining a consumer's cell-site location).

privacy analysis has created confusion and disagreement among the circuits.

C. Different Reasoning; Similar Results

The Third, Fourth, Fifth, Sixth,[183] and Eleventh Circuits have upheld the government's collection of defendant's CSLI without a warrant.[184] Even when circuits reach the same conclusion, they often offer significantly different justifications. For example, the Fifth Circuit has held that a defendant "voluntarily" submits her location information to the cellular service provider, therefore allowing police to obtain it from the cellular company without a warrant.[185] While the Eleventh Circuit agrees to the extent that police do not need a probable cause warrant to collect this location information, that Court has held that this information is not voluntarily conveyed.[186]

The Sixth Circuit in *United States v. Skinner*[187] and in *United States v. Carpenter*[188] opined that law enforcement does not violate Fourth Amendment protections when obtaining CSLI without a probable cause warrant.[189] Sitting en banc, the Eleventh Circuit

183. *See* United States v. Warshak, 631 F.3d 266, 274 (6th Cir. 2010) (suggesting that this holding may be unstable in the Sixth Circuit).

184. *See* Porter, *supra* note 3, at 1782–83 (discussing how courts have analyzed the third-party doctrine (citing United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016); United States v. Davis, 785 F.3d 498, 500–01 (11th Cir. 2015) (en banc), *cert. denied*, 136 S. Ct. 479 (2015); In re Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013); In re United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 313 (3d Cir. 2010))).

185. *See* Porter, *supra* note 3, at 1798–99 (evaluating different reasons for upholding the third-party doctrine (citing In re Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013))).

186. *Id.* at 1798 (clarifying the different conclusion reached by the Eleventh Circuit (citing United States v. Davis, 785 F.3d 498, 500–01 (11th Cir.) (en banc), *cert. denied*, 136 S. Ct. 479 (2015))).

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

188. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016).

189. *See Skinner*, 690 F.3d at 774 (stating that the Constitution does not provide protections for the defendant's "erroneous expectations" of privacy under the Fourth Amendment associated with modern technology); *see also id.* at 887–88 (6th Cir. 2016) (explaining that the CSLI collected by the cellular carrier in this case is "unprotected" by the Fourth Amendment).

recently stated in *United States v. Davis*[190] that because the government is required under the SCA to prove specific and articulable facts before a court order is issued, any expectation of privacy the defendant may have regarding his CSLI is "not justifiable."[191] Agreeing with the Fifth Circuit, the Eleventh Circuit explained as follows:

> Cell 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.[192]

Adopting a different standard than the Eleventh Circuit, the Fifth Circuit has taken the position that the courts do not have "discretion" to deny the government a court order for CSLI as long as the government has complied with the "specified and articulable" facts standard noted in SCA § 2703.[193]

Adding to the varying analyses among the circuits, the Third Circuit has held that law enforcement may obtain CSLI from third-party providers, not based on the third-party doctrine, but rather based on the "public disclosure doctrine."[194] The public disclosure doctrine suggests that law enforcement is justified in obtaining location-based cell phone information because this technology tracks "voluntary movements that are susceptible to visual surveillance" similar to those on a public street or highway.[195] Under this doctrine, police are treated as ordinary citizens and may track the public movements of an individual without violating

---

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

191. *Id.* at 511.

192. *Id.*

193. 18 U.S.C.S. § 2703; *see* In re the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (stating that this standard is the "proper framework" for evaluating privacy concerns associated with CSLI).

194. *See* Bedi, *supra* note 14, at 517 (explaining that the Third Circuit used a different analysis than other courts, but reached the same conclusion about CSLI obtained without a probable cause warrant (citing In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010))).

195. *See id.* at 521 (explaining the analysis of and justification for the public disclosure doctrine).

Fourth Amendment protections.[196] Some scholars suggest that at least in one case, if the Third Circuit used the third-party doctrine instead of the public disclosure analysis, the Court might have required a warrant to obtain location-based information.[197] The Third Circuit and the Fifth Circuit reached the same conclusion, but based their decisions on different doctrines.

D. The Case for a Probable Cause Warrant

Numerous courts reject the Fifth Circuit's position which limits judicial discretion. In the Seventh Circuit, a District Court in Indiana denied the government's SCA §2703 request for "location-based services"[198] revealing CSLI information. Specifically, the Court opined that seeking this information requires a "probable cause" standard.[199] Contrary to the Fifth Circuit's approach, a Seventh Circuit District Court also asserted that CSLI information the government requested was "unobtainable absent a warrant."[200]

Patrick Chamberlain examined a 2008 Western District of Pennsylvania case which held that probable cause is the proper standard when determining whether to allow the government to view customers' cell site location information.[201] In 2014, the First Circuit of Massachusetts Court concluded that suspects have an objective expectation of privacy in their CSLI and therefore, police should be required to obtain a warrant before gathering this

196. *See id.* at 521–22 (analyzing how the public disclosure doctrine relates to the third-party doctrine and Fourth Amendment concerns with modern technology).

197. *See id.* at 517 (suggesting that the Third Circuit would have reached a different conclusion if it did not focus on the public disclosure doctrine (citing In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010))).

198. In re United States for an Order: Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, Nos. 1:06-MC-6, 1:06-MC-7, at 3 (N.D. Ind. 2006).

199. *Id.* at 13–14.

200. *Id.* at 3–4.

201. *See* Chamberlain, *supra* note 161, at 1750 (explaining that the District Court rejected the more general "specific and articulable facts" standard (citing In re United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 586 (W.D. Pa. 2008))).

potentially incriminating and revealing information.[202] While the defendant's motion to suppress CSLI evidence was eventually vacated, one Judge opined that "[a] person obtains a cellular telephone for the purpose of making and receiving telephone calls, not to permit the telephone company or another third-party to track the user's location when the person is not using the telephone."[203]

III. Out of the Bog; Proposed Solutions

The proposed solutions to the problem of how to modernize the third-party doctrine span "the ideological spectrum."[204] This Note proposes that the Fourth Amendment requires the government to obtain a probable cause warrant to acquire CSLI data.[205]

A. Third-Party Search Exception

Akhil Amar (Amar) suggests that the Fourth Amendment and Warrant Clauses are separate and should not be read together.[206] Lucas Issacharoff (Issacharoff) and Kyle Wirshba (Wirshba) explain that using Amar's approach, another way to reexamine the

---

202. *See generally* Commonwealth v. Augustine, 4 N.E.3d 846 (Mass. 2014) (granting defendant's pretrial motion to suppress CSLI evidence), *rev'd*, Commonwealth v. Augustine, 4 N.E.3d 846, 868 (Mass. 2014) (vacating defendant's motion to suppress).

203. *See Augustine*, 4 N.E.3d at 872 (Gants, J., dissenting) (asserting that the third-party doctrine should apply to telephone toll records as well as CSLI).

204. Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 997 (2016).

205. *See* VA. CODE ANN. §§ 19.2–70.3 (2015) (requiring the government to obtain a warrant to collect real-time CSLI tracking from third-parties under Virginia law). While this statute provides law enforcement possible guidance for the third-party doctrine, to provide consistent Fourth Amendment privacy protections the government should also be required to obtain a warrant before collecting historical CSLI.

206. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 761 (1994) (stating that the words of the Fourth Amendment and the Warrant Clause "do not require warrants, even presumptively, for searches and seizures. They do not require probable cause for all searches and seizures without warrants").

third-party doctrine would be to rely on "a single inquiry into reasonableness."[207] The Fourth Amendment analysis under this proposition focuses on whether the law enforcement tactics were reasonable, and places less emphasis on the warrant and probable cause aspect of the analysis.[208] As Issacharoff and Wirshba admit, courts and scholars suggest that focusing only on reasonableness would too often create "an occasion for constitutional review."[209]

As a result, Issacharoff and Wirshba claim that "third-party searches are better characterized as a new type of warrant exception than as either a search subject to the warrant and probable cause requirements or a non-search unregulated by the Fourth Amendment."[210] Accordingly, they propose that courts should "recognize third party searches as another exception to the warrant requirement, and accordingly craft a reasonableness test to gauge when third party searches are constitutionally appropriate."[211] Arguing that in third-party doctrine cases a probable cause requirement "should not attach by default," these scholars opine that "the constitutional imposition of a warrant requirement would both overprotect information in which individuals have a diminished expectation of privacy and unduly hamper law enforcement interests."[212] Rather, third party searches should be governed by, but not solely reliant on, the Reasonableness Clause.

Discussing reasonableness, Issacharoff and Wirshba appear to disagree with Amar's focus on the "kitchen sink reasonableness inquiry in every case."[213] Rather Issacharoff and Wirshba argue that courts should adopt Chief Justice Warren's approach in *Terry*

---

207. Issacharoff & Wirshba, *supra* note 204, at 1009.

208. *See id.* at 1009 ("The core of the Fourth Amendment, as we have seen, is neither a warrant nor probable cause, but reasonableness." (quoting Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 802 (1994))).

209. *See id.* at 1011 (arguing that reliance on this factor would "conver[t] the fourth amendment into one immense Rorschach blot" (citing Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 393 (1974))).

210. *Id.* at 986.

211. *Id.* at 1012.

212. Issacharoff & Wirshba, *supra* note 204, at 1012.

213. *Id.* at 1029 (quoting Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 761 (1994)).

v. Ohio[214] as a model for third-party doctrinal analysis. *Terry* involved a law enforcement officer stopping and frisking a citizen.[215] The Court balanced the government's interest against the individual's interest.[216] Considering the validity of a stop and frisk, the new test the Court considered asked "whether a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger."[217] In *Terry*, this reasonably prudent man was the law enforcement officer.[218]

Attempting to create a single test that law enforcement could apply in the field and courts could easily adopt, the *Terry* Court did not initially focus its analysis on the specific facts of the case. Instead, it created a "general proposition" of balancing the risks associated with the search.[219]

Because some scholars argue that citizens have a diminished expectation of privacy with modern technology, courts considering the third-party doctrine should focus on law enforcement's reasonableness in conducting the search. As a result, instead of examining "total quantity of information" or "types of third party information," it is suggested that under this *Terry* approach courts should "take a step back and conduct a one-time balancing of the reasonableness of government access to third party material 'as a general proposition.'"[220]

Under this framework, it is suggested that "[t]he Terry Court's move from a case-by-case balancing to a uniform standard can be used to create an equally administrable standard for third party materials."[221] This reasonable suspicion test for third party

---

214. Terry v. Ohio, 88 S. Ct. 1868 (1968) (citing Beck v. Ohio, 379 U.S. 89, 91 (1964); Brinegar v. United States, 338 U.S. 160, 174–76 (1949); Stacey v. Emery, 97 U.S. 642, 645 (1878)).

215. *Id.* at 1872–73.

216. *Id.* at 1879.

217. *Id.* at 1883.

218. *See id.* ("The officer need not be absolutely certain that the individual is armed; the issue is whether a reasonably prudent man in the circumstances would be warranted in the belief that his safety or that of others was in danger.").

219. *Id.* at 1879 (citing Camara v. Mun. Ct. 387, U.S. 523, 534–35) (1967)).

220. *Id.* at 1034.

221. *Id.* at 1033.

searches, some scholars argue, is a practical middle ground.[222] Similar to *Terry*, in third party situations, "officers should be able to point to specific, articulable facts supporting a reasonable suspicion that the third party search will turn up information relevant to an ongoing investigation, and searches should be reasonable in scope."[223] While opponents of a warrant requirement argue that consumers lack an expectation of privacy in the information submitted to their cellular provider,[224] even proponents of this theory admit that the expectation of privacy is not totally diminished.[225]

Many judges and scholars agree that cell phone consumers have a legitimate expectation of privacy. As Justice Marshall and Justice Brennan have noted, if there is no practical real alternative to an action, the action should not be considered voluntary.[226] Richard Epstein (Epstein) states that this diminished expectation of privacy is not assumed.[227] Epstein argues that the Fourth Amendment should require a balancing of interests to determine the reasonableness of the privacy component of a particular case. He explains that:

In essence the task is finding that set of rules which, when laid down generally, produces the best mix of privacy and security that can be obtained in light of the limited available knowledge, taking into account that the Fourth Amendment protects not only the guilty, but also innocent persons who may have been swept into a search.[228]

Responding to Epstein's assertion of a cost-benefit test for advanced technologies, Orin Kerr (Kerr) suggests that this

---

222. *Id.* at 1030–31.

223. *Id.* at 1036.

224. *See* Porter, *supra* note 3, at 1789 (articulating the argument that customers lack a reasonable expectation of privacy to this information).

225. *See* Issacharoff & Wirshba, *supra* note 204, at 1021 (explaining that this expectation of privacy is "diminished, though not nonexistent").

226. *See* Smith v. Maryland, 442 U.S. 735, 750 (1979) (Brennan, J., & Marshall, J., dissenting) (stating that consumers do not voluntarily convey this privacy information).

227. *See generally* Richard A. Epstein, *Privacy the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH L. J. 1199 (2009) (discussing the assumption of the risk with CSLI is forced on individuals).

228. *Id.* at 1202.

balancing approach has already been used by courts.[229] Furthermore, Kerr states that Epstein's argument significantly differs from his because Epstein does not subscribe to an "all or nothing"[230] approach to the Fourth Amendment. Kerr believes that police action either is or is not a search.[231] If it is a search, then it requires a probable cause warrant.[232]

Kerr defends the advantages of the third-party doctrine which consist of "technological neutrality of Fourth Amendment rules"[233] and provides "ex ante clarity."[234] While Kerr disagrees with many scholars' arguments, he recognizes that many authors and courts suggest that a significant change to the third-party doctrine is necessary. Kerr explains that the third-party doctrine inquiry should be a fact specific determination of whether the person acted reasonably and had a reasonable expectation of privacy.[235] He explains that "[t]his is a prospective inquiry from the standpoint of the suspect: The question is whether a reasonable person in the suspect's situation would expect the information to be widely disseminated."[236]

Given Kerr's argument about reasonableness, Justice Alito's concurrence in *Jones* is significant. Justice Alito stated that advancing technology may change society's expectations of privacy.[237] If there is no realistic alternative to using a technology, and a particular technology is necessary to function in modern society, then Justice Alito is correct that this information is not "voluntarily" disclosed to third parties. Suggesting that society has

---

229. *See* Orin S. Kerr, *Defending the Third-Party Doctrine: A Response to Epstein and Murphy*, 24 BERKELEY TECH L. J. 1229, 1230 (2009) [hereinafter Kerr, *Defending*] (discussing the balancing analysis many courts already use).

230. *Id.* at 1232.

231. *Id.* (articulating his all-or-nothing standard to Fourth Amendment law).

232. *See id.* (discussing the general implications of a police search).

233. *Id.* at 1231 (stating that balancing the interests of a prisoner's privacy in her cell and society's interest, the interests of society outweigh the prisoner's (citing Hudson v. Palmer, 468 U.S. 517 (1984))).

234. *Id.*

235. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 583 (2009) (evaluating alternatives to replace the third-party doctrine).

236. *Id.*

237. See United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring) (stating that society's reasonable expectation of privacy may change with modern location tracking technology).

already recognized a heightened expectation of privacy because of the pervasive use of technology, many scholars suggest that society may already have an objective expectation of privacy for location emitting devices, such as cell phones.[238] If society has a reasonable expectation of privacy, then perhaps a more persuasive modification to the third-party doctrine is to require a probable cause warrant for CSLI.

B. Probable Cause Requirement for Third-Party Searches

Many scholars argue that the pervasive use and ubiquitous existence of current technologies mandate more protection than a court order based on specific and articulable facts. Scholars Priscilla J. Smith, Nabiha Syed, David Thaw, and Albert Wong suggest the following:

> [The] type and scope of information collected by prolonged automated GPS surveillance enables governments to monitor a person's political associations, their medical conditions and their amorous interests, in a way that invades their privacy and chills expression of other fundamental rights.[239]

As a result of the nature of this technology, law enforcement should be required to obtain warrants "to prevent abuse" of Fourth Amendment privacy protections.[240] Without a warrant, prolonged GPS surveillance disturbs society's reasonable expectation of privacy and "chills the exercise of core constitutional rights."[241] These scholars argue that the continuous monitoring of GPS information presents a different question than the Court's

---

238. See generally Riley v. California, 134 S. Ct. 2473 (2014) (Alito, J., concurring) (holding that individuals have a reasonable expectation of privacy in their personal cell phones because of the amount of personal information they contain).

239. Priscilla Smith et al., *When Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L. J. 1, 6 (2011) [hereinafter *When Machines Are Watching*] http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1001&context=ylas (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

240. *Id.* at 220–21.

241. *Id.* at 221.

precedent of *Knotts*[242] which involved beeper technology.[243] GPS technology not only continuously provides location information, but unlike previous beeper technology, it does not require officers to follow the suspect.[244] Furthermore, GPS is more intrusive because these devices can "store" location information and transmit this information to a variety of parties, revealing common patterns, preferences, and more intrusive information than a traditional beeper.[245]

Additionally, as the Court noted in *Kyllo*,[246] a significant factor for Courts to consider is whether the technology is in "general public use."[247] While GPS technology is embedded in all smartphones today, the use of "GPS *surveillance* technology, however, is not accepted by the public." "[248] Because cell phones may have the capacity to track an individual's movements down to a few feet,[249] it seems credible that this surveillance location information infringes on a reasonable expectation of privacy. Some scholars argue that, "[i]n fact, Americans become uncomfortable with GPS when there is even a slight loss of user-control."[250]

While there are many proposed iterations of the third-party doctrine, there is one consistent, overriding factor: with the

---

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

243. *See id.* (discussing the relationship between beeper technology and Fourth Amendment privacy concerns").

244. *When Machines Are Watching*, *supra* note 239, at 21.

245. *Id.* at 23.

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

247. *Id.* at 34.

248. *When Machines Are Watching*, *supra* note 239, at 24.

249. *See* Jonathan Rodriguez, *Uptick in Police Surveillance Tech Sparks New Opportunity*, WALL ST. DAILY (Feb. 16, 2017), https://www.wallstreetdaily.com /2017/02/16/uptick-police-surveillance-tech-sparks-new-opportunity/ (discussing the recent trend of and accuracy associated with the government using cell phone location tracking technology) (on file with the Washington & Lee Journal of Civil Rights & Social Justice); *see also* Robinson Meyer, *How the Government Surveils Cellphones: A Primer*, ATLANTIC (Sep. 11, 2015), http://www.theatlantic.com/ technology/archive/2015/09/how-the-government-surveils-cell-phones-a-primer/404818/ (explaining the precision of different CSLI technologies the government uses) (on file with the Washington & Lee Journal of Civil Rights & Social Justice).

250. *When Machines Are Watching*, *supra* note 239, at 24, 24 n.35 (stating that "GPS technology is also used by some private and government employers to ensure job performance and service delivery").

amount of tracking information that a smartphone can capture, hold, and reveal, people in modern society have a reasonable expectation of privacy in this information. This expectation should require a higher and clearer standard than specific and articulable facts before such detailed personal information is turned over to law enforcement. As some argue, if there is not a warrant requirement, there is an "unprecedented" potential for abuse of privacy protections.[251] Recently, legislation has been introduced in Congress to address the issue of government searches of cell phone location information.

C. Legislative Solution

As several courts have suggested, given how quickly technology changes, the legislature may be in the best position to modernize the third-party doctrine. In *Riley*, Justice Alito suggested that perhaps Congress or state legislatures should balance the law enforcement interests and citizens' Constitutional protections to "enact legislation that draws reasonable distinctions based on categories of information or perhaps other variables."[252] Justice Alito also emphasized that the "legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future" about this constantly evolving technology.[253]

Legislation addressing Fourth Amendment privacy concerns in government searches of location-based technology was re-introduced in January 2015 by Congressman Jason Chaffetz (R) from Utah and Senator Ron Wyden (D) from Oregon.[254] This bi-partisan support for legislation is titled the Geo-location Privacy and Surveillance Act (GPS Act).[255] It seeks to require a consumer's express consent before location information may be revealed.[256]

---

251. *Id.* at 26.

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

253. *Id.* at 2497–98.

254. H.R. 491, 114th Cong. (2015); S. 237, 114th Cong. (2015).

255. *Id.*

256. *See id.* § 2602(d)(1) ("It shall not be unlawful under this chapter for a person to intercept geolocation information pertaining to another person if such

Notably, there are several exceptions to the consent requirement, including theft or fraud, emergency situations, and most notably, a warrant exception.[257] The GPS Act states that, "[a] governmental entity may intercept geolocation information or require the disclosure by a provider of a covered service of geo-location information only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure" or in the "or the Foreign Intelligence 12 Surveillance Act of 1978 (50 U.S.C. 1801 et seq.)"[258] The Act is structured in the same manner as the federal wiretapping statue and is intended to be applied in a similar manner.[259]

IV. Conclusion

Technology has advanced to the point where cell phone tracking can sometimes locate a phone's precise location within several feet.[260] Most consumers would probably be shocked to learn that, pursuant to the third-party doctrine, cell phone carriers can legally turn over CSLI to law enforcement without a probable cause warrant. The concept that consumers somehow voluntarily consent to the disclosure of such highly detailed personal information when they sign up for cell phone service defies the reality of modern society. Citizens' reasonable Fourth Amendment privacy expectations in the use of cell phones should be protected.

Justice Alito's concurrence in *Jones*, the Court's decision in *Riley*, and the Fourth Circuit's en banc decision in *Graham*, offer an opportunity to pursue Justice Sotomayor's suggestion that it is time to reconsider the third-party doctrine. Using *Jones* and *Riley*, the Supreme Court now has the opportunity to clarify the

---

other person has given prior consent to such interception.").

257. *See generally id.* § 2602(d)–(h) (listing the various exceptions to the requirement of disclosing information).

258. *See id.* § 2602(2) (describing the warrant requirements associated with this piece of legislation).

259. *See Geolocation Privacy Legislation*, GPS.GOV, http://www.gps.gov/policy/legislation/gps-act/ (last visited Dec. 5, 2016) (describing the legislative history and procedure for this Act) (on file with Washington & Lee Journal of Civil Rights & Social Justice).

260. Rodriguez, *supra* note 249.

confusion created by the application of outdated laws to modern technology.[261]

All the Justices' positions in *Jones* suggest that a warrant is preferable. A probable cause warrant requirement for CSLI would allow the courts to keep up with constantly evolving cell phone tracking technology. Analogous to the impact of the *Miranda* warning requirement, requiring a warrant for CSLI would remove the legal confusion in this area. Such a requirement would also assist law enforcement and ensure citizens' reasonable expectations of privacy.

The *Riley* decision is especially helpful in analyzing privacy issues that arise from the use of cell phones. *Riley*, a unanimous decision, specifically addressed what police must do before searching a cell phone seized incident to arrest.[262] The United States Supreme Court should extend its analysis in *Riley* to the government's collection of data created by the use of a cell phone. The path out of the Bog is clear: "get a warrant."[263]

261. United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (*cert granted*).

262. Riley v. California, 134 S. Ct. 2473, 2495 (2014).

263. *Id.*