UIC Law Review

Volume 50 | Issue 3 Article 5

Spring 2017

Reviving the Fourth Amendment: Reasonable Expectation of Privacy in a Cell Phone Age, 50 J. Marshall L. Rev. 555 (2017)

Marisa Kay

REVIVING THE FOURTH AMENDMENT: REASONABLE EXPECTATION OF PRIVACY IN A CELL PHONE AGE

MARISA KAY

I. INTRODUCTION

As I leave my house, I go through the same mental checklist to make sure that I have everything I need for my day: keys, wallet and, most importantly, cell phone. Cell phones have become part of our everyday lives; an extension of our bodies. Oftentimes, it seems like we cannot function without our cell phones. It feels as though a part of us is missing if we inadvertently leave our cell phone at home. However, as commonplace and helpful as a cell phone has become, can the information transmitted and obtained by this 2" x 5" object severely infringe upon our privacy rights? Can this information constitute crucial evidence of the guilt or innocence of an individual in a criminal investigation?

The need for police to obtain search warrants for prolonged searches of cell phone data is increasing in our society where everyone is so dependent on his or her cell phone.[1] Moreover, with

1. Pew Research Center reported that "64% of American adults now own a smartphone of some kind." Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RESEARCH CENTER (Apr. 1, 2015), www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/. Moreover, "15% of Americans age 18-29 are heavily dependent on a smartphone for online access." *Id.*; *see generally* Shannon L. Noder, Note, *Talking and Texting While Driving: A Look at Regulating Cell Phone Use Behind the Wheel*, 44 VAL. U.L REV. 237, 239-43 (2009) (discussing the increase in cell phone ownership and use).

this dependency on technology, it is increasingly necessary to depart from current rules. These rules are encompassed in the Third-Party Doctrine and the Stored Communications Act.[2] Under the Third-Party Doctrine, information revealed to a third party can be conveyed to the government without violating the Fourth Amendment.[3] The Stored Communications Act is a statute enacted by Congress which gives some protections to electronic information stored with third parties.[4]

Part II of this comment begins with a discussion of the development of the Fourth Amendment from its inception to the present.[5] Further, it demonstrates the tension between the Fourth Amendment and the development of technology, with a particular focus on cell phone location data.[6] Part III of this comment then discusses whether there is a Fourth Amendment violation when a police officer conducts a prolonged search of cell phone location data without a search warrant.[7] Part III of this comment also analyzes how the Third-Party Doctrine and the Stored Communication Act affect cell phone location data searches. Additionally, when addressing the reasonableness of the prolonged search of cell phone location data without a warrant, this comment looks at whether the balance of interest tips in favor of the legitimate government interests or the individual's reasonable expectation of privacy.[8] Part IV of this comment proposes that changes to the Stored Communications Act and Third-Party Doctrine can preserve an individual's reasonable expectation of privacy in accordance with the Fourth Amendment.

II. BACKGROUND

The Fourth Amendment places restraints on the government whenever the government seeks to search or seize a person or property.[9] Since its ratification in 1791, the meaning of the Fourth Amendment continues to evolve.[10] With the development of technology, the meaning of what constitutes an unreasonable search or seizure is also changing.

---

2. United States v. Miller, 425 U.S. 435, 443 (1976); 18 U.S.C. §§ 2701-2712 (2012).

3. *Miller*, 425 U.S. at 443.

4. 18 U.S.C. §§ 2701-2712 (2012).

5. U.S. CONST. amend. IV.

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

7. U.S. CONST. amend. IV.

8. Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

9. Barry Friedman and Orin Kerr, *The Fourth Amendment*, NATIONAL CONSTITUTION CENTER (May 12, 2017), https://constitutioncenter.org/interactive-constitution/amendments/amendment-iv.

10. *Id.*

A. The Development of the Fourth Amendment

The Constitutional Amendments guarantee individuals certain personal freedoms and, at the same time, place limitations on the State and Federal Government's powers.[11] The Fourth Amendment is no exception.[12] The Fourth Amendment states that

> [T]he 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 warrant 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.[13]

There are two general ways that the Fourth Amendment has been interpreted: a one clause interpretation or a two clause interpretation.[14] The majority reading follows the one clause interpretation and maintains that in order to have a reasonable search or seizure, the government needs to properly execute a warrant.[15] A warrant is properly executed when there is probable cause.[16] Alternatively, the minority reading of the Fourth Amendment follows the two clause interpretation.[17] The two clause interpretation asserts that searches and seizures have to be reasonable and if a warrant is required, it must be based upon probable cause.[18]

Regardless of the method of interpretation, after the prosecution has satisfied its burden of proof, there are several steps a defendant must establish before a court will hold that the methods

---

11. In 1787 through 1788, in order for James Madison to gain support for the ratification of the Constitution, he had to compromise with the Anti-Federalists and promise to add a Bill of Rights to the Constitution. Akhil Reed Amar, *The Bill of Rights and The Fourteenth Amendment*, 101 YALE L.J. 1193, 1202 (1992). The Anti-Federalists were adamant about the inclusion of a Bill of Rights because they sought to limit the power of the federal government and to preserve the liberty of individuals and of the States. *Id.*

12. U.S. CONST. amend. IV.

13. *Id.*

14. Silas J. Wasserstrom, *The Fourth Amendment's Two Clauses*, 26 AM. CRIM. L. REV. 1389, 1389-90 (1989). There have been many discussions as to how to interpret the overall premise of the Fourth Amendment. *Id.* In determining whether or not a search and seizure is reasonable, a court must balance "the need to search against the invasion which the search entails." New Jersey v. T.L.O., 469 U.S. 325, 337 (1985). A court must look at the context within which the search or seizure took place. *Id.* at 337.

15. Wassterstrom, *supra* note 14.

16. *Id.* Probable Cause is a "fluid concept—turning on the assessment of probabilities in a particular factual context." Illinois v. Gates, 462 U.S. 213, 232 (1983).

17. Wassterstrom, *supra* note 14.

18. *Id.* A warrant is reasonable if there is probable cause to believe that a certain item will be found in a certain location. Camara v. Mun. Ct. of S.F., 387 U.S. 523, 535 (1967). For example, it would be reasonable to look for a sixty-inch television in a closet, but it would be unreasonable to look for a sixty-inch television inside a dresser drawer. *Id.*

used by a police officer violated the Fourth Amendment and order the suppression of the evidence obtained from the search.[19] First, a defendant must show that there was, indeed, a search or a seizure.[20] Then, the defendant must show that the search or seizure was performed without any probable cause, which makes the search or seizure unreasonable.[21] Finally, the defendant must show that even if the search or seizure was unreasonable, there are no exceptions that would make a search or seizure reasonable.[22]

If a defendant proves all three of these contentions, then the evidence may be suppressed.[23] The exclusion of evidence is intended to "cure the invasion of the defendant's rights which he has already suffered."[24] The purpose of suppressing evidence obtained from an unlawful search or seizure is to deter police misconduct and encourage the police to obtain a warrant.[25] The exclusion of

19. Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 682 (2011); Mapp v. Ohio, 367 U.S. 643, 657-58 (1961) (holding that evidence obtained by an illegal search or seizure should be excluded in a criminal trial in both federal and state prosecutions).

20. U.S. CONST. amend. IV.

21. *Id.*

22. Mincey v. Arizona, 437 U.S. 385, 392 (1978)

23. The exclusionary rule is a rule which states that "evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search or seizure." U.S. v. Calandra, 414 U.S. 338, 347 (1974); In Groh v. Ramirez, 540 U.S. 551, 553, 573 (2004) (holding that since the warrant was "obviously deficient" due to the clerical error of the police officer, it is "presumptively unreasonable" and thus invalid). In *Ramirez*, the police officer relied on his own errors, and not on a neutral and unbiased Judge. *Id.* at 553, 573. The Supreme Court seeks to deter this kind of behavior and error. *Id.* Due to the high cost of excluding evidence, the exclusionary rule is one possible remedy, but it is not automatic. United States v. Leon, 468 U.S. 897, 932 (1984). The Supreme Court in *Calandra*, stated that the exclusionary rule is "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect, rather than a personal constitutional right." *Calandra*, 414 U.S. at 348. Therefore, the "courts are not subject to any direct constitutional duty to exclude illegally obtained evidence, because the question of admissibility of such evidence is not addressed by the [Fourth] Amendment." *Leon*, 468 U.S. at 932.

24. Stone v. Powell, 428 U.S. 465, 540 (1976). The exclusionary rule is a remedy to violations of the Fourth Amendment. *Mapp*, 367 U.S. at 657. The exclusionary rule states that fruits of an unconstitutional search or seizure can be inadmissible in court. *Id.* at 658.

25. The purpose of the exclusionary rule is to encourage police officers to be reasonable and deter police misconduct. *Leon*, 468 U.S. at 916. Police officers may have an incentive to be aggressive in order to make an arrest and the exclusionary rule is a remedy that seeks to prevent this misconduct from happening. *Id.* at 916-19. Moreover, a warrant acts like an insurance policy for a police officer because a police officer has the issuing Judge's determination of probable cause to fall back upon if the warrant is later deemed invalid. *Id.* at 922. The exclusionary rule is a remedy only to deter police misconduct. *Id.* at 916. It does not deter mistakes made by the issuing judge or magistrate. *Id.* This is because the issuing judge or magistrate is viewed as a neutral third party with no bias. *Id.* at 917. Therefore, even if the warrant is deemed

evidence, however, places substantial social costs on the State.[26] One such social cost is that the exclusion of evidence inhibits the truth finding process of the criminal justice system.[27] Therefore, there exists a delicate balance between these two competing interests and evidence will only be suppressed when there is a tangible benefit.[28]

This section demonstrates that throughout the years, the meaning of what constitutes a reasonable search and seizure has been continually changing.[29] The Fourth Amendment was first established to prevent a powerful government from issuing broad sweeping general warrants.[30] In particular, the Supreme Court initially interpreted the Fourth Amendment as protecting individuals from unreasonable physical intrusion upon individuals' real property.[31] Then, beginning during the time that Earl Warren became Chief Justice,[32] the Supreme Court greatly expanded the

---

unreasonable, the evidence obtained by the unreasonable warrant will still be allowed in a criminal prosecution if the warrant is issued by a judge. *Id.*

26. United States v. Payber, 447 U.S. 727, 734 (1980).

27. *Id.* at 734.

28. *Id.* The Court in *Calandra* stated, "the application of the [exclusionary] rule has been restricted to those areas where its remedial objectives are thought most efficaciously served." *Calandra*, 414 U.S. at 348; *see generally* Sarah L. Dickey, Comment, *The Anomaly of Passenger "Standing" to Suppress all Evidence Derived from Illegal Vehicle Seizures Under the Exclusionary Rule: Why the Conventional Wisdom of the Lower Courts is Wrong*, 82 MISS. L.J. 183, 188 (2013) (explaining the role of the exclusionary rule in deterring police misconduct).

29. Olmstead v. United States, 277 U.S. 438, 457, 465-66 (1928); Katz v. United States, 389 U.S. 347, 353 (1967).

30. General warrants were used by England to help enforce British mandates. Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, n. 142 (1988). ("Searches and seizures pursuant to general warrants represented the sort of unreasonable conduct prohibited by the [Fourth] amendment's first clause" because general warrants gave those executing the warrant broad power.) *Id.* at 82. This is because the warrant did not specify what locations were to be searched or what items were to be seized. *Id.*

31. *Olmstead*, 277 U.S. at 465-66. The Supreme Court noted that simply placing a listening device on a public telephone pole was not a violation of the Fourth Amendment because the government did not go onto the individual's property. *Id.* There was no trespass and therefore there was no search. *Id.* Moreover, since the thing acquired by the government were words spoken, there was nothing seized since words are intangible. *Id.* at 465. *Olmstead* is distinguishable from Silverman v. U.S., 365 U.S. 505, 510 (1961). In *Silverman*, the Supreme Court held that placing a microphone into the foundation of the Defendant's home is a physical invasion. *Id.* Therefore, it constituted a trespass because the microphone was placed on the Defendant's property. *Id.*

32. The Warren Court refers to the time period in which Justice Earl Warren served as the Chief Justice of the Supreme Court. Justice Warren served as Chief Justice from 1953 through 1969. Sumi Cho, Symposium: *Redeeming Whiteness in the Shadow of Internment: Earl Warren, Brown, and a Theory of Racial Redemption*, 40 B.C.L. REV 73, 73 (1998). This Court is oftentimes characterized by its "liberal judicial activism." *Id.*

protections afforded to criminal defendants in regards to searches and seizures.[33] For example, during this time, the Supreme Court increased the number of situations that required warrants for a valid search or seizure.[34] The Warren Court also established the idea that the Fourth Amendment, through the warrant requirement, guarantees and protects an individual's right to privacy.[35] Specifically, the Fourth Amendment "protect[s] what a person seeks to preserve as private."[36]

Following the Warren Court, the Supreme Court under Chief Justice Warren Burger began to limit the protections enjoyed by criminal defendants in favor of the government's legitimate State interest.[37] Specifically, the Supreme Court increased the

33. *Katz*, 389 U.S. at 353. In *Katz*, the Supreme Court stepped away from the concept of trespass as the only violation of the Fourth Amendment. *Id.* Justice Harlan's concurring opinion established a two-part test for determining a violation of the Fourth Amendment. *Id.* at 361. This test states that first, "a person must have a subjective expectation of privacy in the communication" and, second, "the expectation must be objectively reasonable." *Id.*; *see also* United States v. Jones, 565 U.S. 400, 407 (2012) (holding that trespass, with the intent to gain information, is still a violation of the Fourth Amendment); *see also* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (holding that an unlicensed physical intrusion upon individual's property and intent by police officers to gain information violates the Fourth Amendment). Therefore, *Katz* and *Jones* stand for the proposition that there are two ways to violate the Fourth Amendment: by a physical intrusion on an individual's property with the intent of gaining information and by impinging on a person's reasonable expectation of privacy. *Jones*, 565 U.S. at 407; *Katz*, 389 U.S. at 361.

34. The Warren Court was typically pro-defense, and this can be seen through the Court's various decisions in criminal cases. Once such example is in *Chimel v. California*, in which the Court held that without a search warrant it was unreasonable to extend the area a police officer can search to the entire house. 395 U.S. 752, 768 (1969). This is because it is unreasonable for a defendant to be able to reach a weapon that is not within his immediate reach. *Id.* Thus, since the safety of the police officer was not at risk, the search, done without a warrant, was a violation of the Fourth Amendment. *Id.*

35. Olmstead v. United States, 277 U.S. 438, 351 (1928). Although the Fourth Amendment does not specifically mention privacy, the Supreme Court has read a privacy requirement within the meaning of the Fourth Amendment. *Id.*; U.S. CONST. amend. IV.

36. *Olmstead*, 277 U.S. at 351 (stating that "[t]he Fourth Amendment preserves people, not places. What a person knowingly exposes to the public, even in his own home or office, is not subject of Fourth Amendment protection… [b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

37. The Burger Court was typically pro-state, and this can be seen through its various decisions in criminal cases. Thomas Y. Davies, *The Supreme Court Giveth and the Supreme Court Taketh Away: The Century of Fourth Amendment "Search and Seizure" Doctrine*, 100 J. CRIM. L & CRIMINOLOGY 933, 993, 997 (2010). Many exceptions to otherwise unreasonable searches and seizures were developed in order to restrict the ability to suppress evidence. *Id.* at 997-98. For example, in *United States v. Leon*, the Supreme Court held that while there was an illegal search and seizure because there was not enough evidence to constitute probable cause. 468 U.S. 897, 920 (1984). However, suppression was not an appropriate remedy because the police officer relied in good faith on the

availability of warrant exceptions so that a police officer may execute more lawful searches and seizures without a warrant.[38] As it stands now, a reasonable search or seizure generally requires an officer to obtain a warrant, unless the circumstances fall within certain, specific warrant exception.[39]

B. The Tension Between the Fourth Amendment and the Development of Technology

The meaning of the Fourth Amendment has evolved from a protection of physical property to a protection of privacy rights.[40] The rise of cell phone technology changed and will continue to change how the Fourth Amendment applies to criminal defendants.[41] This is because the protections allowed by the Fourth Amendment do not operate in the conventional manner in regards to the data stored and transmitted by a cell phone.[42] The type of data stored in cell towers by cell phone service providers involves

---

Judge's decision regarding probable cause when issuing the warrant. *Id.* The Court further decided that expanding the exclusionary rule to include these types of situations would not deter police officers from overextending their authority because police officers should rely on judicial determinations. *Id.* at 921. Thus, the Supreme Court created a good-faith exception to a warrant requirement. *Id.* at 920.

38. *See generally Criminal Law Review: Featured Contributors: The U.S. Supreme Court Gets it Right in Arizona v. Gant: Justifications for Rules Protect Constitutional Rights*, 23 ST. THOMAS L. REV. 532 (2011) (discussing different warrant exceptions). For example, the Supreme Court has held that a police officer may require an individual to step out of his or her car, thus seizing the individual, during a routine stop. Pennsylvania v. Mimms, 434 U.S. 106, 113 (1977). The Supreme Court further held that a full search of an individual incident to a lawful custodial arrest is "not only an exception to the warrant requirement of the Fourth Amendment but is also a reasonable search under that Amendment." U.S. v. Robinson, 414 U.S. 218, 235 (1973).

39. Riley v. California, 134 S. Ct. 2473, 2482 (2014). Courts encourage the use of warrants because this "ensures that the inferences to support a search are drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the competitive enterprise of ferreting out crime." *Id.* An example of a warrant exception is an emergency in which a police officer must act quickly and cannot wait for a warrant to be executed. Kentucky v. King, 563 U.S. 452, 460 (2011); *see also* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (reviewing past Supreme Court holdings regarding warrant exceptions); *see* Mincey v. Arizona, 437 U.S. 385, 392-93 (1978) (holding that "the need to protect or preserve life or avoid serious injury is justification for what would be otherwise illegal."). The Court in *Mincey* gave several other examples of situations that do not need a warrant such as "when the police come upon the scene of a homicide they may make a prompt warrantless search of the area to see if there are other victims or if a killer is still on the premise." *Id.* at 392.

40. Olmstead v. United States, 277 U.S. 438, 457 (1928); Katz v. United States, 389 U.S. 347, 353 (1967).

41. *Id.*; *Olmstead*, 177 U.S. at 457, 465-66.

42. Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C.L. REV. 1, 1-2 (2013).

information about communication, which includes the location of the user.[43] Whenever a cell phone is turned on, the cell phone "communicates" every few minutes with a nearby cell site.[44] The communication is called Cell-Site Location Information, or CSLI.[45] By identifying the cell site which is activated, the approximate location of the cell phone and its user can be ascertained at specific points in time.[46] In urban areas, with many cell towers, the location of a cell phone can be located within a range of about 200 feet.[47]

This location identification gives the government a plethora of information regarding an individual and his or her whereabouts at any given time.[48] Given the immense reliance on cell phones today, this means that the government can use this technology to gain information whenever the cell phone is turned on, which in most cases that means twenty-four-hours a day, seven-days-a-week.[49] Further, since a cell phone is likely to always be with an individual, the government can also gain information regarding the exact location of that individual.[50]

Common law dictates that when an individual voluntarily discloses information to another third party, that person loses any reasonable expectation of privacy he or she may have in that information.[51] This is because the individual is allowing others access to otherwise private information.[52] The information communicated to the third party can therefore be obtained without a warrant because there is no longer any expectation of privacy that would otherwise protect that information.[53] This concept is known

---

43. United States v. Graham, 796 F.3d. 332, 343 (4th Cir. 2015). The cell tower captures this information by identifying the cell tower with which the connection was made. *Id.*

44. *Id.*

45. Eric Lode, *Validity of Use of Cellular Telephone or Tower to Track Prospective, Real Time, or Historical Position of Possessors of Phone Under Fourth Amendment*, 92 A.L.R. FED 2D. 1, 2 (2015).

46. *Graham*, 796 F.3d at 434.

47. Lode, *supra* note 45, at 2.

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

49. *Graham*, 796 F.3d at 350; *see generally* Christopher Fox, *Checking In: Historic Cell Site Location Information and the Stored Communications Act*, 42 SETON HALL L. REV. 769, 769-70 (2012) (discussing the increased use of cell phones).

50. *Id.* at 773-75.

51. *Id.*

52. *Id.* This concept is exemplified by the case of *United States v. Miller*, 425 U.S. 443, 435 (1976). In this case, the Court held that since the Defendant voluntarily gave his records to his bank, he had no Fourth Amendment protection as to those documents. *Id.* at 443. It must further be noted that since the time that the Supreme Court decided *Miller*, Congress has enacted a statute which gives Fourth Amendment protection to bank customers. Aditi A. Prahbu, *Contracting for Financial Privacy: The Rights of Banks and Customers Under the Reauthorized Patriot Act*, 39 LOY. U. CHI. L.J. 51, 65 (2007).

53. Bedi, *supra* note 42, at 2; Katz v. United States, 389 U.S. 347, 361 (1967).

as the Third-Party Doctrine.[54] This common law principle creates an inherent problem with regards to cell phones.

The location data retrieved through the communication between a cell phone and a cell site is stored "for various lengths of time on third party servers."[55] This means that an individual, by simply using his or her cell phone, allows location information to be accessed by a third party, the cell phone service provider.[56] Therefore, since third-party service providers automatically retrieve cell phone data, individuals are deemed to have waived any privacy expectations to that information.[57] Consequently, those individuals are denied any protections, as to that information, under the Fourth Amendment.[58]

The Supreme Court first addressed the Third-Party Doctrine and technology in *Smith v. Maryland*.[59] The Court held that the individual using the telephone did not have any expectation of privacy in the numbers dialed.[60] The Court further held that such expectation of privacy would not be reasonable because that individual knew that he or she would have to give the telephone numbers to the telephone company in order to place a call.[61] Since the individual provided the telephone company with the telephone number information, that information was no longer private.[62] *Smith* and similar cases hinge on the concept of an individual's reasonable expectation of privacy.[63] Since the individual is giving information to a third party, or in the case of cell phones, allowing information to be taken by a third party, there is no reasonable expectation of privacy.[64]

The Third-Party Doctrine poses a serious problem for individuals using cell phones. Whenever a cell phone automatically pings or communicates with the cell tower, the individual has been deemed to have waived any Fourth Amendment protections as to the information stored in the cell tower.[65] In order to better deal

54. Smith v. Maryland, 442 U.S. 735 (1979); Bedi, *supra* note 42, at 2.

55. *Id.*

56. *Id.*

57. *Smith*, 442 U.S. at 735; Bedi, *supra* note 42, at 2.

58. *Smith*, 442 U.S. at 742; U.S. CONST. amend. IV.

59. Bedi, *supra* note 42, at 2; *Smith*, 442 U.S. at 735.

60. *Smith*, 442 U.S. at 742.

61. Bedi, *supra* note 42, at 13; *see also Smith*, 442 U.S. at 742 (rejecting claims that there is a reasonable expectation of privacy in numbers dialed). Smith has since been superseded by the Electronic Communications Privacy Act, a federal statute. S. Bell Tel. & Tel. Co. v. Hamm, 306 S. Ct. 70, 75 (1991).

62. *Smith*, 442 U.S. at 472.

63. *See* United States v. Chadwick, 433 U.S. 1, 13 (1977) (holding the privacy expectation in a footlocker is significantly greater than cars); *see* Katz v. United States, 389 U.S. 347, 353 (1967) (asserting individual relied on privacy of phone booth); *see* Rakas v. Illinois, 439 U.S. 128, 148 (1978) (stating cars have different expectation of privacy than houses).

64. *Smith*, 442 U.S. at 742.

65. United States v. Miller, 425 U.S. 435, 443 (1976); *see generally* Fox,

with the rise and expansion of technology, in terms of its implication on searches and seizures, Congress enacted the Stored Communications Act (SCA).[66] The Act concerns the disclosure of electronic communication and stored records held by third-party service providers.[67]

The Act gives individuals some statutory privacy rights to the stored information inevitably held by third-party service providers.[68] For example, service providers cannot voluntarily give information obtained from their customers to the government.[69] The government, however, can compel a service provider to disclose the information under a few circumstances.[70] If the information is in "electronic storage for 180 days or less, the government must obtain a search warrant" in order to obtain the information held by the service provider.[71] In order to obtain a search warrant, the government must prove that it has probable cause to perform the search.[72] If the information is in "electronic storage" for more than 180 days, the government can either issue a subpoena to the third-party service provider or request a court order to obtain the information held by the service provider.[73] By using a subpoena or a court order, the government needs only to establish "specific and articulable facts" showing a "reasonable ground to believe" that the information sought is "relevant and material."[74] In order to obtain a court order or subpoena, a lesser burden is placed upon the government to explain its need to obtain the information requested.[75] Therefore, it is significantly easier to acquire the information by subpoena or court order than it would be if the

supra note 49, at 773-75 (explaining how cell phones communicate with cell towers); U.S. CONST. amend. IV.

66. 18 U.S.C. §§ 2701-2712 (2012).

67. *Id.*

68. *Id.* The court in *United States v. Davis* stated that the Stored Communications Act provides individuals with more protection than would be the case under the Third-Party Doctrine because it requires law enforcement officers to go to court and have a Judge review the facts before a court order is issued. 785 F.3d 498, 506 (11th Cir. 2015).

69. Orin S. Kerr, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA Patriot Act: Surveillance, Law: Reshaping the Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 GEO. WASH. L. REV 1208, 1212 (2004).

70. 18 U.S.C § 2703 (2012).

71. Kerr, *supra* note 69, at 1218-19; 18 U.S.C. § 2703 (2012).

72. Shadwick v. Tampa, 407 U.S. 345, 350 (1972). Moreover, probable cause deals with the totality of the circumstances of whether there is a fair possibility that a crime was committed. *Gates*, 462 U.S. at 230. The idea of probable cause cannot be reduced into numbers or percentages. *Id.* It is a fluid concept that is dependent on the situation. *Id.*

73. Kerr, *supra* note 69, at 1218-19; 18 U.S.C. § 2703 (2012).

74. United States v. Graham, 796 F.3d. 332, 344 (4th Cir. 2015); Lode, *supra* note 45, at 2.

75. Kerr, *supra* note 69, at 1218-19; 18 U.S.C. §2703 (2012).

government was required to obtain a search warrant.[76] This means that an individual's privacy expectation can be significantly diminished when dealing with old cell phone location data.[77]

The Supreme Court finally addressed the issue of searching a cell phone incident to a lawful arrest in *Riley v. California*.[78] The Court held that a warrant is required to search a cell phone even if it is seized incident to a lawful arrest because of the "significant diminution of privacy" resulting from the search of the cell phone.[79] Precedent established that searches are constitutional incident to a lawful arrest.[80] Society places great importance not only in the safety of the arresting officer but also in the preservation of the evidence to be used in a potential criminal proceeding.[81] However, in *Riley*, the Supreme Court noted the inherent differences between other items of personal property that are found on a person and a cell phone.[82] The Court placed great emphasis on the fact that a cell phone contains a plethora of private information.[83] The Court stated that once a cell phone is secured and is outwardly inspected for any weapons, the cell phone itself, taken away from the arrestee, poses no harm to the officer.[84] Additionally, since the cell phone is no longer in the possession of the arrestee, the arrestee can no longer

---

76. *Id.*; Kerr, *supra* note 69, at 1218-19; *Graham*, 796 F.3d at 344 (requiring higher standard for obtaining warrant than obtaining court order).

77. 18 U.S.C. § 2703 (2012).

78.. Riley v. California, 134 S. Ct. 2473, 2473 (2014). In this case, the defendant was arrested on a weapons charge. *Id.* at 2480. Upon searching his person, as allowed by *United States v. Robinson*, 414 U.S. 218 (1973), the arresting officers found a cell phone on his person. *Riley*, 134 S. Ct. at 2480. Upon opening and viewing the contents of the cell phone, the officers found reference to terms associated with a street gang. *Id.* Upon further examination of the cell phone content, the officers were able to charge the defendant with a shooting that had occurred weeks earlier. *Id.*

79. *Id.* at 2493. This is the case unless there is some "exigencies of the situation [which] make the needs of law enforcement so compelling that a warrantless search is objectively reasonable." *Id.* at 2494.

80. Chimel v. California, 395 U.S. 752, 762-63 (1969).

81. The Supreme Court noted that during an arrest, the officer can be in danger because the officer has no way of knowing if the arrestee has any dangerous objects on his person that can be used against the officer unless the officer is able to search the arrestee. *Id.* Moreover, the Court noted that another exigent circumstance is the preservation of evidence because it is a possible that the individual on the premise may remove or destroy evidence. *Id.* at 773-74.

82. "Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person." *Riley*, 134 S. Ct. at 2489. For example, an arrestee may have a weapon or dangerous object on his or her person which can cause significant harm to the officer if not obtained at the time of the arrest. *Chimel*, 395 U.S. at 762-63. The Court noted that a cell phone is essentially a minicomputer. *Riley*, 134 S. Ct. at 2489. The information contained in the cell phone has no real ability to harm an officer, but can contain significant private information about the individual. *Id.* at 2489-91.

83. *Id.* at 2489.

84. *Id.* at 2486.

delete or alter the information contained on the phone, thus the evidence contained in the cell phone will be preserved.[85]

In the case of *United States v. Graham*, the Defendants were arrested for several robberies.[86] During the post-arrest investigation, the police officers investigating the matter recognized some similarities between these robberies and other earlier robberies in the area.[87] Pursuant to the SCA, the government obtained two court orders for the disclosure of the Defendants' cell site location information.[88] The court orders requested information regarding text messages and phone calls that the two Defendants sent and received from each other.[89] In accordance with the SCA, the government was able to obtain court orders for this information as opposed to a search warrant because the location information that the officers requested was in storage for more than 180 days.[90] The Fourth Circuit stated that individuals have a reasonable expectation of privacy in their location information.[91] Moreover, the Court stated that the Third-Party Doctrine was inapplicable since cell phone users do not "voluntarily convey their [cell site location information] to their service providers."[92] Thus, the government conducted a search of the Defendants' cell phone information, without a search warrant, which constituted a violation of the Fourth Amendment.[93] The cell cite location information, however, was admissible since the police officers relied in good faith on the Stored Communications Act.[94]

The Fourth Amendment generally involves physical intrusions, but as technology advances, the parameters of the Fourth Amendment should also expand to encompass electronic intrusions.[95] Currently, there is a circuit court split regarding the

85. *Id.* Even if the cell phone is in the possession of a law enforcement official, the government may be concerned about remote date wiping. *Id.* "Remote wiping occurs when a phone, connected to a wireless network, receives a signal [from a third party] that erases the date." *Id.* at 2486. Remote data wiping can also occur if a cell phone enters into or "leaves certain geographic areas." *Id.* However, remote data wiping can be easily prevented by "disconnecting a phone from the network" by either turning off the phone or by taking out the battery. *Id.* at 2487.

86. United States v. Graham, 796 F.3d. 332, 340 (4th Cir. 2015)

87. *Id.*

88. *Id.* at 341.

89. *Id.*

90. *Id.* at 343.

91. *Id.* at 345.

92. *Id.* at 356.

93. *Id.* at 344-45.

94. *Id.* at 338.

95. Riley v. California, 134 S. Ct. 4273, 2493 (2014); *see also* Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for the Probable Cause Standard*, 66 WASH & LEE L. REV. 1745, 1783-84 (2009) (stating proposition that Congress having "taken pains to protect electronically-derived location information from unwarranted disclosure serves independently to make subjectively-held expectations of

issue of the expectation of privacy in obtaining cell site location information without a warrant.[96] Some courts, such as the Third, Fifth and Eleventh Circuits have deemed such a search reasonable while others courts, such as the Fourth Circuit, have not.[97] These inconsistencies may be a result of the dissimilar rulings by the Supreme Court regarding privacy expectations as the Supreme Court tackles changing technological advancements.[98] Thus, a need for uniformity is necessary so that an individual's rights are not infringed upon depending on which state he or she resides.[99]

For a Fourth Amendment violation, the Supreme Court has repeatedly held that an individual must claim a reasonable expectation of privacy that has been impinged upon by the government.[100] Therefore, this comment addresses whether an individual has a reasonable expectation of privacy in his or her cell site location information. Additionally, this comment looks at whether an individual waives his or her expectation of privacy when a third-party service provider acquires information from the individual's cell phone.

III. ANALYSIS

As society advances technologically, the expectation of privacy within the parameters of the Fourth Amendment should also expand to encompass electronic intrusions. This section analyzes whether it is a violation of the Fourth Amendment for police officers to conduct a search of cell phone location data without a warrant.[101] Specifically, this section examines the Fourth Circuit appellate case of *United States v. Graham* and discusses whether there was a Fourth Amendment violation when a police officer conducted a search of the Defendants' cell phone location data without a search

---

privacy objectively reasonable.").

96. *Id.* at 1784-86.

97. In re United States for an Order Directing Provider of Elec. Commun. Serv. To Disclose Records to the Gov't, 620 F. 3d 304, 313 (3rd Cir. 2010) (holding cell site location information "is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination."); In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (holding court order requiring disclosure of historical cell site information is constitutional); United States v. Davis, 785 F.3d 498, 506 (11th Cir. 2015) (holding production of cell site location information did not violate Defendant's Fourth Amendment rights); *Graham*, 796 F.3d. at 332 (holding that there is a reasonable expectation of privacy in cell phone location data); *see generally* Raymond Boyce, *The Stored Communications Act: Proper Law Enforcement Tool or Instrument of Oppression?*, 118 W. VA. L. REV 919 (2015) (commenting on the circuit court split in decisions regarding cell site location information).

98. Boyce, *supra* note 97, at 930.

99. Chamberlain, *supra* note 95, at 1789.

100. Katz v. United States, 389 U.S. 347, 353 (1967)

101. *Id.*

warrant.[102] This section uses *Graham* to analyze and balance the interests between an individual's privacy rights and a government's legitimate state interest.[103]

To determine whether a violation of the Fourth Amendment occurred, this section first examines whether or not the monitoring of cell phone data constitutes a search. Second, it discusses the reasonable expectation of privacy. Third, it investigates whether a police officer seeking to examine the cell phone location date stored in a cell tower should invoke the Third-Party Doctrine. Fourth, it considers the implication of the Stored Communications Act. Fifth, it analyzes whether the balance of interest tips in favor of the legitimate government interests or the defendant's reasonable expectation of privacy in his or her cell phone location data.[104]

In *Graham*, the Defendants were charged with multiple felonies arising out of multiple robberies.[105] During the Defendant's "post-arrest investigation," the police officers executed search warrants for the Defendants' homes and pick-up truck and, among other things, found two cell phones in the pick-up truck.[106] The State, pursuant to the SCA, obtained two court orders for the disclosure of the cell site location information from Spring/Nextel "for all calls and text messages transmitted to and from both phones" for a 221 day time period.[107] The State was able to obtain this information without a search warrant because the information was in storage for more than 180 days.[108] The State used the information acquired from the cell sites to establish the locations of the Defendants at times before and after other similar robberies in the area.[109] The Defendants filed a motion to suppress the cell site location information obtained from Spring/Nextel asserting that the disclosure of the information constituted an unreasonable search since it was done without a warrant based on probable cause.[110] Thus, the Defendants asserted that the search violated their Fourth Amendment rights.[111] The Fourth Circuit held that obtaining the cell phone location information constituted an unreasonable search.[112] However, since the police officers acted with good faith

---

102. United States v. Graham, 796 F.3d 332, 340 (4th Cir. 2015); U.S. CONST. amend. IV.

103. *Graham*, 796 F.3d. at 332.

104. Terry v. Ohio, 392 U.S. 1, 27 (1968); Kathryn R. Urbonya, *Rhetorically Reasonable Police Practices: Viewing the Supreme Court's Multiple Discourse Paths*, 40 AM. CRIM. L. REV. 1387, 1394-95 (2003).

105. *Graham*, 796 F.3d. at 338.

106. *Id.* at 340.

107. *Id.* at 341-42.

108. *Id*. at 343.

109. *Id.* at 342.

110. *Id.* at 341-42.

111. *Id.*; U.S. CONST. amend. IV.

112. *Graham*, 796 F.3d at 343.

reliance on the SCA, the information was not suppressed.[113] Upon receiving this holding, the government "moved for a rehearing en banc."[114] Upon rehearing, the Fourth Circuit held "that the government's acquisition of historical CSLI from Defendants' cell phone provider did not violate the Fourth Amendment" because an individual does not enjoy Fourth Amendment protection to information turned over to a third party.[115]

A. Applicability of the Fourth Amendment

For the Fourth Amendment to be applicable, the government action must constitute either a search or a seizure.[116] A search occurs when the government impinges on an individual's reasonable expectation of privacy or when the government trespasses upon an individual's private property with the intent to gain information.[117] A seizure occurs when there is a meaningful interference with an individual's possessory interest in the property or when a "reasonable person would have believed that he was not free to leave."[118] The acquisition of cell site location information is not a seizure since it does not involve either the interference of possessory interest nor does it involve an individual.[119] Thus, this comment will solely focus on whether the government's action constituted a search. If the government action of obtaining the cell site location information constitutes a search, then a defendant

113. *Id.* Good faith is a warrant exception. United States v. Leon, 468 U.S. 897, 924 (1984). Good faith is an important concept in that the Supreme Court does not mandate that a police officer be absolutely correct in executing his or her actions in every circumstance. *Id.* Rather, good faith only mandates that an officer acts objectively reasonably with the information that is available to that officer. *Id.*

114. *Graham*, 824 F.3d at 424.

115. *Id.* at 424-25. This comment relies on the original decision by the Fourth Circuit in 2015. *Id.* at 345.

116. U.S. CONST. amend. IV. If the government action does not involve either a search or a seizure, then the Fourth Amendment does not apply, and the action can be performed as long as it does not violate any other portion of the United States Constitution. *Id.*; *see Twenty-Fifth Annual Review of Criminal Procedure: I. Investigation and Police Practices*, 84 GEO. L.J. 717, 718-19 (1996) (stating "Fourth Amendment applies only to searches and seizures that are the product of government action."); *see* Burdeau v. McDowell, 256 U.S. 465, 475 (1921) (applying Fourth Amendment protections when actions done by government actors).

117. United States v. Jones, 565 U.S. 400 (2012); Katz v. United States, 389 U.S. 347, 360 (1967).

118. United States v. Jacobsen, 466 U.S. 109, 113 (1984); United States v. Mendenhall, 446 U.S. 544, 554 (1980).

119. This government action is not a seizure because an individual is still able to use his or her cell phone without any disturbance from the government. *Jacobsen*, 466 U.S. at 113; *Mendenhall*, 446 U.S. at 554.

must show that it interferes with an individual's reasonable expectation of privacy.[120]

B. Reasonable Expectation of Privacy

"The ultimate touchstone of the Fourth Amendment is reasonableness."[121] In order to decide whether or not the search conducted by a police officer is constitutional, the question really being asked is whether the search was reasonable.[122] The default position taken by the Supreme Court is that a search is reasonable if it is conducted pursuant to a warrant.[123] However, there are exceptions in which a search can be reasonable without a warrant.[124]

---

120. This comment contends that the government action constitutes a search because an individual has a reasonable expectation of privacy that his or her every movement will not be observed by a government actor. *Katz*, 389 U.S. at 361. Moreover, this comment will focus exclusively on searches conducted by public officials and will not address any outcomes relating to a seizure.

121. Brigham City v. Stuart, 547 U.S. 398, 403 (2006).

122. *Id.*; *Katz*, 389 U.S at 361.

123. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995). If a police officer is required to have a warrant in order to search or seize an item, this limits a police officer's discretionary authority and requires the police officer to have "particularized suspicion" as to that individual or piece of property. Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 485 (1994); United States v. Carroll, 267 U.S. 132, 153-54 (1925). Thus, eliminating the fear of "arbitrary and general searches and seizures" which have been deemed "intolerable and unreasonable." Clancy, at 485. Moreover, a search pursuant to a warrant is deemed reasonable because a Judge decided whether there was probable cause to issue a warrant and a police officer can rely on a judge's decision. United States v. Leon, 468 U.S. 897, 958 (1984).

124. There are a number of exceptions in which the Court allows police officers to conduct searches and seizures without a warrant. *See generally Fourteenth Annual Review of Criminal Procedure: United States Supreme Court and Courts of Appeals 1983-84: I. Investigation and Police Practices (Part 1 of 2)*, 73 GEO. L.J. 253, 316 (1984) (explaining when exigent circumstances may lead to a warrantless search or seizure). One such warrant exception is for emergency situations. Preston v. United States. 364 U.S. 364, 367 (1964). For example, one type of emergency situation is if there is a fear of the imminent destruction of evidence. *Id.* The Supreme Court in *Preston* found that a warrantless search is justified by the need to "prevent the destruction of evidence of the crime." *Id.* Another type of exigent situation is when there is a risk of danger to the police or to the general public. Chimel v. California, 395 U.S. 752, 762-63 (1969). In the case of *Chimel*, the Court found it reasonable to conduct a full search of an individual pursuant to his or her lawful custodial arrest. *Id.* This is because the Court wants to ensure the safety of the officer when dealing with a potentially armed suspect. *Id.* In the case of *Brigham City*, the Court found it reasonable for a police officer to enter the dwelling in order to prevent physical harm to the individual who was spitting blood inside. Brigham City v. Stuart, 547 U.S. 398 (2006). The acceptable reasons to have a warrantless search and seizure have been expanding to allow for more exigent circumstances. Clancy, *supra* note 122, at 486.

Justice John Marshall Harlan noted in his concurring opinion in *Katz v. United States* that individuals have an expectation of privacy from intrusions into a place that is private.[125] An intrusion into this private sphere is unreasonable.[126] On a separate occasion, the Supreme Court also stated that "individuals have privacy rights in [their] movements, in [their] location, and in the location of [their] personal property in private spaces, particularly when such information is available only through technological means not in use by the general public."[127]

In order to analyze whether the search of cell phone location data information is reasonable, the Supreme Court would look at the uniqueness of the information gained from the search, the timeframe of the search in relation to the expectation of privacy and the location of the individual during the time period of the search.[128]

1. Uniqueness of the Information Gained

The type of information acquired by government action is essential in determining whether or not a search actually occurred and whether or not it is reasonable.[129] The more unique and intrusive the information acquired, the more this conduct resembles a search.[130] When the government accesses cell site location information, regarding a particular cell phone, the government is able to acquire information regarding the location of the cell phone and its user at different points in time.[131] Moreover, the government

125. Katz v. United States, 389 U.S. 347, 361 (1967). It is Justice Harlan's opinion that the Fourth Amendment protects people and their expectation of privacy. *Id.*

126. *Id.*

127. United States v. Graham, 796 F.3d. 332, 345 (2015) (citing a proposition held by the Supreme Court).

128. *Id.*

129. Illinois v. Caballes, 543 U.S. 405, 408-09 (2005). The Supreme Court held that given the binary character of the use of a drug sniffing dog, the action cannot be considered a search because the only thing that the government has learned from the action is whether or not the substance in the car was illegal drugs. *Id.* The government is not able to obtain any other information regarding non-contraband items from the dog's indication. *Id.* at 409. The Court further noted that the individual has no expectation of privacy in the possession of contraband and emphasized the importance of the fact that the dog sniff was performed while the individual was subject to a lawful traffic stop. *Id.* at 408-09.

130. In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 117 (E.D.N.Y 2011). This District Court noted that "read together, *Karo* and *Knotts* stand for the proposition that the Government's obtaining of some electronically collected location information constitutes a search under the Fourth Amendment depending on the location […] and quality of that information." *Id.*

131. United States v. Graham, 796 F.3d. 332, 350 (2015).

is able to ascertain how long that individual stayed at that location.[132]

In *Graham*, the records revealed 29,659 location points for one Defendant and 28,410 location points for the other Defendant.[133] This means that the government was able to ascertain over approximately 100 location points for each Defendant for each day.[134] This information can give the government a detailed picture of the movements of each Defendant.[135] In *Graham*, the police officers sought to obtain this information to ascertain whether or not the Defendants were in the vicinity of other similar robberies that took place in the area.[136] Therefore, the government sought this information to learn more than just simple non-intrusive facts.[137] Rather, the government sought this information to learn intimate and intrusive details of the whereabouts of the cell phone user and potentially charge the Defendants with other crimes.[138]

---

132. *Id.*

133. *Id.* Every time that an individual moves from place to place, the cell phone communicates with the nearest cell tower in order to establish a viable signal. Freiwald, *supra* note 19, at 702-03. While the frequency of this connection depends on the individual service provider and the situation, "it appears that [the connection is made] as frequently as every seven seconds." *Id.* While the provider does not keep every single piece of data, the service provider does keep data from when the individual uses his or her cell phone to write a text message, place a phone call or browse the internet. *Id.* Moreover, the provider "could report location information every fifteen minutes." *Id.* at 708.

134. *Graham*, 796 F.3d at 350.

135. *Id.* The information gained is more than just simply indicating whether or not an illegal item or situation exists, this information gives specific details regarding an individual's location. *Id.* at 378; *see contra* Illinois v. Caballes, 543 U.S. 405, 408-09 (2005) (holding that desire for privacy is not equivalent to expectation of privacy). The Court further explained the "expectation that certain facts will not come to the attention of the authorities is not the same as an interest in privacy that society is prepared to consider reasonable." (citing *United States. v. Jacobsen*, 466 U.S. 109, 122 (1984)). The government is able to ascertain a significant amount of information regarding a person from that person's cell phone. *Graham*, 796 F.3d at 378. While this comment does not address the Fourth Amendment protection of accessing information from the actual cell phone, it should be noted that cell phones store a plethora of information regarding a person. Riley v. California, 134 S. Ct. 4273, 2473 (2014) A cell phone can store thousands of pictures labeled with dates, a calendar, financial information, social networking pages, emails and the like. *Id.* There is great potential of the government, when accessing a cell phone, to gain intimate private details of an individual. *Id.*

136. *Graham*, 796 F.3d. at 351. The FCC Commercial Mobile Services, 47 C.F.R. § 20.18(h)(1) (2012) requires that by 2012, cell phone carriers must have the ability to locate a phone within "300 meters for 95% of calls." *Id.*

137. United States v. Jones, 656 U.S. 400, 415 (2012).

138. *Graham*, 796 F.3d at 351; *Jones*, 656 U.S. at 414. A police officer can learn more about an individual from his or her cell phone data than what can be observed from following an individual down a public street. *Riley*, 134 S. Ct. at 2473; United States v. Knotts, 460 U.S. 276, 281 (1983). Justice Sotomayor in her concurrence in *Jones* noted that the nature of GPS monitoring violations the Fourth Amendment because the quality of the information obtained

Some courts allege that the cell site location information should be treated like a business record since the cell service provider is keeping these types of records during the course of their normal business operations.[139] Yet, the information revealed from these location records provides the government with much more detail about an individual than can be obtained from some other third-party records kept during the course of normal business operations.[140] Therefore, this type of information is more unique then other types of business records.[141]

2. Timeframe of a Search

The amount of time allowed for a search is equally important when analyzing whether or not the government action meets society's reasonable expectation of privacy.[142] The Supreme Court previously stated in *United States v. Knotts* that there is no reasonable expectation of privacy in short-term monitoring of an individual conducted on public streets.[143] The Court reasoned that anyone on that public street can see the individual traveling in a particular direction or stopping at a particular destination.[144] Therefore, a search, within the meaning of the Fourth Amendment, does not occur.[145] However, the use of long term monitoring pushes the boundary of what is consistent with society's reasonable expectation of privacy.[146] In *United States v. Jones*, the Supreme

impinges on an individual's reasonable expectation of privacy. *Jones*, 656 U.S. at 414. She notes that "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual orientation." *Id.* at 407. The government in assessing this information can ascertain when an individual goes to the doctor, sees an attorney, goes to a bar, goes home, enters a church and so much more. *Id.* This is the same type of information that can be gained from cell phone location information. *Graham*, 796 F.3d at 350.

139. In Re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611-12 (5th Cir. 2013). The cell phone service provider is independently storing this location information in order to better optimize its service. United States v. Madison, No. 11-60285, 2012 U.S. Dist. LEXIS 105527, at *1 (S.D. Fla. July 30, 2012). For example, a cell phone company may use the information acquired in order to appropriately bill its customers. *Id.* If an individual's plan requires an additional charge for roaming, then the cell phone company will use location information in order to bill accordingly. *Id.*

140. Lauren E. Babst, *No More Shortcuts: Protect Cell Site Location Data With a Warrant Requirement*, 21 MICH. TELECOMM. TECH. L. REV 363, 393 (2015). The Court stated that the location of a person within his or her residence is an intimate detail about the residence; *see also* United States v. Karo, 468 U.S. 705, 715 (1984) (holding warrantless searches and seizures inside a home are "presumptively unreasonable absent exigent circumstances.").

141. Babst, *supra* note 140.

142. United States v. Knotts, 460 U.S. 276, 281-82 (1983).

143. *Id.*

144. *Id.*

145. *Id.*; U.S. CONST. amend. IV.

146. United States v. Jones, 565 U.S. 400, 429 (2012).

Court held the "installation of the GPS device" and the use of "the GPS devise to monitor the vehicle's movement" constituted a search.[147] In that case, the Defendant was under suspicion of trafficking narcotics.[148] The State obtained a search warrant which authorized the police officers to install a GPS device on the Defendant's vehicle and monitored the vehicle for twenty-eight days.[149] However, the State did not install the GPS device in compliance with the warrant.[150] Thus, the warrant was invalid.[151] The Supreme Court held that the installation of the GPS device constituted a search; and it was impermissible for the government to "physically occupy private property for the purpose of obtaining information."[152]

Justice Samuel Alito in his concurring opinion in *Jones* further suggested that society expects law enforcement officials to refrain from "secretly monitor[ing] and catalogue[ing] every single movement of an individual's car for a very long period" of time.[153] In a case like *Graham*, the amount of information that can be acquired during a long term surveillance is astonishing since a cell tower frequently acquires new location information from a cell phone.[154] Using the location information, law enforcement officials can fairly accurately track the individual throughout the day.[155] The monitoring of cell phone data is similar to the GPS monitoring in *Jones* because the law enforcement agent acquires a plethora of location information in a given time period.[156] In essence, the law enforcement agents are able to monitor every single movement of the individual.[157] This long term electronic monitoring greatly impinges on individual's reasonable expectation of privacy.[158] This is because an individual's every movement can be assessed and

147. *Id.* at 403. The Court reasoned that "the government physically occupied private property for the purpose of obtaining information." *Id.* at 404. Thus, that "physical intrusion would have been considered a search." *Id.* at 404-05. The Court does not address whether there was a reasonable expectation of privacy since it found the action to constitute a search. *Id.* at 406.

148. *Id.* at 400.

149. *Id.*

150. *Id.* at 402-03. The warrant authorized the "installation of the device in the District of Columbia and for the installation to be made within 10 days." *Id.* The GPS was installed on the 11th day and in Maryland. *Id.* at 403.

151. *Id.*

152. *Id.* Justice Sotomayor, in her concurring opinion, addressed that "a Fourth Amendment search [also] occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Id.* at 414.

153. *Id.*

154. United States v. Graham, 796 F.3d. 332, 350 (2015).

155. *Id.*

156. *Id.*; *Jones*, 565 U.S. at 469.

157. *Id.*

158. *Id.*

scrutinized more thoroughly than what could be assessed by watching an individual as he or she travels down a public street.[159]

While neither Justice Alito nor the Court in *Jones* indicated the amount of time required to pass before a police officer's warrantless monitoring of an individual moves from a reasonable observation to an unreasonable search, Justice Alito argued that in *Jones* it occurred before four weeks of monitoring.[160] In *Graham*, the search consisted of 55 weeks, or 221 days, of surveillance, well beyond the approximate four-week threshold.[161]

3. Location of the Individual While a Search is Conducted

The Supreme Court also bases its reasonableness analysis on the location of the individual being subjected to a search.[162] The government usually argues that it is not requiring the cell phone service provider to create or keep this location information.[163] Thus, the government should have access to information already independently created by cell service providers.[164] However, the problem is the inherently intrusive nature of cell site location information.[165] If allowed to access this information, the government can gain knowledge about an individual's private and public movements, including information about individuals while they are inside of their homes.[166] Details about information occurring in the home, including the location of an individual, is

159. *Id.*

160. *Id.*

161. *Graham*, 796 F.3d. at 347. This search is certainly an infringement of an individual's reasonable expectation of privacy. *Jones*, 565 U.S. at 429. However, given the wealth of information acquired from the near constant location information gained from cell towers, a search may begin significantly before four weeks of monitoring. *Graham*, 796 F.3d. at 341. Maybe even just after a day or two. *Id.* at 340. The district court in Maryland in quoting Senator Wyden stated, "tracking an individual's movements on a twenty-four-hour basis for an extended period of time […] is qualitatively different than visually observing the person during a single trip." In re U.S. ex rel. an Order Authorizing Disclosure of Location Info. Of a Specified Wireless Tel., 849 F. Supp. 2d 526, 556 (Md. 2011).

162. United States v. Knotts, 460 U.S. 276, 281-82 (1983). The Court held that since the car is traveling on a public street there is no expectation of privacy. Kyllo v. United States, 533 U.S. 27, 37 (2001). Conversely, the Supreme Court held that all details within a home are intimate details to be "held safe from prying government eyes." United States v. Karo, 468 U.S. 705, 714 (1984). The Supreme Court held that the monitoring of a beeper within a private residence violates the reasonable expectation of privacy of a residence. *Id.*

163. In Re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611-12 (5th Cir. 2013).

164. *Id.*

165. *Graham*, 796 F.3d. at 378.

166. *Id.* The cell towers are constantly gathering information regarding the user's location not only "around town, but also within a particular building including the privacy of his or her own home." *Id.*

subject to more stringent privacy standards than would be the case in other more public locations.[167] This is because the Supreme Court has read into the Fourth Amendment "special protection[s]" for an individual within his or her own home.[168]

Some courts also allege that the monitoring of the individual within the house is not directly recorded or collected by the government.[169] Therefore, these courts argue, the monitoring does not impinge on a person's reasonable expectation of privacy, since the Fourth Amendment only gives individual's protection against government actions.[170] For example, the Court in *United States v. Jacobsen* held that the expectation of privacy had already been extinguished when a private individual initially opened and looked into a package.[171] Therefore, the government was not prohibited by the Fourth Amendment from also looking into the package.[172] However, the ruling in *Jacobsen* rests on the proposition that the

---

167. Just like in *Kyllo*, details, such as how warm a house is, are intimate details of the home. *Kyllo*, 533 U.S. at 37-38. The police officer should not be given free reign into any and all details of a home regardless of how presumptively non-intimate an item within the house appears to be. *Id.*; *see* Silverman v. United States., 365 U.S. 505, 512 (1961) (stating that man has right to retreat into home without "unreasonable governmental intrusion.").

168. Welsh v. Wisconsin, 466 U.S. 740, 754 (1984). An individual expects the most privacy when she is within her own home. United States v. Karo, 468 U.S. 705, 714 (1984).

169. United States v. Davis, 785 F.3d 498, 511 (2015); United States v. Miller, 425 U.S. 435, 443 (1976); Smith v. Md., 442 U.S. 735, 742 (1979); *see generally* U.S. v. Caraballo, 963 F. Supp. 2d 341, 362 (D. Vt. 2013) (discussing Sprint/Nextel's policy of collecting "information regarding the location of its customer's cell phones while in use.").

170. The Court in *Walter v. United States* held that an action by a private individual, "not acting as an agent of the government or with the participation or knowledge of any governmental official" does not violate the Fourth Amendment even if the private individual conducts an unreasonable search or seizure. 447 U.S. 649, 662 (1980). Moreover, the court in *In Re Application of the U.S. for Historical Cell Site Data* cites and distinguishes *Smith* from *Karo*. 724 F.3d 600, 611-12 (5th Cir. 2013). This court says that while both *Smith* and *Karo* involve the "government's acquisition of information about the interior of a home: that a particular canister was located in the home or that a person was calling particular numbers for a phone in the home. But in *Karo* […], the Government was the one collecting and recording that information." *Id.* In *Smith*, the phone service provider was obtaining the records and the government just sought the information from the phone service provider. *Id.*

171. United States v. Jacobsen, 466 U.S. 109, 117-120 (1984). In this case, a FedEx employee opened a damaged package in order to examine its contents pursuant to "company policy" and found a white substance believed to be cocaine. *Id.* at 111. Upon finding this substance, the company called a federal agent who took and tested the white substance and determined it was cocaine. *Id.* Since the government agent does not learn anything that was not already learned before by the private individual, there is no "legitimate expectation of privacy." *Id.* at 120. Moreover, this does not constitute a search under the Fourth Amendment since the testing of the substance was a binary procedure. *Id.*

172. *Id.* at 117-120.

Government did not learn anything more than what was previously learned by the private individual's search of the package.[173] In a situation where the government is monitoring historical cell site location information, the government learns more than what was previously known by the private individual.[174] The cell service providers use the location information to provide better service to its customers.[175] The service providers are probably not using the information to monitor and actually track the movements of its customers from place to place in order to determine the exact whereabouts of its customers at certain points in time.[176] However, by searching the cell site location information, law enforcement officials learn unique and private facts about an individual's movements that do not advance the business interests of the cell service provider.[177] Thus, this type of monitoring furthers only the government's interests.[178]

This type of surveillance impinges on the reasonable expectation of privacy because of the prolonged and unique nature of the information obtained through historical cell site information.[179] This type of search also impinges on an individual's reasonable expectation of privacy because individuals will likely enter their residences during the timeframe of the prolonged search.[180]

C. Third-Party Doctrine

The Supreme Court is firm in its conclusion that when there is a reasonable expectation of privacy, the government cannot impinge upon this privacy right unless it has probable cause to do so.[181] However, the Supreme Court has been reluctant to expand what reasonableness means in a changing technological environment.[182]

---

173. *Id.* at 120.

174. United States v. Place, 462, U.S. 696, 707 (1983). The Court held that the type of information gained from the dog sniff is pivotal in the determination of whether it is reasonable. *Id.* Since the government was not acquiring any private facts about legal items held in the luggage, it did not impinge on any reasonable expectation of privacy. *Id.*

175. *In Re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 611-12.

176. United States v. Graham, 796 F.3d. 332, 343 (2015).

177. Susan Freiwald, *Law Enforcement Access to Third Party Records: Light in the Darkness: How the Leatpr Standards Guide Legislators in Regulating Law Enforcement Access to Cell Site Location Records*, 66 OKLA. L. REV. 875, 903 (2014).

178. *Id.*

179. Riley v. California, 134 S. Ct. 2473, 2490 (2014); *Graham*, 796 F.3d at 349.

180. *Id.*

181. Katz v. United States, 389 U.S. 347, 361 (1967).

182. Smith v. Md., 442 U.S. 735, 743-44 (1979). This ruling came out in 1979, and even so, 36 years later the Court has not significantly amended its thoughts

While there are currently a few Justices that suggest changing the meaning of reasonableness, the majority of the Court still maintains that there is no expectation of privacy "that society is prepared to recognize as reasonable" when an individual "voluntarily turns over [information] to third parties."[183] The Third-Party Doctrine states that the Fourth Amendment "does not protect a person's privacy in information she has volunteered to a third party."[184]

The Fifth Circuit has noted that, in the context of cell phone use and conveyance of information to the third-party cell phone company, the user knows and understands that his or her cell phone sends a signal to a nearby cell tower in order to connect his or her phone call.[185] While individuals may know and understand that they are turning over their electronic records to a third party, they are not voluntarily turning over these records.[186] In order to use a cell phone, the third-party service provider automatically retrieves the cell phone user's information without any sort of active or passive participation from the user.[187] Some courts argue that there

---

regarding expectations of privacy when information is given to a third party despite societies' technological advancements in those 36 years. *See generally* Evan Peters, *The Technology We Exalt Today is Everyman's Master*, 44 WASH. U. J.L. & POL'Y 103, 119-20 (2014) (illustrating flaw with technology and the Third-Party Doctrine).

183. Thomas P. Crocker, *Symposium on Cybercrime: Order, Technology, and the Constitutional Meanings of Criminal Procedure*, 103 J. CRIM. L. & CRIMINOLOGY 685, n. 4 (2013) ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable." (quoting Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. REV. 1, 60-61 (2001)).

However, it seems as though the Court may soon change its mind regarding information provided to third-party servers. For example, Justice Sotomayor in United States v. Jones, 565 U.S. 400, 417 (2012) stated that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.*

184. Elspeth A. Brotherton, Comment: *Big Brother Gets a Makeover: Behavioral Targeting and the Third-Party Doctrine*, 61 EMORY L.J. 555, 559 (2012).

185. In Re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 613 (5th Cir. 2013). The Fifth Circuit Court also suggests that even if the individual does not realize or know that their cell phone must connect to the cell tower in order to place a phone call, the individual is deemed to know this fact. *Id.* This is because in the individual's cell phone contract it states that the "provider uses a subscriber's location information to route his cell phone calls" and collects it. *Id.* Yet, the average reasonable person may not actually realize that the cell phone company can take and store this information so that it can be used by other entities, such as the government. United States v. Graham, 796 F.3d. 332, 354 (5th Cir. 2015).

186. *Id.*

187. *Id.* at 354-55. It can be argued that an individual actively participates

is no need for active participation for an action to be voluntary.[188] Since the government "does not require a member of the public to own or carry a cell phone," this makes the use of a cell phone completely voluntary.[189] By extension, this makes the conveyance of information voluntary.[190]

However, the use of a cell phone has become "essential to full cultural and economic participation."[191] The simple act of using a cell phone or carrying a cell phone cannot automatically mean that the cell phone user has voluntarily conveyed his or her location information to the cell phone provider, and thus extinguished all expectation of privacy.[192] While the government is not actually requiring an individual to purchase and use a cell phone, in order to function efficiently and effectively in society, an individual must have and use a cell phone.[193] Thus, a person "cannot be deemed to have volunteered to forfeit expectations of privacy" by simply participating in society.[194]

The Defendants in *Graham* did not voluntarily terminate their reasonable expectation of privacy in the information retrieved by the cell phone provider just because the Defendants used cell phones in their day to day lives.[195] Additionally, a government agent should not have been able to request the Defendants' cell phone location information without a warrant and probable cause just because the Defendants were required to allow the third-party cell phone service provider to retrieve information regarding their location.[196]

---

when that individual makes a phone call or sends a text message. *Id.* at 355. However, the cell phone provider also retrieves information when the cell phone user receives a phone call or test message. *Id.* The cell phone user has absolutely no control over the receipt of such calls or messages, yet the information is still conveyed to the cell phone provider. *Id.* Even so, this may be a flawed argument since the use of cell phones have become an integral part of everyday society in which individuals need the use of cell phones in order to complete all sorts of tasks during the course of the day. *Id.*

188. *In Re Application of the U.S. for Historical Cell Site Data*, 724 F.3d at 613.

189. *Id.*

190. *Id.*

191. *Graham*, 796 F.3d. at 355-56. In *Riley* the Court stated that "[c]ell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification." Riley v. California, 134 S. Ct. 2473, 2490 (2014).

192. *Graham*, 796 F.3d. at 355-56.

193. *Id.*; *Riley*, 134 U.S. at 2484.

194. *Graham*, 796 F.3d. at 356.

195. *Id*. at 340.

196. U.S. CONST. amend. IV.

D. Stored Communications Act

In 1986, Congress enacted the Stored Communications Act in order to address the changes and advancements in technology.[197] Prior to the enactment of this law, the government simply issued subpoenas to third-party service providers in order to require those entities to produce "a wide variety of business records" and other information.[198] With the passage of this law, the government is forced to take the additional step of obtaining judicial approval and obtaining a court order prior to any information being tendered to the government.[199] A court order is issued if the court finds "specific and articulable facts showing that there are reasonable grounds to believe that … the records or other information sought […] are relevant and material to an ongoing criminal investigation."[200] This standard, however, is drastically lower than a probable cause standard needed before any other warrant can be issued.[201]

Some courts have stated that individuals are afforded less rights when their information is tendered to a third party.[202] Therefore, these courts argue that the SCA actually gives individuals more protection by imposing a judicial review requirement prior to the issuance of the court order.[203] However, many other courts are unimpressed with this line of reasoning.[204] This is because the Fourth Amendment imposes a probable cause requirement upon searches.[205] The reasonable expectation of privacy is too great for certain types of electronic mediums to be bypassed by a lower standard of evidence requirement.[206] These

197. 18 U.S.C. §§ 2701-2712 (2012); United States v. Warshak, 631 F.3d 266, 335 (6th Cir. 2010) (stating purpose of Store Communications Act is to "maintain boundaries between citizen's reasonable expectation of privacy and crime prevention in light of quickly advancing technology.").

198. United States v. Davis, 785 F.3d 498, 505 (11th Cir. 2015). This court further noted that Congress required more than just a subpoena before the government can obtain telephone records from a third party. *Id.* at 506.

199. *Id*. at 505.

200. *Id*.

201. *Id.*

202. *Id.*; United States v. Miller, 425 U.S. 435, 443 (1976).

203. *Id.*; *Davis*, 785 F.3d at 505.

204. The court in *Warshak* stated that the Stored Communications Act is unconstitutional since it allows the government to obtain emails without a search warrant. *Warshak*, 490 F.3d at 288.

205. U.S. CONST. amend. IV. In a limited number of circumstances, the Supreme Court has allowed the state to perform searches and seizure with less than probable cause. For example, in Terry v. Ohio, 392 U.S. 1 (1968), the Supreme Court held that where a police officer "has reason to believe that he is dealing with and armed and dangerous individual, regardless of whether he has probable cause to arrest," he can seize the individual and search for weapons. *Id*. at 27.

206. The court in *Warshak* stated that stated that individuals have a reasonable expectation that their emails, which are stored with a commercial ISP are kept private. 490 F.3d at 473. Just like an email is a mode of private

courts would insist the Fourth Amendment requires that a law enforcement officer obtain a warrant prior to searching information provided to third parties from electronic mediums,[207] thereby protecting an individual's reasonable expectation of privacy.[208]

E. Balancing Test between Legitimate Government Interest and an Individual's Expectation of Privacy

In order to determine the constitutionality of a government action, society must balance opposing interests in order to determine whether or not the action meets with society's privacy expectations.[209] The two interests that must be balanced are the degree to which the government action is necessary to promote its own legitimate interest and the degree to which the government action intrudes upon an individual's reasonable expectation of privacy.[210]

1. Legitimate Government Interest

There are two primary government interests at play regarding searches of cell site location information.[211] The first is safety of the officer and the second is crime prevention.[212] Law enforcement officers may argue that in order to ensure their safety while on the job, it is essential that they secure a cell phone in order to ensure

---

communication, cell phones, like landline telephones before them, are equally private modes of communication. *Id.* The information that can be obtained from the search of the cell phone location data should also be protected in the same way as the communication itself. *Id.* The decision in *Warshak*, 490 F.3d 455 was later vacated by *Warshak*, 532 F.3d 266. However, in Warshak, 631 F.3d 266, the court found that since the government relied in good faith on the Stored Communication Act, the evidence obtained from the search was allowed. The court, however, still maintained that individuals have a "reasonable expectation of privacy in the contents of emails." *Id.* at 288.

207. *Warshak,* 631 F.3d at 288. The Appellate Court in *Graham* noted "if a new technology permits the government to access information that it previously could not access without a warrant, using techniques not regulated under preexisting rules that predate that technology, the effect will be that the Fourth Amendment matters less and less over time." United States v. Graham*,* 796 F.3d 332, 360 (2015).

208. *Id.*

209. Wyo. v. Houghton, 526 U.S. 295, 300 (1999).

210. *Id.*

211. United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012); *see also* United States v. Knotts, 460 U.S. 276, 284 (1983) (stating devices such as beepers facilitate police efficiency.").

212. Riley v. California, 134 S. Ct. 2473, 2486 (2014). Additionally, the Supreme Court has conceded that the government has an interest in preventing the destruction of information so that a police officer can also secure the cell phone in order to prevent the individual from deleting or altering any incriminating information on the cell phone. *Id.*

that there are no weapons on the cell phone.[213] This government interest is well accepted and is not at issue.[214]

Law enforcement officers may also argue that in order to ensure that officers are able to do their job of solving crimes in the most efficient and effective manner, officers should be allowed to use electronic aids that merely enhance sensory facilities.[215] Some courts suggest that in order to keep up with technological advancements, a police officer must also use technology to "prevent criminals from circumventing the justice system."[216] Furthermore, these courts suggests that the best way to gauge the interests that the public seek to protect is by Congress enacting legislation, such as the SCA, in order for officers to effectively balance between competing interests.[217]

2. An Individual's Reasonable Expectation of Privacy Interest

As previously discussed, individuals have a reasonable expectation of privacy in their location.[218] A police officer can acquire intimate details about an individual's private life by acquiring and tracking the individual's precise whereabouts.[219] The government infringes upon this Fourth Amendment protection if the search is done without probable cause and a warrant.[220]

---

213. The Supreme Court has accepted as true the proposition that a cell phone can be secured in order to ensure that there are no weapons on the cell phone, like a razor blade hidden in the cell phone case. *Id.* at 2486.

214. *Id.*

215. *Knotts*, 460 U.S. at 282. The law enforcement official can argue that since he can obtain the same type of information from the cell site information that he could have obtained through visual surveillance, the officer should be allowed to use the more efficient method in order to advance the government interest of keeping fellow officers safe and solving crimes. Skinner, 690 F.3d at 778; *see also* United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (holding DEA agents can call cell phone to "ping" suspect's location information to find suspect on public road).

216. *Knotts*, 460 U.S. at 284. For example, there are features on modern cell phones which allows cell phone to erase data or automatically lock in order to prevent others from accessing information. *Riley*, 134 S. Ct. at 2486. However, this particular threat of destruction of evidence can be eliminated by removing the battery from the cell phone or taking the phone off the network. *Id.* at 2486-87.

217. United States v. Jones, 565 U.S. 400, 429 (2012) (Alito, J., concurring). Since Congress, as representatives of the people, believed that the Stored Communications Acts provides the best protection for the people while still allowing police to solve crimes, then these protections should be deemed reasonable. *Id.*

218. *Graham*, 796 F.3d 332, 351 (2015).

219. *Jones*, 565 U.S. at 414.

220. *Id.*; U.S. CONST. amend. IV.

3. Balancing of Interests

Some courts argue that the mere desire to keep cell site location information private does not equate to a reasonable expectation of privacy.[221] These courts reason that the desire for these circumstances to remain private does not alone mean that there is a reasonable expectation of privacy in these circumstances.[222] However, desire for privacy alone does not drive the analysis of a reasonable expectation of privacy.[223] In *Graham*, law enforcement officials gained a plethora of private information from cell site location information.[224] Thus, the conduct of the law enforcement officers began to closely resemble an unlawful search using an attached GPS device when completed without a warrant and without probable cause.[225] What is more, these types of searches begin to look more like general searches, conducted in colonial times, because law enforcement officials can indiscriminately search vast amounts of information over an extensive period of time.[226] The expectation of privacy in the location of the individual along with the quality and quantity of information gained makes the expectation of privacy reasonable.

---

221. *In Re Application of the U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (2013). For example, some individuals may want the contents of their trash bags to be kept private. California v. Greenwood, 486 U.S. 35, 40-41 (1988). Some individuals may want their property to be protected from law enforcement officials flying overhead. Florida v. Riley, 488 U.S. 445, 451 (1989). Just because these individuals want these things to be private, does not mean that they are private under the meaning of the Fourth Amendment. United States v. Jacobsen, 466 U.S. 109, 122 (1984).

222. *Id.* The Supreme Court stated that "the concept of an interest in privacy that society is prepared to recognize as reasonable is […] critically different from the mere expectation, however well justified." *Id.*

223. Katz v. United States, 389 U.S. 347, 361 (1967). Not only must the individual have "an actual (subjective) expectation of privacy" but also, there must be an expectation of privacy "that society is prepared to recognize as reasonable." *Id.*

224. Having access to cell site location information is just like having access to GPS information. *Jones*, 565 U.S. at 400. The Court in *Jones* held that a GPS device which monitors "vehicle's movements constitutes a search under the Fourth Amendment." *Id.*

225. *Id*.

226. In Re U.S. ex rel. an Order Authorizing Disclosure of Location Information of a Specified Wireless Tel., 849 F. Supp. 2d 526, 551 (Md. 2011). These types of searches begin to look more like general warrant searches because the search "informs the government on an almost continuous basis where the subject is, at places where the government lacked probable cause to believe he was, and with the persons about whom the government may have no knowledge." *Id.* The intrusion upon the individual's everyday life is enormous. *Id.* The reason why the Fourth Amendment was implemented was to ensure that this type of search was impermissible. Clancy, *supra* note 122. However, it seems as though the Fourth Amendment has lost its strength and these types of searches are again being allowed. United States v. Graham, 796 F. 3d. 332 (2015)

These types of broad searches, without warrants, are precisely what the Fourth Amendment sought to prevent against.[227] Without abiding by the protections afforded by the Fourth Amendment, individuals would not enjoy any privacy expectations.

While the government has a legitimate interest that it seeks to preserve, it seems as though the balance of interest tips in favor of the individual's reasonable expectation of privacy in matters relating to cell phone location information.[228]

IV. PROPOSAL

In a time when nearly all individuals have a cell phone on their person at all times, the ramifications of allowing law enforcement officials to acquire cell site location information without a search warrant are enormous.[229] In order to prevent law enforcement officers from weakening the protections afforded to individuals by the Fourth Amendment, this section proposes a uniform system that dictates how law enforcement officials are to treat cell site location information.[230] The retrieval of cell site location information should always be treated as a search that must conform to the safeguards of the Fourth Amendment.[231] Therefore, adherence to the Fourth Amendment can be accomplished by revising the SCA to exclude the court order requirement and eliminating the Third-Party Doctrine from cell site location information search situations.

Currently, pursuant to the SCA, if cell site location information is stored by the cell service provider for less than 180 days, in accordance with the Fourth Amendment, law enforcement officers must obtain a search warrant in order to retrieve the location information.[232] If the cell site location information is stored by the cell service provider for more than 180 days, then law enforcement officers can obtain the information with just a court order.[233] As it stands, the SCA allows different methods of obtaining the same cell

227. Clancy, *supra* note 123.

228. *Id.* at 343.

229. Law enforcement officers can, with only a court order, obtain information about an individual's whereabouts and track where that individual was minute by minute at certain points in the past. 18 U.S.C. §§ 2701-2712 (2012); *Graham*, 796 F.3d. at 341.

230. If law enforcement officers are able to obtain old cell site location information without a warrant, the law enforcement officer can still perform a search, within the meaning intended by the Fourth Amendment, while circumventing the protections afforded to individuals by the Fourth Amendment. U.S. CONST. amend. IV. If law enforcement officers are able to do this, this weakens the Fourth Amendment and leaves it meaningless in relation to advancements in technology. United States v. Warshak, 631 F.3d 266 360 (2010).

231. U.S. CONST. amend. IV.

232. 18 U.S.C. §§ 2701-2712 (2012).

233. *Id.*

site location information.[234] These different methods solely depend on the length of time that the cell site location information is held by the cell service provider.[235]

Additionally, the standard of proof for obtaining a court order is significantly less than the standard of proof for obtaining a search warrant.[236] While both methods require that the law enforcement officer go to court and plead the matter in front of a Judge, it is significantly easier to obtain a court order and retrieve location information from cell phone service providers than it is to obtain a search warrant.[237] Therefore, the government's ability to easily obtain information from the cell phone service provider in certain situations is problematic.[238]

Acquiring cell site location information solely with the use of a court order is a violation of the Fourth Amendment.[239] In order to acquire cell site location information, a law enforcement officer should have to demonstrate to the court that there is probable cause to perform the search and a search warrant must be issued by a court.[240] It is not enough for a judge to review the evidence to ascertain whether or not it is relevant and material.[241] This standard of proof is too low to protect an individual's reasonable expectation of privacy.[242] The Fourth Amendment requires more protection for an individual's reasonable expectation of privacy.[243] In order to protect all individuals' privacy rights within a society, law enforcement officers should be required to have enough evidence to satisfy the probable cause standard of proof.[244]

---

234. *Id.*

235. *Id.*

236. *Id.* The standard of proof for obtaining a Court Order is "specific and articulable facts" which show a "reasonable ground to believe" that the information is "relevant and material." United States v. Graham, 796 F.3d. 332 344 (2015). The standard of proof for obtaining a warrant is probable cause. *Id.* It requires much more evidence to obtain a warrant than to obtain a court order because it requires more evidence to prove that there is probable cause than that the information is relevant and material. *Id.*

237. Allowing a court order in some situations and a warrant in other situations leads to situations wherein law enforcement officers are left with complete discretion as to the request in order to bypass the more stringent burden of proof. *Id.* at 341. In the case of *Graham*, law enforcement officers only requested data that was over 180 days old. *Id.* Therefore, the law enforcement officers only needed to obtain a court order, which requires a lower standard of proof. *Id.*

238. *Id.* at 341, 344.

239. *Id.* The Fourth Amendment protects "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 warrant shall issue, but upon probable cause." *Id.*

240. *Id.*

241. *Id.* at 344.

242. U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 361 (1967).

243. U.S. CONST. amend. IV.

244. *Id.*; *Graham*, 796 F.3d at 344.

When examining the balance of interest between an individual's privacy interest and the government's public safety interest, the balance tips in favor of the individual for three reasons.[245] First, there is a reasonable expectation of privacy regarding an individual's location information obtained from cell sites, regardless of how long that information was held in storage.[246] An individual's expectation of privacy of an individual does not magically diminish just because the information is held in storage for more than 180 days. Second, there is no real reason why there is a different standard of proof between information stored for more or less than 180 days when the only difference in the information obtained is the amount of time that location information sat in storage.[247] There is no difference in the type of information acquired.[248] It is unreasonable to allow law enforcement officers to infringe upon an individual's reasonable expectation of privacy without giving that individual the protections granted by a properly executed warrant.[249] Third, the government does have a legitimate interest in protecting the public and ensuring that law enforcement officers efficiently prevent crime.[250] However, this valued goal does not become devalued just because law enforcement officers would have to obtain more evidence to acquire a warrant in order to search the cell site location information.[251] The goals of the government and an individual's reasonable expectation of privacy are not

245. *Id.* at 351.

246. Location information, obtained from cell towers, provides law enforcement officers with unique information about an individual. *Graham*, 796 F.3d. at 350. It allows law enforcement officers to know exactly where that individual was at a certain point in time and how long that individual stayed there. *Id.* This is especially troublesome because having this type of information means that law enforcement officers are able to learn intimate details about a person simply by knowing the location of the individual. *Id.* Law enforcement officers are able to ascertain when an individual goes home, goes to the store, goes to a religious center and so on. *Id.*

247. The content of "old" location information does not become less private by simply being in storage for a longer period of time. *Graham*, 796 F.3d. at 350; Katz v. United States, 389 U.S. 347, 361 (1967). The information that can be obtained from this information still violates an individual's reasonable expectation of privacy because the information contained in the location data still pertains to the individual's private life. *Graham*, 796 F.3d at 350; *Katz*, 389 U.S. at 361. Law enforcement officers are able to ascertain where the individual was at a certain time and for how long that individual was at that location, including activities performed within the home. *Graham*, 796 F.3d at 350.

248. *Id.*

249. Wasserstrom, *supra* note 14; U.S. CONST. amend. IV.

250. Riley v. California, 134 S. Ct. 2473, 2488 (2014)

251. Requiring a warrant does not make police work harder. *Graham*, 796 F.3d. at 344. A law enforcement officer would only need to acquire more evidence before infringing on an individual's reasonable expectation of privacy. *Id.*; U.S. CONST. amend. IV. A law enforcement officer would only be required to abide by the rules set forth in the Constitution. U.S. CONST. amend. IV.

mutually exclusive and both can be upheld by simply abiding by the Fourth Amendment.[252]

Therefore, this comment proposes that the SCA be revised in order to conform to the Fourth Amendment.[253] The SCA should be revised to expand the privacy rights to all stored information held by third-party service providers. The SCA should not make a distinction between older and newer stored information. Instead, the Act should simply state that a search warrant is required in order to obtain any electronic information stored by the cell phone service provider. This way, the individuals' reasonable expectation of privacy is protected. In accordance with the Fourth Amendment, law enforcement officials should only obtain cell site location information, or any other type of electronic information, through a showing of probable cause and obtaining a warrant.[254]

Furthermore, the application of the Third-Party Doctrine should be excluded from situations involving cell site location information.[255] The Third-Party Doctrine should only be applied in situations when the individual has voluntarily provided information to a third party.[256] This was not the case in *Graham* and is oftentimes not the case with cell site location information, which is automatically obtained by cell phone providers.[257] Individuals have no choice but to allow cell phone providers to obtain their location information in order for the individual to use his or her cell phone.[258] An individual does not voluntarily give the information to the cell phone service provider by simply using a cell phone or signing the cell phone contract.[259] In order for the reasonable expectation of privacy to be waived, there needs to be more affirmative steps on the part of the individual to satisfy the voluntariness requirement of the Third-Party Doctrine.[260] Therefore, the Third-Party Doctrine should not apply when a cell phone service provider automatically obtains the cell site location information. Consequently, there would remain a reasonable

252. *Id.*

253. *Id.*

254. *Id.*

255. The Third-Party Doctrine should be excluded as referenced in the Stored Communications Act, but also as it applies in other situations regarding electronic data automatically obtained by a third-party service provider.

256. *Graham*, 796 F.3d at 340.

257. In Re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 611-12 (5th Cir. 2013).

258. A cell phone automatically pings to the nearest cell tower every few minutes in order to better the service provided to its customers. *Id.* If an individual wants to use their phone, then the individual absolutely has to give the cell phone provider access to this important information. *Id.* The individual has no voluntary choice in the matter. *Id.*

259. Not having a cell phone is realistically no longer an option for individuals. *Graham*, 796 F.3d. at 355. Cell phones are an integral part of individuals' everyday lives. *Id.*

260. *Id.* at 355-56.

expectation of privacy in information obtained by the cell phone service provider. Hence, law enforcement officials would still need a search warrant in order to obtain cell site location information from cell phone service providers.

The SCA should require warrants in all cases involving electronic information and the Third-Party Doctrine should be eliminated in situations involving cell site location information in order to preserve the meaning of the Fourth Amendment and ensure an individual's reasonable expectation of privacy in his or her cell phone location data.

V. CONCLUSION

Without a warrant, the search of cell site location information violates an individual's Fourth Amendment right to be free from an unreasonable search. While there are times when a search of the cell site location information is essential to the preservation of justice, such justice cannot be achieved if essential individual rights are regularly thwarted without any reason. Therefore, in order to deter potential police misconduct and preserve the integrity of the criminal justice system, the SCA should be revised so that it requires a search warrant to be issued prior to any search of cell site location information. Furthermore, the principles of the Third-Party Doctrine should be excluded from discussions of cell site location information because individuals do not voluntarily convey their personal information to a third party. Thus, these individuals still have a reasonable expectation of privacy in their location.

This comment suggests that these two proposals will help revive the true meaning of the Fourth Amendment and ensure that individuals can reaffirm their reasonable expectation of privacy in the age of cell phones.