# NO WARRANTS SHALL ISSUE BUT UPON PROBABLE CAUSE: THE IMPACT OF THE STORED COMMUNICATIONS ACT ON PRIVACY EXPECTATIONS

ERIK E. HAWKINS†

## I. INTRODUCTION

The Fourth Amendment to the United States Constitution protects the people's right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1] Further, it provides that "no Warrants shall issue, but upon *probable cause*, supported by Oath or affirmation."[2] This comment addresses the impact of the Stored Communications Act ("SCA") on the Fourth Amendment and how, over time, it will continue to negatively impact the constitutional protection we now enjoy. Because the Fourth Amendment provides protection from unreasonable searches unsupported by a warrant based on probable cause,[3] and because the SCA permits government procurement of personal information based on "specific and articulable facts"[4]—a lower standard than probable cause—this comment addresses the inappropriateness of the SCA's low standard in an age of burgeoning technology. In particular, I will address how permitting disclosure under the SCA's low threshold in a society pervaded by laptops and cell phones will eviscerate the "reasonableness" of privacy expectations under the Supreme Court's traditional Fourth Amendment analysis.[5] Finally, I will recommend that courts adopt an exception to the third-party

† Erik Hawkins is a third-year law student at Wake Forest University. Erik is grateful to his wife, Jill, as well as his daughter, Neve, and mother, Edith, for their constant encouragement and support.

1. U.S. CONST. amend. IV.
2. *Id.* (emphasis added).
3. *Id.*
4. 18 U.S.C. § 2703 (2006).
5. *See* Katz v. United States, 389 U.S. 347 (1967).

doctrine to address the privacy concerns attached to modern technology.

## II. THE FOURTH AMENDMENT

The Framers adopted the Fourth Amendment to the United States Constitution to protect the citizens of our fledgling republic from two instruments of "censorship and tyranny" formerly wielded by the British: writs of assistance and general warrants.[6] Both devices were employed by British authorities to search whatever and whomever they chose with unbridled discretion.[7] Abuse was commonplace.[8] And only after the general warrant was destroyed in England[9] was the seed for the Fourth Amendment planted in the United States.[10] Yet, while history informs us that the amendment was enacted to combat the tyranny of writs of assistance and general warrants,[11] surprisingly, the Fourth Amendment's legislative history "divulges little about [its] intended scope" and even less about the emergence and evolution of its corollary—the exclusionary rule.[12]

### *A. The Exclusionary Rule*

Under the exclusionary rule, evidence obtained in violation of the Fourth Amendment is not admissible in a subsequent trial.[13] Significantly, the Fourth Amendment itself is silent on the exclusion of illegally obtained evidence.[14] What is more, none of the cases responsible for the creation of the

6. Justice Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1369, 1371 (1983).

7. *Id.* at 1370.

8. *Id.* at 1369–70.

9. Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (K.B.); 3 Geo 3.

10. Controversy arose upon the death of George II in 1760 when customs inspectors requested new writs despite colonial opposition. James Otis took up the case on behalf of Bostonians who stood vehemently opposed to the issuance of any further writs. Otis lost, but after listening from the back of the courtroom, John Adams professed: "Every man of a crowded audience appeared to me to go away, as I did, ready to take arms against writs of Assistance." Stewart, *supra* note 6, at 1370–71. Eventually, in 1789, the Fourth Amendment emerged. *Id.*

11. *Id.* at 1371.

12. *Id.*

13. Herring v. United States, 555 U.S. 135, 139 (2009).

14. U.S. CONST. amend. IV.

exclusionary rule involved requests that evidence be excluded or that such a rule be created.[15] Yet, in 1914, the exclusionary rule emerged.[16]

Despite the rule's hazy boundaries, courts applying it must decide in each case whether evidence should be excluded to protect a defendant alleged to have broken the law.[17] Now, modern courts must undertake the additional task of analyzing the impact of new and constantly evolving technology on an amendment drafted over 220 years ago.[18] Indeed, emerging technology has transformed the field of law enforcement and the manner in which courts must balance the rights of defendants with those of the government.[19] Unfortunately for defendants, this former bastion of liberty has been reduced to a narrow evidentiary rule[20] primarily "relegated to the obscurity of dissents, footnotes, and law review articles."[21] Simply put, the exclusionary rule is now considered a "massive remedy," the expansion of which the current Supreme Court considers an impediment to the "truth-seeking mission of the jury trial."[22] Even blatant violations of the Fourth Amendment are excused if an offending officer can demonstrate that his actions were undertaken in "good faith."[23]

15. *See* Weeks v. United States, 232 U.S. 383 (1914); Adams v. New York, 192 U.S. 585 (1904); Boyd v. United States, 116 U.S. 616 (1886).

16. *Weeks*, 232 U.S. at 394.

17. C. Maureen Stinger, Case Note, Arizona v. Evans*: Adapting the Exclusionary Rule to Advancing Computer Technology*, 2 RICH. J.L. & TECH. 4 (1996).

18. Alex R. Hess, Herring v. United States*: Are Errors in Government Databases Preventing Defendants from Receiving Fair Trials?*, 11 J. HIGH TECH. L. 129, 129 (2010).

19. *Id.*

20. *Compare Weeks*, 232 U.S. at 393 (holding that if evidence seized in violation of the Fourth Amendment can be used "against a citizen accused of an offense, the protection of the 4th Amendment . . . is of no value"), *with* Messerschmidt v. Millender, 132 S. Ct. 1235, 1239, 1245 (2012) (explaining that the exclusionary rule is a "narrow exception" and the "threshold for [exclusion] is a high one, and it should be").

21. Scott E. Sundby & Lucy B. Ricca, *The Majestic and the Mundane: The Two Creation Stories of the Exclusionary Rule*, 43 TEX. TECH L. REV. 391, 394 (2010).

22. *Id.* at 393.

23. United States v. Leon, 468 U.S. 897, 919–20 (1984) (citation omitted) (establishing the good faith exception to the exclusionary rule).

### *B. The "Good Faith" Exception to the Exclusionary Rule*

Justice Cardozo once famously explained that "[t]he criminal is to go free because the constable has blundered."[24] Six decades later, the Supreme Court found a reason to pardon the blundering constable—his "reasonable" belief that his actions were lawful.[25] With that, the "good faith exception" to the exclusionary rule was born.[26] The reasoning behind the exception is that the suppression of evidence wrongfully obtained, in light of an officer's good faith, would produce little benefit considering the significant cost of exclusion.[27] Put differently, suppression of evidence will not deter police misconduct where an officer has obtained a search warrant and has acted in good faith within its scope. When applied, the exclusionary rule "almost always harm[s]" the prosecution's case against the accused.[28] When the rule is not applied, or when the good faith exception is relied upon, police may not be effectively deterred from violating the constitutional rights of defendants. Proper application of the rule is made more challenging when law enforcement appears to have acted in error, rather than in deliberate violation of the defendant's constitutional rights.[29] While effective application may have been straightforward in 1914 when the exclusionary rule was articulated,[30] and in 1984 when the good faith exception emerged,[31] modern courts must grapple with the application of a rule and an exception fashioned long before the advent of low-cost smartphones.

### *C.* Katz v. United States*: Ascertaining Reasonableness*

The standard for evaluating when a Fourth Amendment "search" has occurred by use of electronic surveillance was set forth in *Katz v. United States*.[32] In his concurring opinion, Justice

24. People v. Defore, 150 N.E. 585, 587 (N.Y. 1926), *abrogated by* Linkletter v. Walker, 381 U.S. 618 (1965).

25. *Leon*, 468 U.S. at 919–20.

26. *Id.* at 920 n.20.

27. *Id.* at 918–19.

28. Stinger, *supra* note 17, at 2.

29. *Id.* at 7.

30. Weeks v. United States, 232 U.S. 383, 398 (1914).

31. *Leon*, 468 U.S. at 919–20.

32. Katz v. United States, 389 U.S. 347, 359 (1967).

Harlan articulated two requirements.[33] First, the accused must "have exhibited an actual (subjective) expectation of privacy."[34] Second, the expectation must "be one that society is prepared to recognize as 'reasonable.'"[35] Put simply, under *Katz*, a potentially illegal search occurs when a defendant's "reasonable" expectations of privacy are violated.[36] Although reasonableness is analyzed in reference to concepts of property law and to "understandings that are recognized and permitted by society,"[37] precisely what makes an expectation of privacy "reasonable" has never been clearly articulated.[38] Thus, despite being the standard for over four decades, *Katz* is not without its vulnerabilities.

Situations can be contemplated in which this two-step analysis fails as an accurate barometer of Fourth Amendment protection.[39] For instance, "if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," individuals would no longer have any "expectation [of] privacy regarding their homes, papers, and effects."[40] Or what if "a refugee from a totalitarian country," oblivious to United States traditions, understandably but erroneously assumed that the government was monitoring his every move?[41] Fortunately, historic cell-site tracking affords a real-life opportunity to explore these vulnerabilities.

## III. THE IMPACT OF THE STORED COMMUNICATIONS ACT ON THE REASONABLENESS OF PRIVACY EXPECTATIONS

Every few seconds one's cell phone transmits information to a local cell tower signaling the user's location.[42] These "pings"

33. *Id.* at 361 (Harlan, J., concurring).

34. *Id.*

35. *Id.*

36. *Id.*

37. Rakas v. Illinois, 439 U.S. 128, 144 n.12 (1978).

38. O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("We have no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable.").

39. Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979).

40. *Id.*

41. *Id.*

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

help determine which towers to route "incoming and outgoing calls [to] in order to ensure [ample] reception."[43] During calls—whether outgoing or incoming—the user's location is transported to these towers.[44] Accordingly, this signal location information can assist law enforcement officers in tracking a cell phone and its owner's location with surprising accuracy. In certain locations, it is capable of tracking a person within a specific building or even within rooms therein.[45] In this sense, modern cell phones provide law enforcement with a glimpse into an area traditionally entitled to the highest protection from warrantless intrusion—the home.[46] What is more, user location data is being transmitted from almost ninety percent of our country's homes and offices, every hour of every day.[47] Each transmission "generate[s] network-based location information, much of it as precise as GPS data."[48] In fact, even if no calls or texts are made, an "automatic registration process" will likely inform local cell towers of a phone's location.[49] As a result, "cellular service providers have records of the geographic location of almost every American at almost every time of day and night."[50] Herein lies the danger. Under the SCA, these records can be obtained without a warrant based on probable cause.[51]

The SCA addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by third-party Internet Service Providers ("ISPs").[52] Under § 2703 of the SCA, the government may obtain a court order requiring these service providers to disclose customer information if the government "offers *specific and articulable facts*

43. *Id.*

44. *Id.*

45. *Id.*

46. *See, e.g.*, Silverman v. United States, 365 U.S. 505, 511 (1961).

47. *See, e.g.*, Susan Spencer, *Texting: Can we pull the plug on our obsession?*, CBS NEWS (Sept. 30, 2012, 9:16 AM), http://www.cbsnews.com/8301-3445_162-57523072/texting-can-we-pull-the-plug-on-our-obsession.

48. *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 836 (S.D. Tex. 2010), *vacated*, No. 11-20884, 2013 WL 3914484 (5th Cir. July 30, 2013).

49. *Id.* at 836.

50. *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011).

51. Stored Communications Act (SCA), 18 U.S.C. §§ 2701–2712 (2006 & Supp. IV 2011).

52. SCA § 2701.

showing that there are reasonable grounds to believe that [the information sought] is relevant and material to an ongoing criminal investigation."[53] This location-based data is precisely the type of information that enjoys Fourth Amendment protection under *United States v. Karo*.[54] Yet, unlike the Fourth Amendment, the SCA does not require "a warrant based on probable cause."[55] Indeed, the SCA enables the government to track an individual's movements without meeting this critical standard embodied in the Fourth Amendment.[56] Under the SCA, without obtaining a warrant based on probable cause, the police can study the pages of our digital diaries to ascertain extremely personal information such as our "political and religious beliefs, sexual habits, and so on."[57] In the end, the SCA gives police officers and prosecutors a powerful tool, but leaves personal privacy twisting in the wind. *United States v. Graham*[58] is a case in point.

### *A.* United States v. Graham *and the Destruction of Reasonable Privacy Expectations*

During an ongoing investigation into a litany of robberies in and around Baltimore, Maryland, police arrested and charged Aaron Graham and Eric Jordan with firearm violations.[59] Then, the government applied for an order pursuant to the SCA.[60] The magistrate granted the order after concluding that the government presented "specific and articulable facts" which demonstrated reasonable grounds "to believe that the records . . . sought [were] relevant and material to [the officers'] ongoing . . . investigation."[61] Sprint/Nextel was then directed to disclose to the government historical cell site data on Graham and Jordan.[62] Both men were subsequently indicted.[63]

53. SCA § 2703(d) (emphasis added).

54. United States v. Karo, 468 U.S. 705, 714 (1984), *reh'g denied*, 468 U.S. 1250 (1984).

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

56. *See* SCA § 2703(d).

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

58. United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012).

59. *Id.* at 386.

60. *Id.*

61. *Id.*

62. *Id.*

63. *Id.*

In their motion to suppress the cell site location data obtained from Sprint/Nextel, Graham and Jordan argued that the "twenty-four hour 'dragnet' surveillance" made possible by this emerging technology infringed their Fourth Amendment right to be free from unreasonable searches and seizures.[64] Specifically, the defendants argued that the "privacy intrusions" available through historical cell site data "are far reaching and unconstitutional" insofar as they allow the government to surveil a suspect through his cell phone.[65] The question of first impression for the Maryland District Court was "whether a defendant's Fourth Amendment rights are violated when the government acquires historical cell site location data without a warrant based on probable cause."[66]

The *Graham* court took note of the decisions handed down by the Eastern District of New York and the Southern District of Texas, both of which held that an application seeking cell site location data must be supported by probable cause and not the "specific and articulable facts" standard found in the SCA.[67] The *Graham* District Court was not persuaded. *Graham* held that the SCA's "specific and articulable facts" standard, despite its potential Orwellian consequences,[68] is consistent with the "third-party doctrine"[69] under which information disclosed to third parties receives no Fourth Amendment protection.[70] Under the third-party doctrine, courts have held that the Fourth Amendment does not restrict police in their efforts to browse one's financial records;[71] phone, e-mail, and internet records;[72] or garbage left at one's curb for pick up.[73] Under the third-party doctrine, any

64. *Id.* at 386–87.

65. *Id.*

66. *Id.* at 388.

67. *Id.* (discussing *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113 (E.D.N.Y. 2011); *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *vacated*, No. 11-20884, 2013 WL 3914484 (5th Cir. July 30, 2013)).

68. *Id.* at 389.

69. *Id.*

70. *Id.* at 389–90.

71. United States v. Miller, 425 U.S. 435 (1976).

72. United States v. Forrester, 512 F.3d 500, 509–12 (9th Cir. 2008) (holding that a computer user has no legitimate expectation of privacy in the to-from addresses of email messages sent from, and the internet protocol addresses visited by, a defendant on his home computer because they are conveyed to his service provider).

73. California v. Greenwood, 486 U.S. 35, 37 (1988).

expectation of privacy over such items is futile to prevent a government search.[74] Accordingly, when the *Graham* court applied the *Katz* test, it found that because the defendants "voluntarily" turned their cell phone data over to third parties, they "had no legitimate expectation of privacy."[75] Specifically, *Graham* found the Supreme Court's application of the third-party doctrine to dialed telephone numbers "particularly instructive."[76] Yet, *Graham* erroneously relied on cases decided in the 1960s and 1970s—well before cell phones were commercially available, let alone inexpensive and pervasive.[77]

*Graham* concluded that historic cell site data records are the "business records" of a third-party service provider.[78] In so reasoning, the court relied on *United States v. Miller*, a case which applied the third-party doctrine to the government seizure of a bank's "business records."[79] Yet, the business records seized in *Miller* were bank records preserved in microfilm—a tangible medium for document preservation first introduced in the mid-nineteenth century.[80] This analogy is tenuous at best. Unlike the cell site data obtained in *Graham*, the "business records" in *Miller* were "voluntarily" turned over.[81] Depositing and cashing checks, filling out loan applications, and signing up for credit cards are all voluntary acts.[82] By contrast, the automatic pings emanating from cell phones to cell towers are not voluntary. Further, phone calls and text messages provide the user with no indication that her location is being tracked.

Bank customers also expect financial institutions to keep records of checks they have deposited and cashed, loan applications they have filled out, and credit cards for which they

74. Erin Murphy, *The Case Against the Case For Third-Party Doctrine: A Response to Epstein and Kerr*, 24 BERKELEY TECH. L.J. 1239, 1240 (2009).

75. *Graham*, 846 F. Supp. 2d at 398–99 (citation omitted).

76. *Id.* at 398.

77. *Id.* at 398 n.10 (citing SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); Donaldson v. United States, 400 U.S. 517, 522–23 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966)).

78. *Id.* at 398.

79. United States v. Miller, 425 U.S. 435, 444 (1976).

80. *See Chronology of Microfilm Developments*, UNIV. OF CAL. REGIONAL LIBRARY FACILITY, http://www.srlf.ucla.edu/exhibit/html/section3_briefhist/Chronology.htm (last visited Oct. 5, 2013).

81. *Miller*, 425 U.S. at 439, 449, 451.

82. *Id.* at 442.

have signed up.[83] On the other hand, do cell phone customers expect their service provider to amass records of their location twenty-four hours each day? What is more, the bank records, whether characterized as "business records" or not, reflect tangible items turned over to the bank—deposits, checks, loan applications, etc. In contrast, the SCA makes available to the government not just applications and cell phone service agreements, but intangible and extremely detailed personal information.[84]

Perhaps in an effort to create a more persuasive argument, *Graham* then analogized cell site data to the list of dialed phone numbers seized in *Smith v. Maryland*.[85] Yet, *Graham* again sidestepped a crucial distinction. A list of phone numbers dialed and received—traditional "phone records"—is not nearly as revealing as the information obtainable under the SCA. Phone records, such as those seized in *Smith*, provide the government with nothing more than a list of numbers dialed and received.[86] Modern cell site data, on the other hand, "generat[es] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[87]

Following these feeble analogies, the court held that the defendants lacked a reasonable expectation of privacy in their cell site data because, like the microfilm records in *Miller* and the phone number lists in *Smith*, the information was released to a third party—the defendants' service provider.[88] But *Graham* does not stop there. Under *Graham*, the third-party rule applies even if the information was released to the third party on the assumption that it would be used for a limited purpose, such as improving call quality.[89] Further, according to *Graham*, the cell phone customer lacks a reasonable expectation of privacy even if she signed up assuming "the confidence placed in [her service provider] would

83. *Id.* at 442–43.

84. Stored Communications Act (SCA), 18 U.S.C. § 2703 (2006).

85. United States v. Graham, 846 F. Supp. 2d 384, 399 (D. Md. 2012) (citing Smith v. Maryland, 442 U.S. 735, 737 (1979)).

86. Smith v. Maryland, 442 U.S. 735, 737 (1979).

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

88. *Graham*, 846 F. Supp. 2d at 389, 400.

89. *Id.* at 400.

not be betrayed."[90] Given the potential privacy ramifications inherent in this reasoning, it hardly comes as a surprise that current Supreme Court Justices are urging a reconsideration of the third-party doctrine.[91] For, if the reasoning in *Graham* were to become the rule, it would be unreasonable for an individual to assume that information, such as cell phone data that is turned over to third parties, will be used for a limited purpose, such as improving the quality of cell phone service. But if every phone call, email, and text message involves a third-party service provider, will an individual's expectation of privacy ever be reasonable?

### *B. Texas and New York District Courts Are Upholding the Fourth Amendment*

In reality, the world's six billion cell phone users[92] do not "voluntarily" convey their location to cell phone providers "in any meaningful way."[93] If anything, cell phone users convey the numbers dialed and received as in *Smith*. A customer dialing his cell phone receives no information from his service provider that his call will reveal his location.[94] To make a call or send a text message, cell phone users are not required to enter their address or zip code. Nothing in the process of placing or receiving calls, emails, or text messages divulges anything about the user's location. Thus, unlike *Smith* and *Miller*, where the defendants knowingly conveyed tangible information to a third party, cell site data is not "knowingly" conveyed by the user, but is generated automatically via invisible radio signals regardless of whether the user makes or receives a call.[95] Admittedly, someone steeped in

90. United States v. Miller, 425 U.S. 435, 433 (1976) (internal citations omitted).

91. *See, e.g.*, *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

92. *See World Has About 6 Billion Cell Phone Subscribers, According to U.N. Telecom Agency Report*, HUFFINGTON POST (Oct. 11, 2012, 7:11 AM), http://www.huffingtonpost.com/2012/10/11/cell-phones-world-subscribers-sixbillion_n_1957173.html.

93. *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 844 (S.D. Tex. 2010), *vacated*, No. 11-20884, 2013 WL 3914484 (5th Cir. July 30, 2013) (quoting *In re* United States For an Order Directing Provider of Electronic Communication Service to Disclose Records to Government, 620 F.3d 304, 317–18 (3d Cir. 2010)).

94. *In re* United States For an Order Directing Provider of Electronic Communication Service to Disclose Records to Government, 620 F.3d 304, 317–18 (3d Cir. 2010).

95. Curtiss, *supra* note 42, at 144.

technology may know of the risk that third-party providers may track and record his movements.[96] Even so, "the bare possibility of disclosure by a third party cannot by itself dispel all expectations of privacy."[97] Holding otherwise would eviscerate *Katz*.[98] *Katz* stressed that no Fourth Amendment protection attaches to information "a person *knowingly* exposes to the public."[99] Thus, the reasoning regarding phone number lists in *Smith* and bank records in *Miller*—that the defendant has no reasonable expectation of privacy in tangible information *knowingly* conveyed to third parties—comports with the third-party doctrine. But involuntary pings transmitted from a cell phone are far from analogous to bank records and phone call logs.[100] Because cell phones now allow us to take pictures, download music, and check email, most people carry their phones with them wherever they go, including constitutionally protected places such as their homes. Accordingly, the government should have a very good reason to access such sensitive data—not just "specific and articulable facts" as required by the SCA.[101]

Rather than follow *Graham*, the Supreme Court, if presented with the question, should adopt the reasoning of the New York and Texas district courts. For instance, the District Court for the Southern District of Texas, when presented with an order to compel data under the SCA similar to the order presented in *Graham*, denied the government's request.[102] The court recognized that it had previously granted similar requests but held the request insufficient absent a showing of probable cause.[103] The court reasoned that "important developments in both technology and caselaw" now "rais[e] serious constitutional doubts about such rulings [granting government requests based on less-than-probable-cause]."[104] Taking this reasoning one step

96. *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d at 845.

97. *Id.*

98. *Id.*

99. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

100. *See In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d at 844.

101. Stored Communications Act (SCA), 18 U.S.C. § 2703 (2006).

102. *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d at 845–46.

103. *Id.* at 829.

104. *Id.*

further, the District Court for the Eastern District of New York adopted an exception to the third-party doctrine for historic cell site data.[105]

## IV. IMPROVING THE LAW: AN EXCEPTION TO THE THIRD-PARTY DOCTRINE SHOULD BE CREATED FOR HISTORIC CELL SITE DATA

When the Fourth Amendment was drafted over 220 years ago, "searches" were understood in a spatial context—a man's home is his castle.[106] To see that the "right to be secure" is defined in spatial terms, one needs to look no further than the concept of "curtilage."[107] Accordingly, as we see in *Graham*, this framework has created difficulties for courts attempting to define "reasonable expectations of privacy" in a digital age.[108] The Court avoided breathing life into *Katz*, and instead applied eighteenth-century law to a twenty-first-century issue.[109] Instead, the Court needs to heed the advice of Justice Sotomayor and re-evaluate its approach to this important body of law.[110]

For example, take the case of Antoine Jones. Jones was suspected of trafficking narcotics.[111] After obtaining more than 2000 pages of data from an FBI-installed GPS on his car, Jones was tried for drug trafficking and conspiracy.[112] He was found guilty and sentenced to life in prison.[113] After the appellate court reversed,[114] the Supreme Court granted certiorari.[115] The question

105. *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 122–24 (E.D.N.Y. 2011).

106. *See* Georgia v. Randolph, 547 U.S. 103, 116 (1984) (noting centuries of special protection afforded to one's home).

107. *See, e.g.*, Oliver v. United States, 466 U.S. 170, 180 (1984) (defining "curtilage" as "the land immediately surrounding and associated with the home").

108. *See generally* Michael L. Snyder, Katz*-ing Up and (Not) Losing Place: Tracking the Fourth Amendment Implications of* United States v. Jones *and Prolonged GPS Monitoring*, 58 S.D. L. REV. 158 (2013); Courtney Burten, Note, *Unwarranted! Privacy in a Technological Age: The Fourth Amendment Difficulty in Protecting Against Warrantless GPS Tracking and the Substantive Due Process and First Amendment Boost*, 21 S. CAL. INTERDISC. L.J. 359 (2011); Quin M. Sorenson, Comment, *Losing a Plain View of* Katz*: The Loss of a Reasonable Expectation of Privacy Under the Readily Available Standard*, 107 DICK. L. REV 179 (2002).

109. United States v. Jones, 132 S. Ct. 945, 954–57 (2012) (Sotomayor, J., concurring).

110. *See id.*

111. *Id.* at 948 (majority opinion).

112. *Id.*

113. *Id.* at 949.

114. *Id.*

presented in *United States v. Jones* was whether the installation of a GPS tracking device placed on a car to monitor the car for a month was a "search" under the Fourth Amendment.[116] Unanimously, the Court found that it was a search.[117]

According to *Jones*, the government cannot place a GPS tracker on a suspect's car for the purpose of continuously monitoring him absent a warrant supported by probable cause.[118] Yet *Jones* was decided narrowly, under the antiquated trespass doctrine.[119] According to Justice Alito, by deciding *Jones* on this "physical intrusion" rationale, the Court was giving the green light to law enforcement's use of a litany of electronic tracking possibilities that do not involve any physical trespass,[120] including historic cell site data available under the SCA.[121] Alito echoed an earlier statement of Justice Harlan: "It would surely be an extreme instance of sacrificing substance to form were it to be held that the Constitutional principle of privacy against arbitrary official intrusion comprehends only physical invasions by the police."[122] For instance, *Jones* does not prevent the police from using a factory-installed vehicular GPS device, or one installed in a cell phone.[123] In turn, these ubiquitous devices could be used for surveillance as extensively as the FBI's GPS tracking device in *Jones*, which yielded over 2000 pages of information.[124] More significantly, the Court avoided reinvigorating the *Katz* test and instead upheld Jones's property-based privacy rights. In so doing, the Court resolved that it must "[a]t bottom . . . 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[125] Apparently, the Court considers privacy expectations "reasonable" when they aspire to the "degree of privacy" enjoyed by Americans

115. *Id.*

116. *Id.* at 948.

117. *Id.* at 954 (Sotomayor, J., concurring).

118. *Id.* at 949 (majority opinion).

119. *Id.* at 949–54.

120. *Id.* at 961 (Alito, J., concurring).

121. See Stored Communications Act (SCA), 18 U.S.C. § 2703 (2006), for regulations on government access to stored communications or transaction records in the hands of third party service providers.

122. Poe v. Ullman, 367 U.S. 497, 551 (1961) (Harlan, J., dissenting).

123. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

124. *Id.* at 948 (majority opinion).

125. *Id.* at 950 (citation omitted).

in 1791. Yet, in 2012, the vast majority of Internet users—by necessity—entrust their online information to ISPs.[126] Consequently, as the law currently stands, these users have abandoned any expectation of privacy by knowingly revealing such information to third parties.[127] Thus, Internet users are constantly, albeit unknowingly, eviscerating their Fourth Amendment protection by logging on. Indeed, while a search warrant and probable cause are required to search one's home, under the third-party doctrine only a subpoena and prior notice—a much lower hurdle than probable cause—are required to compel an ISP to disclose the contents of an email or of files stored on a server.[128] And because the records available to law enforcement under the SCA paint such a detailed picture of an individual's movements and associations, an exception to the third-party doctrine is in order.

Only three months before *Graham* was decided, Justice Alito predicted that "[t]he availability and use of [cell-site location records] and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements."[129] In the same case, Justice Sotomayor projected that such technology "will also affect the *Katz* test by shaping the evolution of societal privacy expectations."[130] *Graham* illustrates the prescience of these two justices. *Graham* applied *Katz* and found that the defendants lacked any reasonable expectation of privacy in light of the third-party doctrine.[131] And if *Graham* becomes the rule, Justice Sotomayor's opinion will be vindicated. Once it becomes common knowledge that all electronic communications are freely discoverable by the government, "society" will no longer "expect" any privacy in such information. In theory, cell phone users will have a choice: enjoy the privacy promised by the Fourth Amendment or enjoy the convenience of multimedia technology in the palm of one's hand. In reality, no such choice exists. Cell phones and smartphones are essential

126. *Cf. id.* at 957 (Sotomayor, J., concurring) (stating that, as a general matter, in the current digital age people disclose their web information to ISPs).

127. *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 389 (D. Md. 2012).

128. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1211–12 (2004).

129. *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

130. *Id.* at 955 (Sotomayor, J., concurring).

131. *Graham*, 846 F. Supp. 2d at 389.

today, particularly in the business world where many employers issue company cell phones. If *Graham* becomes the rule, people may, in fact, "reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[132] The Framers of the Fourth Amendment would neither have anticipated nor endorsed such a result.

The SCA's "specific and articulable facts" standard is inappropriate in a digital age. By setting the standard below probable cause, the SCA gives law enforcement the ability to traipse on Fourth Amendment rights, particularly when it comes to cell location data, such as historic cell site reports. For this reason, an exception to the third-party rule should be created to accommodate historic cell site data. First, as the District Court for the Eastern District of New York pointed out, case law supports such an exception.[133] Just last year, that court created such an exception by reasoning, in direct opposition to *Graham*, that "cell-phone users have a reasonable expectation of privacy in cumulative cell-site-location records, despite the fact that those records are collected and stored by a third party."[134] As the court explained, an exception for historic cell site data does not prevent the government from obtaining all information from an individual's service provider.[135] In fact, the exception "preserve[s] the third-party-disclosure doctrine in typical cases where information is disclosed to third parties, such as consensual surveillance cases."[136] For instance, the exception could permit the disclosure merely of phone number lists as in *Smith*, or a bank's "business records" as in *Miller*, but still afford traditional Fourth Amendment protection to more "private user information," such as that received from more sophisticated modern cell phones.[137]

132. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

133. *In re* Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 125 (E.D.N.Y. 2011); *see also In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010), *vacated*, No. 11-20884, 2013 WL 3914484 (5th Cir. July 30, 2013).

134. *Id.* at 126.

135. *Id.* at 125; *see* Smith v. Maryland, 442 U.S. 735, 747 (1979) (Marshall, J., dissenting).

136. *In re Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 125.

137. *Id.*

Without such an exception, the government could continue to obtain "information which is objectively recognized as highly private."[138] Over time, it will be unreasonable for any cell phone customer to expect that his confidences will be respected and that his communications will be kept private. Meanwhile, cases upholding Fourth Amendment rights will be anomalous because society will become conditioned to expect the discovery of their private information. However, as much as one may resent the government exploring the pages of one's life, the necessity and attraction of sophisticated cell phones is far too intoxicating for the average consumer. It is hard to believe that the Framers of the Fourth Amendment would have contemplated that consumers would be faced with an impractical choice between privacy and convenience.

## V. CONCLUSION

If the third-party doctrine continues to allow the government to obtain historic cell site data under the SCA based on "specific and articulable facts,"[139] it will become virtually impossible for a cell phone user to manifest his expectation of privacy without also relinquishing his phone. The Framers of the Bill of Rights did not envision a government capable of monitoring a citizen's every move.[140] Such an idea would have been inconceivable. Yet more than 200 years later, such is the reality. The government can obtain, store, and instantly retrieve a map of one's movements through digital diaries. Nowadays, one cannot communicate electronically without involving a third party. Justice Sotomayor is right. The Supreme Court needs to revisit the third-party doctrine and start creating exceptions for technology such as historic cell site data that reveals much more than numbers dialed and received. The illusion that millions of Americans have consented to warrantless intrusions of their personal information by virtue of owning a cell phone is absurd. Given the necessity of technology in our modern world, people should not be forced to choose between privacy and convenience,

138. *Id.* at 126; *see* U.S. v. Maynard, 615 F.3d 544, 555 (D.C. Cir. 2010).

139. United States v. Graham, 846 F. Supp. 2d 384, 388 (D. Md. 2012).

140. *In re Application for the United States for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 125.

as the SCA now requires. The Fourth Amendment does not demand as much and neither should the courts.