Northern Illinois University Law Review

Volume 35 | Issue 2 Article 6

2-1-2015

Playing Hide and Seek with Big Brother: Law Enforcement's Use of Historical and Real Time Mobile Device Data

Ryan Merkel

Playing Hide and Seek with Big Brother: Law Enforcement's Use of Historical and Real Time Mobile Device Data

RYAN MERKEL*

Cell phones and smartphones are everywhere. Today the majority of Americans own one of these mobile devices. Because these devices are only useful when within arm's reach, they are almost always in the same location as their owner. Even when not in use, these devices are in contact with the towers which allow them to function. Via this contact, the device's location, and as a byproduct the owner's location, is recorded by the service provider. In addition, smartphones are equipped with GPS technology which allows for precise real-time and historical tracking of the device. Law enforcement agencies across the country are obtaining this mobile device location data from providers to aid them in a variety of investigations. This data has proven to be an invaluable resource to law enforcement. Currently federal law enforcement agencies can obtain this data without first seeking a warrant based upon probable cause. Section 2703 of the Stored Communications Act allows law enforcement to obtain this data pursuant to a court order upon establishing that there are "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." This is a lesser standard than probable cause. This Comment argues that pursuant to the Fourth Amendment law enforcement should be required to obtain a warrant based upon probable cause prior to receiving this data from service providers. This data can reveal sensitive and intimate details about an individual's activities and whereabouts otherwise unknowable. It is the position of this Comment that these details should be afforded the minimal protection of a probable cause showing before they are disclosed. To be clear, this Comment recognizes the invaluable resource of mobile data as a crime fighting tool and in no way suggests that law enforcement should be barred from using this data. Rather, law enforcement

* Juris Doctor Candidate, May 2015, Northern Illinois University College of Law and Assistant Editor of the *Northern Illinois University Law Review*; B.A. in Political Science, University of Illinois at Urbana-Champaign. I would like to thank my family, friends and loved ones for all of their support and understanding during the construction of this Comment. Also, a special thanks to everyone at the *Northern Illinois University Law Review* for their hard work during the editing and publication process.

should simply have to obtain a warrant before being granted access to the data.

I. INTRODUCTION

One Mississippi, two Mississippi, three Mississippi, four Mississippi, five Mississippi, six Mississippi, seven Mississippi. If you are the owner of a cell phone or smartphone and your phone is currently turned on, in the seven seconds it took you to read the first sentence of this Comment, your phone's location was recorded by your service provider.[1] Odds are that your cell phone or smartphone is in the same place as you, and if so, your location was recorded as a by-product and will be again in seven seconds as long as the phone is turned on whether or not you have been using it.[2] This may very well come as a surprise, but it is no surprise to municipal, state, and federal law enforcement agencies across the nation who are obtaining this information from service providers to aid in criminal investigations.[3]

---

1. *See* New Jersey v. Earls, 70 A.3d 630, 636 (N.J. 2013) (citing *In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 750 (S.D. Tex. 2005).

2. *Id.*

3. *See* AM. CIV. LIBERTIES UNION, *Cell Phone Location Tracking Public Records Request* (Mar. 25, 2013), https://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request [hereinafter *Cell Phone Location Tracking*].

This Comment will explore the constitutionality of federal law enforcement agencies obtaining historical cell-site data and real time site data from service providers. In order to discuss the constitutionality of law enforcement using this data, it is necessary to have a basic background understanding of what this data is and how it is gathered. The first few pages of this Comment are designated for that purpose. This Comment will then examine historical Supreme Court jurisprudence interpreting the protections afforded to civilians by the Fourth Amendment. Further, this Comment will discuss three recent cases that have reached differing conclusions as to the constitutional burdens placed on law enforcement before it can obtain location information from service providers.[4] Specifically, this Comment will argue that the Fourth Amendment and United States Supreme Court jurisprudence interpreting the Fourth Amendment mandate that federal law enforcement agencies wishing to obtain location data from service providers first obtain a warrant based upon probable cause, except in exigent circumstances. This argument is based on the premise that individuals have a reasonable expectation of privacy in the location data given off from their mobile devices, that individuals do not knowingly expose their location data to the public by simply possessing a mobile device, that location data reveals intimate details about the home otherwise unknowable to law enforcement and that jurisprudence affording less Fourth Amendment protection to business records is outdated and incompatible with modern technology.

II. BACKGROUND

Like it or not, it is an unavoidable fact of American life that cell phones and smartphones are everywhere. According to the *Pew Research Center*, as of May 2013, ninety-one percent of American adults own a cell phone and fifty-six percent own a smartphone.[5] Further, the number of cell phone owners has been on the rise, growing from sixty-five percent of Americans in November 2004, to ninety-one percent in May 2013.[6] As a result of the increased popularity of cell and smartphones, the number of cell towers in the United States has grown from 104,288 in 2000 to 301,779 in 2012.[7]

---

4. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); *Earls*, 70 A.3d 630.

5. Lee Rainie, *Cell Phone Ownership Hits 91% of Adults*, PEW RES. CTR. (June 6, 2013), http://www.pewresearch.org/fact-tank/2013/06/06/cell-phone-ownership-hits-91-of-adults/.

6. *Id.*

7. *Earls*, 70 A.3d at 637.

Cell phones and smartphones (hereinafter "mobile devices") can be tracked using two primary methods.[8] The two methods are network based (hereinafter "cell-site") tracking and handset based (Global Positioning System, hereinafter "GPS") tracking.[9] Network based tracking was alluded to in the introduction of this Comment with reference to a mobile device's location being recorded by a service provider every seven seconds. Network based tracking occurs automatically as a mobile device communicates with the network via radio waves between the device and cell-sites or radio bases.[10] Cell-sites are essentially the large radio towers which are commonplace on the sides of roadways, but as modern technology has advanced, these cell-sites can be much more discreet.[11] Mobile devices communicate with the cell-site that is nearest to the device because it provides the strongest signal.[12] This automatic and continuous communication between mobile devices and cell-sites is necessary to ensure that incoming calls can be routed to the mobile device.[13]

Each time a mobile device communicates with the nearest cell-site, the location of the mobile device is subsequently stored in a database maintained by the specific service provider.[14] The amount of time a service provider will retain this location data gained from individual cell-sites depends on the service provider.[15] According to data compiled by the United States Department of Justice, the retention times can be substantial, ranging from one rolling year in the case of Verizon Wireless, to indefinitely for communications with cell-sites from AT&T customers subsequent to 2008.[16]

The accuracy of the location information that network based tracking provides depends on how closely cell-sites are located to one another.[17] The area serviced by an individual cell-site is known as a sector and the closer cell-sites are spaced, the smaller an individual sector will be.[18] As mentioned above, the number of cell-sites has nearly tripled over the last dec-

---

8. *Id.*
9. *Id.*
10. *Id.* at 636.
11. *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 13 (2010) [hereinafter *Hearing*] (statement of Prof. Matt Blaze), *available at* http://judiciary.house.gov/_files/hearings/printers/111th/111-109_57082.PDF.
12. *Id.* at 20.
13. *Id.* at 13.
14. *Id.* at 27.
15. *Id.* at 16.
16. AM. CIV. LIBERTIES UNION, *Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart* (Aug. 2010), https://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.
17. *See Hearing*, *supra* note 11, at 23-24.
18. *Id.* at 24-25.

ade, resulting in greater accuracy in network based tracking.[19] The size of a sector largely depends on the population density of a specific area.[20] According to Professor Matt Blaze of the University of Pennsylvania:

> [T]he largest sectors can still be several miles in diameter in rural areas, sparsely populated areas. But the latest technology has trended toward what are called variously microcells, picocells and femtocells that are designed not to serve an area of miles in diameter, but rather to serve a very, very specific location, such as a floor of a building or even an individual room in a building such as a train station waiting room or an office complex or hotel or *even a private home*.[21]

Federal regulations now require a baseline of accuracy that service providers must meet in regards to locating mobile devices. Regulations by the Federal Communications Commission required cell phone carriers to have, by 2012, the ability to locate phones within one hundred meters for sixty-seven percent of calls and three hundred meters for ninety-five percent of calls for network based calls.[22] They must also be able to locate phones within fifty meters for sixty-seven percent of calls and one hundred and fifty meters for ninety-five percent of calls for handset based calls.[23]

It is clear that mobile devices are becoming more prevalent, while at the same time, the sectors used by the devices are shrinking. It is a fair assumption that this trend will continue in the future. As a result, the location information provided by network based tracking will also likely improve in accuracy as time progresses.

The second primary means to track a phone is handset based, which relies on GPS to locate the mobile device.[24] The majority of cell phones today contain GPS receivers.[25] Further, many mobile devices contain GPS chips that can be used for emergency tracking.[26] For example, since December 31, 2003, all new handsets sold by Verizon Wireless (which happens to be one of America's largest service providers) contain such chips to

---

19. New Jersey v. Earls, 70 A.3d 630, 637 (N.J. 2013).
20. *Hearing*, *supra* note 11, at 14-15.
21. *Id.* at 15-16 (emphasis added).
22. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013) (citing 47 C.F.R. § 20.18(h) (2012)).
23. *Id.*
24. *Earls*, 70 A.3d at 636.
25. *Id.* at 637 (citing Jagdish Rebello, *Four Out of Five Cell Phones to Integrate GPS by End of 2011*, IHS TECH. (July 16, 2010), https://technology.ihs.com/388892/).
26. *Earls*, 70 A.3d at 637.

help locate a phone in the case of an emergency.[27] Utilizing these GPS receivers, mobile devices so equipped, calculate their location on their own by communicating with satellites in orbit.[28] This technology works reliably outdoors and can locate a phone "to within about 10 meters of accuracy."[29]

III. CONTROLLING STATUTORY PROVISIONS

The Fourth Amendment to the United States protects the people of the United States from "unreasonable searches and seizures."[30] Specifically, the Fourth Amendment states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon *probable cause*, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[31]

Of special importance for purposes of this Comment is the constitutional requirement that before a warrant can be issued probable cause must be established.[32]

The second statutory provision of central importance to this Comment is Section 2703 of the Stored Communications Act (hereinafter "SCA").[33] This statute provides in part:

> A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers *specific and articulable facts* showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not is-

---

27. *Id.* (citing VERIZON WIRELESS, *Wireless Issues: Enhanced 911* (2014), http://aboutus.verizonwireless.com/commitment/safety_security/).

28. *See Hearing*, *supra* note 11, at 20-21.

29. *Id.* at 14, 22.

30. U.S. CONST. amend. IV.

31. *Id.* (emphasis added).

32. *See id.*

33. 18 U.S.C. § 2703(d) (2012).

> sue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.[34]

For purposes of this Comment it is critical to point out at this juncture the differences between the Fourth Amendment requirements and those in the SCA. The Fourth Amendment concerns warrants relating to a search or seizure by government officials, while Section 2703 of the SCA concerns court orders allowing government officials to obtain information from service providers.[35] Further, the Fourth Amendment requires a showing of probable cause before a warrant will be issued, while the SCA requires a showing of "specific and articulable facts" by the government before a court order will be issued requiring a service provider to turn over customer information to the police.[36]

IV. HISTORICAL FOURTH AMENDMENT INTERPRETATIONS

In 1967, the Supreme Court released a decision that spawned a line of precedent interpreting Fourth Amendment protections. *Katz v. United States*, involved FBI agents attaching a listening and recording device to the outside of a phone booth in order to listen in on Katz's phone calls while Katz was involved in taking illegal bets.[37] The Court determined that the FBI's use of the recording device without first obtaining a warrant based on probable cause violated Katz's Fourth Amendment right against unreasonable searches and seizures.[38] Of most significance to the issue at hand in this Comment is the rule that the Court has adopted, which was first expressed in the concurring opinion of Justice John M. Harlan II.[39] The test is twofold and reads:

> [F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus a man's home is, for

34. 18 U.S.C. § 2703(d) (2012) (emphasis added).
35. U.S. CONST. amend. IV; 18 U.S.C. § 2703(d) (2012).
36. U.S. CONST. amend. IV; 18 U.S.C. § 2703(d) (2012).
37. Katz v. United States, 389 U.S. 347, 348 (1967).
38. *Id.* at 358.
39. *Id.* at 361.

> most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected" because no intention to keep them to himself has been exhibited.[40]

Also significant to the discussion of this Comment is the Court's determination that what a person "knowingly exposes to the public" is afforded less protection under the Fourth Amendment.[41] Specifically, the Court stated:

> For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[42]

In 1983, the Supreme Court applied the *Katz*[43] test in *United States v. Knotts* where law enforcement caused an electronic monitoring device placed in a container of chemicals to come into the possession of the defendant without first obtaining a warrant.[44] Law enforcement used this device to aid in their surveillance of the defendant but only in areas where the defendant could have been watched by ordinary means, such as, public roadways.[45] The Court determined that the use of the electronic device did not constitute a Fourth Amendment violation.[46] The Court reasoned that the defendant did not have a "reasonable expectation of privacy" when traveling from one place to another because in doing so he had conveyed that information to anyone who was looking.[47]

Just one year later, the Court addressed a similar case involving the use of a concealed electronic monitoring device without a warrant by law enforcement in *United States v. Karo*. In *Karo*, the Court reached a conclusion contrary to *United States v. Knotts* regarding whether a Fourth Amendment violation had occurred.[48] The distinction between *Karo* and

---

40. *Id.*
41. *Id.* at 351.
42. Katz v. United States, 389 U.S. 347, 351-52 (1967) (citations omitted).
43. *Id.* at 347.
44. United States v. Knotts, 460 U.S. 276, 278-79 (1983).
45. *See id.*
46. *Id.* at 281-82.
47. *Id.* at 281.
48. United States v. Karo, 468 U.S. 705, 715 (1984).

Knotts turned on the fact that in *Karo* the device entered the defendant's home and in doing so revealed sensitive information that could not have otherwise been observed.[49] Further, unlike *Knotts* the Court in *Karo* determined that the defendant had not "voluntarily conveyed to anyone who wanted to look" by bringing the device into his house.[50] The Court summarized saying, "[i]n sum, we discern no reason for deviating from the general rule that a search of a house should be conducted pursuant to a warrant."[51]

Karo does not stand alone in its expression that an individual's home is afforded the highest levels of Fourth Amendment protection.[52] The Court has stated "when it comes to the Fourth Amendment, the home is first among equals."[53] "At the Amendment's 'very core' stands 'the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.'"[54] Further, the Court has opined that "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."[55]

The Supreme Court has expanded upon *Katz* to further define when an individual has "knowingly expose[d]" something to the public therefore waiving his Fourth Amendment guarantee that said information would not be known by the government absent a warrant.[56] One such example is *United States v. Miller*, where the Court determined that individuals do not have a reasonable expectation in bank records relating to an account of theirs.[57] The Court explained that "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[58] Similarly, in *Smith v. Maryland*, the Court found that when a telephone company installs a device to record the numbers dialed by an individual in response to a police request that no Fourth Amendment violation has occurred.[59] The Court determined that the "petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[60] "In so doing, petitioner assumed the risk that the company would

---

49. *Id.*
50. *Id.* (quoting *Knotts*, 460 U.S. at 281).
51. *Id.* at 718.
52. *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); Kyllo v. United States, 533 U.S. 27, 31 (2001); Silverman v. United States, 365 U.S. 505, 511 (1961).
53. *Jardines*, 133 S. Ct. at 1414.
54. *Id.* (quoting *Silverman*, 365 U.S. at 511).
55. *Kyllo*, 533 U.S. at 37.
56. Katz v. United States, 389 U.S. 347, 351 (1967).
57. United States v. Miller, 425 U.S. 435 (1976).
58. *Id.* at 443.
59. Smith v. Maryland, 442 U.S. 735, 744 (1979).
60. *Id.*

reveal to police the numbers he dialed."[61] Justice Thurgood Marshall was of the opposite opinion, writing "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[62]

While *Miller* and *Smith* certainly represent that an individual's "reasonable expectation of privacy" shrinks when they expose information to third parties,[63] the Supreme Court in other circumstances has held that while a third party may be allowed to view an individual's private information in the course of business, it does not give them free reign to turn that information over to law enforcement.[64] For example, the Supreme Court has determined that when a landlord had authority to enter the house of a tenant renter under certain circumstances that authority did not permit the landlord to give police permission to search the rented house absent a warrant.[65] Doing so in the Court's opinion would reduce the Fourth Amendment privacy in one's home to the discretion of a landlord.[66] Similarly, the Court has determined that while the janitorial staff at a hotel does have the authority to enter a rented hotel room, that authority does not allow them to grant access to law enforcement that do not have a search warrant.[67]

V. RECENT CASES ON POINT

A. *UNITED STATES V. JONES*

The question of the constitutionality of electronic surveillance of persons by law enforcement is by no means a new controversy as evidenced by *Olmstead v. United States*,[68] a prohibition era phone tapping case, which was overturned by *Katz v. United States*.[69] In 2012, the Supreme Court was called upon to resolve a conflict between the use of GPS trackers by law enforcement and the Fourth Amendment protection against unreasonable searches in *United States v. Jones*.[70] In *Jones*, law enforcement officers installed a GPS tracking device on the vehicle which was operated by the

61. *Id.*
62. *Id.* at 749 (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 95-96 (1974) (Marshall, J., dissenting)).
63. *See Miller*, 425 U.S. at 435; *Smith*, 442 U.S. at 735.
64. *See* Chapman v. United States, 365 U.S. 610 (1961); Stoner v. California, 376 U.S. 483 (1964).
65. *See Chapman*, 365 U.S. at 616-17.
66. *Id.*
67. *Stoner*, 376 U.S. at 487-88.
68. Olmstead v. United States, 277 U.S. 438 (1928).
69. Katz v. United States, 389 U.S. 347 (1967).
70. United States v. Jones, 132 S. Ct. 945 (2012).

defendant after he became the target of a narcotics trafficking investigation.[71] The officers had obtained a warrant to install the device, but when the device was installed it was done outside the temporal and geographic scope of the warrant.[72] The government used the information from this GPS device to track the vehicle for twenty-eight days.[73] After being indicted for several narcotics related offenses, Jones sought to have the evidence gained by the government's use of the GPS tracker suppressed as a search in violation of the Fourth Amendment.[74]

The issue reached the Supreme Court and Justice Antonin Scalia issued the plurality opinion of the Court in which Chief Justice John G. Roberts, Justice Anthony Kennedy, Justice Clarence Thomas, and Justice Sonia Sotomayor joined, concluding the government's installment of the GPS tracker outside the scope of the warrant constituted a Fourth Amendment violation.[75] Justice Sotomayor also authored a separate opinion concurring in the judgment, as did Justice Samuel Alito who was joined by Justice Ruth Bader Ginsberg, Justice Stephen Breyer, and Justice Elena Kagen.[76] In sum, all nine Justices agreed that the government's installment of the GPS tracking device on Jones' vehicle was outside the limits of the warrant and therefore constituted a Fourth Amendment violation.[77] But, the three opinions were based on differing rationales as to how that conclusion was reached.[78]

Justice Scalia concluded that it was not necessary to apply the *Katz*[79] analysis because Justice Scalia determined the instillation of the beeper to be a "trespassory search" in violation of the Fourth Amendment.[80] Further, Justice Scalia opined that *Katz* analysis is not the exclusive manner for the Court to address possible Fourth Amendment violations.[81] Of specific importance for purposes of this Comment is Justice Scalia's opinion that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[82]

While Justice Sotomayor joined Justice Scalia's opinion, she wrote separately expressing that while the use of the GPS tracker violated Jones's reasonable expectation of privacy under *Katz*, Justice Scalia's approach

71. *Id.* at 948.
72. *Id.*
73. *Id.*
74. *Id.*
75. United States v. Jones, 132 S. Ct. 945, 947-54 (2012).
76. *Id.* at 954-64.
77. *See id.* at 945.
78. *Id.*
79. Katz v. United States, 389 U.S. 347 (1967).
80. *Jones*, 132 S. Ct. at 954.
81. *Id.* at 953.
82. *Id.*

provided a narrower basis for the decision.[83] In doing so, Justice Sotomayor wrote, "[m]ore fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"[84] in reference to the Court's decisions in *Miller*[85] and *Smith*.[86] Further, Justice Sotomayor opined:

> 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. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[87]

Justice Alito's concurrence concludes that the long-term GPS tracking of Jones' vehicle impinged on his reasonable expectation to privacy under *Katz*[88] and was therefore a search in violation of the Fourth Amendment.[89] In reaching this conclusion, Justice Alito commented, in regards to reasonable expectations to privacy under *Katz*,[90] that "[d]ramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile."[91] Further, Justice Alito recognized that the traceable nature of mobile devices may be the most significant technological change effecting reasonable expectations of privacy.[92]

---

83. *Id.* at 957.
84. *Id.*
85. United States v. Miller, 425 U.S. 435 (1976).
86. Smith v. Maryland, 442 U.S. 735 (1979).
87. *Jones*, 132 S. Ct. at 957.
88. Katz v. United States, 389 U.S. 347 (1967).
89. *Jones*, 132 S. Ct. at 964.
90. *Katz*, 398 U.S. 347.
91. *Jones*, 132 S. Ct. at 962.
92. *Id.* at 963.

B. *UNITED STATES V. SKINNER*

While *United States v. Jones*[93] did not directly focus on the constitutionality of law enforcement obtaining location data from mobile devices absent a warrant, a few federal appellate courts have had to address the issue head-on, while many others have yet to do so.[94] One such jurisdiction that ruled on the issue was the Sixth Circuit Federal Court of Appeals in *United States v. Skinner*.[95] In *Skinner*, Federal Drug Enforcement Agency (hereinafter "DEA") agents tracked the defendant's movements in real time along public highways between Arizona and Tennessee using GPS "ping data" obtained via court order from the defendant's pay-as-you-go service provider.[96] Ping data is gathered by calling an individual's mobile device and then hanging up before it rings in order to reveal the phones physical location via GPS.[97] Based on this location data, DEA agents were able to locate the defendant and his son at a Texas rest stop and seize 1,100 pounds of marijuana.[98] The court in *Skinner* held that there was no Fourth Amendment violation when DEA agents obtained and used the location data given off by the defendant's mobile device.[99] The court stated that the defendant "did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."[100] This language is clearly alluding to the second prong of the *Katz*[101] analysis, yet the majority in *Skinner* never directly references *Katz*.[102] The court in *Skinner* found the facts of *Skinner* to be directly comparable to those in *Knotts*,[103] where the Supreme Court found no constitutional violation because location information revealed by electronic surveillance along public roadways could have been obtained by visual observation.[104] Further, the *Skinner* court distinguished the case from *Jones* on the basis that there was no governmental trespass in *Skinner*,[105] which was the basis of Justice Scalia's opinion,[106] nor was the tracking so extensive in time to violate a reasonable expectation of

93. *Id.* at 948.
94. *E.g.*, United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
95. *Skinner*, 690 F.3d 772.
96. *Id.* at 774-76.
97. *Id.* at 778.
98. *Id.* at 774.
99. *Id.* at 777.
100. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).
101. Katz v. United States, 389 U.S. 347, 361 (1967).
102. *Id.*
103. United States v. Knotts, 460 U.S. 276 (1983).
104. *Skinner*, 690 F.3d at 778.
105. *Id.* at 779-80.
106. United States v. Jones, 132 S. Ct. 945, 954 (2012).

privacy[107] discussed by Justice Alito in *Jones*.[108] Additionally, the *Skinner* court determined, based on *Karo*,[109] that Skinner accepted his mobile device with the GPS technology inside and therefore could not complain when that technology subsequently revealed his location on public thoroughfares.[110]

C. *IN RE U.S. FOR HISTORICAL CELL SITE DATA*

A year after *Skinner*[111] was decided, the Fifth Circuit in *In re U.S. for Historical Cell Site Data* was called upon to decide the constitutionality of law enforcement obtaining location data from a service provider based on a 18 U.S.C. § 2703(d) court order.[112] The United States government in *In re U.S. for Historical Cell Site Data* submitted three applications to a federal magistrate judge pursuant to 18 U.S.C. § 2703(d) seeking evidence relevant to three separate criminal investigations from mobile device service providers.[113] The government sought the same type of evidence in each application.[114] Specifically, the government wanted sixty days of historical cell-site data relating to three mobile devices based on network based tracking which relies upon a mobile device communicating with a cell-site such as a cell tower as discussed previously in this Comment.[115] The magistrate judge denied the applications despite the government having demonstrated the "specific and articulable facts" required by 18 U.S.C. § 2703(d), on the grounds that "[c]ompelled warrantless disclosures of cell site data violate[] the Fourth Amendment."[116] The government challenged the magistrate judge's ruling in the federal district court and lost.[117] The district court judge determined that such disclosure of cell-site data may only be acquired by a warrant issued on probable cause and that the "specific and articulable facts" standard under 18 U.S.C. § 2703(d) is below the standard required by the United States Constitution.[118]

---

107. *Skinner*, 690 F.3d at 780.
108. *Jones*, 132 S. Ct. at 964.
109. United States v. Karo, 468 U.S. 705 (1984).
110. *Skinner*, 690 F.3d at 780-81.
111. *Id.* at 772.
112. *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
113. *Id.* at 602 (a showing of probable cause is not required by 18 U.S.C § 2703(d) (2012)).
114. *Id.*
115. *Id.*; *see also Hearing*, *supra* note 11, at 12-30.
116. *In re U.S. for Historical Cell Site Data*, 724 F.3d at 602 (alteration in original) (quoting *In re* United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 846 (S.D. Tex. 2010) (internal quotation marks omitted)).
117. *Id.* at 602-03.
118. *Id.* at 602.

The Fifth Circuit reviewed the district court's determination and reached the opposite conclusion.[119] In doing so, the court rejected the American Civil Liberties Union's (hereinafter "ACLU") amici argument that individuals have a reasonable expectation of privacy in their location information when they are tracked based on cell-site data.[120] The court distinguished the facts of the case before them from those in *Karo*[121] and *Smith*[122] on the basis that in those cases the government was the one responsible for the collection and recording of an individual's information.[123] Further, the court determined that "the [g]overnment does not require service providers to record this information or store it."[124] The court determined that the historical cell-site data obtained from service providers is "clearly a business record."[125] This determination that cell-site data is a business record is critical to the court's ultimate determination that the government need not obtain a warrant before requiring service providers to turn over cell-site data.[126] The court cited Supreme Court precedent relating to exposures of information to third parties stating, "It is established that, when a person communicates information to a third party *even on the understanding that the communication is confidential*, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."[127] In sum, the court concluded that:

> Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.[128]

In the court's opinion, because individuals who own mobile devices voluntarily convey this cell-site data to their service providers, who in turn

---

119. *Id.*
120. *Id.* at 608.
121. United States v. Karo, 468 U.S. 705 (1984).
122. Smith v. Maryland, 442 U.S. 735 (1979).
123. *In re U.S. for Historical Cell Site Data*, 724 F.3d at 609.
124. *Id.* at 612.
125. *Id.* at 611.
126. *Id.* at 610.
127. *Id.* (quoting SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984)) (internal quotation marks omitted).
128. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013).

create business records from this information, there is no Fourth Amendment violation when law enforcement obtains this information absent a warrant based on probable cause.[129]

D. *NEW JERSEY V. EARLS*

While the Fifth and Sixth Circuits have determined that law enforcement compelling service providers to turn over location data derived from mobile devices does not violate the Fourth Amendment, the New Jersey Supreme Court determined that such practice is a violation of the New Jersey Constitution.[130] It is important to note that the decision in *New Jersey v. Earls* was based on an interpretation of the New Jersey Constitution rather than on an interpretation of the United States Constitution.[131] Nonetheless, this decision is a valuable resource when discussing the constitutionality of location data being obtained via court order because the court in *New Jersey v. Earls* engaged in much of the same analysis as the courts in *Skinner*[132] and *In re U.S. for Historical Cell Site Data*,[133] yet it reached the opposite conclusion.

In reaching this conclusion, the court addressed the idea that location data is voluntarily conveyed to a third party service provider by the individual who owns a mobile device and therefore does not necessitate warrant protection.[134] In doing so, the court recognized the Supreme Court precedent in *Smith*[135] and *Miller*[136] underlying this rational but distinguished this precedent in relation to the present issue of location data.[137] The court opined that "cell-phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."[138] Further, the court noted that location data reveals much more information to service providers than in other third party situations.[139] Specifically, the court stated in regards to law enforcement tracking a mobile device that "[i]t is akin to using a tracking device and can function as a substitute for 24/7 surveillance without police having to confront the limits of their resources. It also involves a degree of intrusion that a reasonable person

129. *See id.* at 615.
130. New Jersey v. Earls, 70 A.3d 630, 644 (N.J. 2013).
131. *Id.*
132. United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).
133. *In re U.S. for Historical Cell Site Data*, 724 F.3d 600.
134. *See Earls*, 70 A.3d at 641.
135. Smith v. Maryland, 442 U.S. 735 (1979).
136. United States v. Miller, 425 U.S. 435 (1976).
137. *Earls*, 70 A.3d at 641.
138. *Id.*
139. *Id.* at 642.

would not anticipate."[140] Moreover, the court stated that "details about the location of a cell phone can provide an intimate picture of one's daily life."[141] The court then proceeded to examine what reasonable expectations of privacy individuals have in their mobile devices location data.[142] The court took into account the increased accuracy and frequency of the information recorded by network based tracking commenting, "[C]ell phones can be pinpointed with great precision—to within feet in some instances. That information is updated every seven seconds through interactions with cell towers, whether the phone is in public or private space."[143] Based on this understanding of network based tracking the court reasoned that:

> [C]ell phones are not meant to serve as tracking devices to locate their owners wherever they may be. People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with the police. That was true in 2006 and is equally true today. Citizens have a legitimate privacy interest in such information. Although individuals may be generally aware that their phones can be tracked, most people do not realize the extent of modern tracking capabilities and reasonably do not expect law enforcement to convert their phones into precise, possibly continuous tracking tools.[144]

The court concluded that due to this reasonable expectation of privacy in an individual's location data, the New Jersey Constitution requires that law enforcement must obtain a warrant before compelling service providers to turn over that information.[145]

VI. ANALYSIS

A cursory comparison of the text of the Fourth Amendment with that of section 2703(d) of the SCA reveals one glaring discrepancy.[146] The dis-

---

140. *Id.*
141. *Id.*
142. *Earls*, 70 A.3d at 643.
143. *Id.*
144. *Id.* (footnote omitted).
145. *Id.*
146. U.S. CONST. amend. IV; 18 U.S.C. § 2703(d) (2012).

crepancy is that while the Fourth Amendment requires a warrant based on probable cause before law enforcement can search or seize "persons, houses, papers, and effects,"[147] section 2703(d) of the SCA allows law enforcement to obtain location data from service providers via court order based on a showing of "specific and articulable facts."[148] This discrepancy is not de minimis because the standard law enforcement must meet under the SCA is lower than that required by the Fourth Amendment.[149] It is a well-settled principle of constitutional law that while federal statutes and state statutes may afford greater protections than those contained in the Constitution, they cannot conflict with constitutional protections.[150] The fact that the discrepancy exists between the Fourth Amendment and the SCA is not in and of itself determinative that law enforcement obtaining location data without a warrant is barred by the Fourth Amendment, but, when taken in light of Supreme Court jurisprudence interpreting the Fourth Amendment such a practice cannot be reconciled with the protections afforded by the Fourth Amendment.[151] As a result, the Fifth and Sixth Circuits have erred in determining that a warrant based on probable cause is not required before law enforcement can obtain location data.[152]

A. LOCATION DATA AND *KATZ* TWO PRONG TEST

A proper examination of location data in relation to the Fourth Amendment is not possible without applying the two prong rule for determining when Fourth Amendment protections will apply,[153] which was first spelled out by Justice Harlan in his concurring opinion in *Katz v. United States*,[154] and subsequently adopted by the Court in numerous later opinions.[155] According to the *Katz* test, law enforcement must obtain a warrant

147. U.S. CONST. amend. IV.

148. 18 U.S.C. § 2703(d) (2012).

149. U.S. CONST. amend. IV; 18 U.S.C. § 2703(d) (2012).

150. *See, e.g.*, Marbury v. Madison, 5 U.S. 137 (1803); Cooper v. California, 386 U.S. 58, 62 (1967).

151. *See, e.g.*, United States v. Jones, 132 S. Ct. 945 (2012); Kyllo v. United States, 533 U.S. 27 (2001); United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983); Katz v. United States, 389 U.S. 347 (1967).

152. *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (holding that law enforcement obtaining location data from service providers without a warrant did not violate the Fourth Amendment); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

153. *See* New Jersey v. Earls, 70 A.3d 630, 638 (N.J. 2013); California v. Ciraolo, 476 U.S. 207, 211 (1986) (stating "The touchstone of Fourth Amendment analysis is whether a person has a 'constitutionally protected reasonable expectation of privacy.'").

154. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

155. *See, e.g.*, *Jones*, 132 S. Ct. 945; *Kyllo*, 533 U.S. 27; *Karo*, 468 U.S. 705; *Knotts*, 460 U.S. 276.

to gather information via a search if an individual has first "exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[156]

Because the first prong of the test is viewed subjectively from the viewpoint of the individual whose person or effects have been searched, this part of the test will be met as long as an individual has taken steps to preserve the privacy of the location of their mobile device and consequently himself.[157] This is due to the simple fact that a defendant who wishes to use the Fourth Amendment as a means of excluding evidence is sure to argue that they expected their mobile device's location to remain private from the eyes of law enforcement. The first prong of the test is a relatively low hurdle for a defendant to clear; as a result, the meat of the test is centered on the second prong.[158] So for the issue at hand, the question becomes is society prepared to recognize that individuals have a reasonable expectation of privacy in the location data transmitted by their mobile device to their service provider? Answering this type of question poses several types of difficulties, such as judges confusing their own expectations of privacy for those of society and the reality that rapid technological advancements may alter society's reasonable expectations of privacy.[159]

Given these difficulties individuals who own a mobile device nonetheless should be viewed to hold an expectation of privacy in their location data that society is prepared to recognize as reasonable.[160] As discussed in the background section of this Comment, the vast majority of Americans now own a mobile device,[161] and the precision at which their location can be tracked can be as exact as an individual room in a building or home.[162] The precision of this tracking reveals some of the most sensitive information imaginable about an individual, information that law enforcement would otherwise be unable to obtain based on the traditional restraints on abusive police practices "limited police resources and community hostility."[163] For example, information about activities such as, "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the un-

156. *Katz*, 389 U.S. at 361.

157. *See* Mark J. Kwasowski, Note and Comment, *Thermal Imaging Technology: Should Its Warrantless Use By Police be Allowed in Residential Searches?*, 3 TEX. WESLEYAN L. REV. 393, 398 (1997) (citing United States v. Cusumano, 67 F.3d 1497, 1503 (10th Cir. 1995); *Ciraolo*, 476 U.S. at 209; Florida v. Riley, 488 U.S. 445, 448 (1989)).

158. *See id.* (citing *Riley*, 488 U.S. at 449-50; *Ciraolo*, 476 U.S. at 212-13).

159. *Jones*, 132 S. Ct. at 962 (Alito, J., concurring).

160. *See* New Jersey v. Earls, 70 A.3d 630, 643 (N.J. 2013).

161. Rainie, *supra* note 5.

162. *Hearing*, *supra* note 11, at 15-16.

163. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)) (internal quotation marks omitted).

ion meeting, the mosque, synagogue or church, the gay bar and on and on" are all revealed to law enforcement without first having to establish probable cause to a neutral magistrate.[164] It is hard to believe that these sensitive types of activities (which are often engaged in privately) would not be recognized as reasonable by society and the Court in light of other expectations of privacy the Court has found to be reasonable.[165] If Katz's phone booth conversation about illegal gambling was protected under a reasonable expectation of privacy a logical inference is that an individual's location that reveals a likely communication with a healthcare provider, attorney, cleric, bartender, and so on would enjoy the same privacy protections.[166]

Under *Katz* it is clear that law enforcement could not place a listening device in an examining room in a doctor's office, where the doctor specializes in certain illness, for example, to eavesdrop on the conversation between a suspect and his doctor without first obtaining a warrant.[167] Yet, location data gathered pursuant to the SCA without a warrant would reveal essentially the same information. While the location data would not reveal the exact conversation between this hypothetical patient and doctor, if the doctor specialized in the treatment of a certain ailment it takes very few inferential leaps to determine what the two were talking about. While this is only one hypothetical where location data reveals more than just the location of law enforcement's target it is not hard to imagine many other similar situations where reasonable expectations of privacy are intruded upon by location data gathering. This Comment is in no way suggesting that the ability of law enforcement to conduct visual surveillance on suspects should be altered as visual surveillance of the hypothetical doctor visit would likely pass Fourth Amendment muster according to *Katz* and *Knotts*.[168] The use of location data exposes a much broader picture of an individual's life than traditional surveillance due to its seemingly limitless reach without the safeguards imposed by limited agency resources.[169] While it would be foolish to celebrate the detriment imposed on law enforcement's ability to fight crime due to limited resources it would be equally unwise to embrace the limitless use of location data gathering without judicial oversight.[170] To be clear, this Comment is not advocating keeping relevant location data out of

164. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (quoting New York v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)) (internal quotation marks omitted).

165. *See, e.g.*, Katz v. United States, 389 U.S. 347 (1967) (finding a reasonable expectation of privacy in a phone booth conversation).

166. *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (citing *Weaver*, 909 N.E.2d at 1199).

167. *See Katz*, 389 U.S. 347.

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

169. *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citing Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

170. *See id.*

the hands of law enforcement because it is clearly an invaluable tool. Rather, this Comment is suggesting that law enforcement be required to obtain a warrant based on probable cause before obtaining location data that interferes with reasonable expectations of privacy.

As discussed above, the court in *United States v. Skinner* determined that the defendant did not have a reasonable expectation of privacy in the location data emitted from his cell phone.[171] Oddly, as the concurring opinion of Judge Bernice B. Donald points out, the majority in *Skinner* seems to base this finding of no reasonable expectation of privacy on the basis that the defendant was engaged in illegal activity.[172] The majority expresses this by opining "[w]hen criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[173] Similarly, the majority found no constitutional violation "because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone. If a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal."[174] Whether or not an individual has a reasonable expectation of privacy in the location data emitted from his mobile device should not turn on the criminality of the conduct in which he has engaged. [175] To do so would give non-criminals a reasonable expectation of privacy in their location data while denying the same to those engaged in criminal activity. Under this type of analysis, Katz's phone call about illegal gambling certainly would not be protected but that is not what the Supreme Court determined.[176]

The *Skinner* majority also determined that *United States v. Knotts*[177] was the controlling precedent because like in *Knotts*, Skinner's location data from his cell phone revealed his location on public thoroughfares where his location could have been monitored visually.[178] Here, the *Skinner* majority seems to rely on hind sight because as the facts played out in *Skinner* only location data the DEA agents obtained could have observed visually.[179] This begs the question: what if the location data that was obtained

171. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).
172. *Id.* at 784-85.
173. *Id.* at 774.
174. *Id.* at 777.
175. *Id.* at 785 (citing United States v. Hicks, 59 F. App'x 703, 706 (6th Cir. 2003); United States v. Pitts, 322 F.3d 449, 458 (7th Cir. 2003); United States v. Fields, 113 F.3d 313, 321 (2d Cir. 1997); United States v. Taborda, 635 F.2d 131, 139 n.10 (2d Cir. 1980)).
176. *See* Katz v. United States, 389 U.S. 347 (1967).
177. United States v. Knotts, 460 U.S. 276 (1983).
178. *Skinner*, 690 F.3d at 777-78.
179. *See id.*

without a warrant revealed Skinner's location somewhere unobservable by traditional visual surveillance, such as in the basement of his home? This question highlights a large problem with law enforcement obtaining location data without a warrant. When police request location data, they have no way of knowing up front if the data will reveal private or public location information.[180] As a result, a system of allowing law enforcement to only access location data revealing information that could be viewed through visual surveillance without a warrant would not be practicable.[181] At least where a warrant has been issued there is the safe guard of probable cause in addition to police discretion before the target's privacy is invaded.[182]

B. LOCATION DATA NOT KNOWINGLY EXPOSED

Even if an individual has exhibited a subjective expectation of privacy in something that society is prepared to recognize as reasonable, therefore passing both prongs of the *Katz* test, it may still fail to be protected under the Fourth Amendment if the individual has knowingly exposed the subject matter to the public.[183] Specifically, the Court in *Katz* stated that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[184] So does a mobile device owner knowingly expose anything to the public sufficient to render the location of their mobile device and as a byproduct their location unprotected by the Fourth Amendment?

It is the position of this Comment that a mobile device owner has not. Perhaps the strongest argument against this position is found by analogizing location data to numbers that were recorded by a pen register installed on a telephone in *Smith v. Maryland*.[185] However, this analogy is a stretch. In *Smith*, the Court determined that "petitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business" when he dialed phone numbers on his telephone that would be used by the company to complete his call.[186] The Court reasoned that the defendant knew he was exposing this information, which would be subsequently recorded by the company because long distance calls were reflected on his billing statements.[187]

---

180. New Jersey v. Earls, 70 A.3d 630, 642 (N.J. 2013).
181. *Id.*; *see also* Kyllo v. United States, 533 U.S. 27, 38-39 (2001).
182. *See* Katz v. United States, 389 U.S. 347, 358-59 (1967).
183. *Katz*, 389 U.S. at 351.
184. *Id.*
185. Smith v. Maryland, 442 U.S. 735, 744 (1979).
186. *Id.*
187. *Id.* at 742.

Outside of when an individual purchases a mobile device, places a phone call, sends a message or communicates in some other way via their device like in *Smith*, it is questionable that the owner or user has knowingly exposed anything else. To view otherwise is to assume that owners of mobile devices are well versed in the intricacies of wireless communication and the procedures service providers engage in when connecting communications. The Fifth Circuit court in *In re U.S. for Historical Cell Site Data* seems to have had high expectations for what mobile device owners are aware of when it opined that mobile device users voluntarily convey their cell-site data to law enforcement because they decide to "get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order . . . ."[188]

The expectations adopted by the Third Circuit and the Supreme Court of New Jersey in regards to what a mobile device owner knowingly exposes to the public when using the device are more realistic. The Third Circuit took a drastically different approach than that of the Fifth Circuit stating:

> A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all."[189]

Similarly, the Supreme Court of New Jersey is of the opinion that "[a]lthough individuals may be generally aware that their phones can be tracked, most people do not realize the extent of modern tracking capabilities and reasonably do not expect law enforcement to convert their phones into precise, possibly continuous tracking tools."[190] Because some mobile

188. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 614 (5th Cir. 2013).

189. *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317-18 (2010) (citing amici brief of the Elec. Frontier Found.).

190. New Jersey v. Earls, 70 A.3d 630, 643 (N.J. 2013).

device owners are certainly more knowledgeable than others in regards to what they are exposing to their service provider by using their mobile device, determining what a large group knows is likely impossible beyond speculating into generalities. Regardless of what the average mobile device user knows about what they are exposing by making a call or sending a message, the reality of the matter is that law enforcement obtains location data from mobile devices even where the owner or user takes no affirmative step,[191] such as dialing a call. As discussed in the background section of this Comment, mobile devices' location is recorded every seven seconds as long as the device is turned on,[192] GPS equipped mobile devices can be tracked in real time,[193] and mobile devices can be pinged without any action or knowledge on the part of the user as was the case in *United States v. Skinner* in order to reveal their location.[194] In theory, a mobile device user could be tracked without ever using the device other than to turn on the power button.[195] To say that by simply possessing a mobile device that is turned on, an individual has knowingly exposed their whereabouts to the public is a big leap from the Supreme Court holding that an individual knowingly exposes phone numbers they dial[196] and should not be accepted. To accept this leap gets away from the idea of an individual actually exposing something. When the defendant in *Smith* dialed numbers, all he conveyed to the company was the numbers he dialed.[197] He was not said to have conveyed a mountain of other information as a byproduct. Imagine a Christmas tree on display in a front room picture window. The tree's owner has clearly knowingly exposed that Christmas tree to the public, yet it would be absurd to say that by knowingly exposing the tree they have also knowingly exposed everything else in the home to the public. Following the same reasoning, it is illogical to say that by virtue of buying a product and perhaps not even using it in any meaningful way that an individual has somehow knowingly invited his service provider and accompanying law enforcement to chaperone his every move. It may sound elementary, but what a mobile device user knowingly exposes to the public, and therefore loses Fourth Amendment protections, should be limited to what has actually been knowingly exposed by the user to the service provider.[198]

---

191. *See id.* at 637.
192. *See id.*
193. *Id.*
194. United States v. Skinner, 690 F.3d 772, 776 (6th Cir. 2012).
195. *See Earls*, 70 A.3d at 637.
196. Smith v. Maryland, 442 U.S. 735, 744 (1979).
197. *Id.*
198. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

C. LOCATION DATA REVEALS INTIMATE INFORMATION ABOUT THE HOME

The Supreme Court has opined that "the Fourth Amendment protects people, not places."[199] Nonetheless, it is hard to ignore the special designation the Court has given to an individual's home in connection with the Fourth Amendment. The Court has stated "when it comes to the Fourth Amendment, the home is first among equals."[200] The Court's jurisprudence has made it clear that an individual's protections under the Fourth Amendment are at their height in the home.[201]

For example, in *United States v. Karo* the Court's holding turned upon the fact that the beeper entered the defendant's home revealing information to law enforcement that could not have otherwise been observed, which amounted to a search.[202] Further, the Court in *Karo* opined that as a general rule, searches of a home should be done pursuant to a warrant.[203] Similarly, in *Kyllo v. United States* law enforcement's use of thermal imaging equipment directed at a home was deemed an unreasonable search because all details within the home are intimate and "the entire area is held safe from prying government eyes."[204]

As discussed previously in this Comment, tracking of mobile devices, whether done via network based tracking or GPS tracking, can locate a mobile device to within a matter of feet or an individual room.[205] Homes are not exempt from this tracking ability.[206] Because mobile devices are only useful to their owners if they are at hand, they are usually located in close proximity to their owner. As a result, common sense dictates that mobile devices spend a large amount of time within homes because their owners do. Location data requests can seek data from months at a time, all but guaranteeing the device's location will be revealed within the owner's home at some point.[207] When law enforcement obtains location data that reveals a mobile device's location within a home, there can be little doubt that a search has occurred. This is a search because the location data has revealed intimate information about the interior of the home (the location of

---

199. *Id.*

200. Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); *see also* Kyllo v. United States, 533 U.S. 27, 31 (2001); Silverman v. United States, 365 U.S. 505, 511 (1961).

201. *Jardines*, 133 S. Ct. at 1414.

202. United States v. Karo, 468 U.S. 705, 715 (1984).

203. *Id.* at 718.

204. *Kyllo*, 533 U.S. at 37.

205. *See Hearing*, *supra* note 11, at 14-15, 22.

206. *See id.*

207. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (law enforcement compelled a service provider absent a warrant to turn over sixty days of location data emanating from a cell phone).

the mobile device and likely the owner's location) that would otherwise have been unknowable to law enforcement.[208] To hold that law enforcement is entitled to know where a suspect's mobile device is without first obtaining a warrant would render the Supreme Court's statement that "[i]n the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes"[209] hollow and erode the Court's position that searches of the home are to be done pursuant to a warrant.[210]

D. BUSINESS RECORD EXCEPTION IS OUTDATED

When the Fifth Circuit determined that warrantless gathering of location data by law enforcement to be constitutional in *In Re U.S. for Historical Cell Site Data*, the court based its ruling on the principle that location data is a business record maintained by service providers in their course of business.[211] This principle is founded in Supreme Court precedent holding that what an individual exposes to a third party, even if done confidentially, is not entitled to Fourth Amendment protections and may be acquired by law enforcement absent a warrant.[212] At first blush, this designation as business records appears reasonable because a mobile device owner when dialing a number can be said to have exposed the same thing as the defendant in *Smith* or by selecting as service provider may expose some information to the provider similar to that of the bank account holder in *Miller*.[213]

While this may seem reasonable at first blush, this precedent does not fit with modern advancements in technology.[214] It is important to note that the criticisms voiced at the time the Supreme Court adopted the business records doctrine still carry the same force today. For example, Justice Marshall doubted that individuals somehow give up all expectations of privacy by handing over something for a limited business purpose when he wrote, "Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[215] Justice William J. Brennan Jr. called

208. *Karo*, 468 U.S. at 715.
209. *Kyllo*, 533 U.S. at 37.
210. *Karo*, 468 U.S. at 718.
211. *In re U.S. for Historical Cell Site Data*, 724 F.3d at 611-12.
212. *Id.* at 610-12 (citing SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984); Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 440-41 (1976)).
213. *See Smith*, 442 U.S. 735; *Miller*, 425 U.S. 435.
214. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).
215. *Smith*, 442 U.S. at 749 (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 95-96 (1974) (Marshall, J., dissenting)).

into question how voluntary exposures to certain businesses really are given that many services have become nearly essential when he opined, "For all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[216]

The arguments made by these dissenting Justices apply equally to the issue of location data gathered from mobile devices. Following Justice Marshall's logic in *Smith*, it is reasonable that a mobile device owner (who may likely not know that his service provider can track his device twenty-four hours a day) would not expect that information to be shared with anyone else for purposes other than business, including the police.[217] This logic has carried the majority of the Court in other cases where the Court held that just because some information may have been exposed to a third party for a limited purpose did not grant police the right to access that information without a warrant.[218] The ability of landlords and hotel staff to access information that is kept private by their tenant or guest has not been extended to law enforcement just because the landlord or staff has that access.[219] If a landlord cannot reveal to police what his tenant keeps private, a service provider should not be allowed to reveal intimate private information about a customer without first obtaining a warrant.[220] To hold otherwise would reduce the Fourth Amendment privacy to the discretion of a landlord or, in this case, a service provider.[221]

Just as Justice Brennan found having a bank account essential for participation in contemporaneous economic life, the same can be said of mobile devices today.[222] It can be argued that for most Americans not having a mobile device is not an option because they are often necessary to stay in contact with work, finances, family, and to ensure safety as evidenced by the fact that ninety-one percent of Americans own them.[223] Interestingly, a similar number of American families have bank accounts at ninety-two percent, demonstrating that if a bank account can be considered essential so

---

216. *Miller*, 425 U.S. at 451 (citing Burrows v. Superior Court, 529 P.2d 590 (Cal. 1974) (Brennan, J., dissenting)).

217. *See Smith*, 442 U.S. at 749 (citing *Cal. Bankers Ass'n*, 416 U.S. at 95-96 (Marshall, J., dissenting)).

218. *See* Stoner v. California, 376 U.S. 483 (1964); Chapman v. United States, 365 U.S. 610 (1961).

219. *Stoner*, 376 U.S. 483; *Chapman*, 365 U.S. 610.

220. *Stoner*, 376 U.S. 483; *Chapman*, 365 U.S. 610.

221. *See Chapman*, 365 U.S. at 616-17.

222. United States v. Miller, 425 U.S. 435, 451 (1976) (citing Burrows v. Superior Court, 529 P.2d 590 (Cal. 1974) (Brennan, J., dissenting)).

223. *See* New Jersey v. Earls, 70 A.3d 630, 643 (N.J. 2013); Rainie, *supra* note 5.

can a mobile device.[224] To conclude that by simply owning a mobile device its owner has given up all expectations of privacy about where they go would be to hold privacy hostage at the expense of technology.[225] Under this perspective, mobile device purchasers are faced to choose between privacy and having a device they may find necessary to conduct their modern life. This is not a choice individuals should have to make.[226] Given the vast amount of information which service providers are privy to, the proper approach would be to keep information that has been exposed to them, only exposed to them.[227] Any other approach relegates an individual's privacy right to the level of record keeping a service provider chooses to engage in.

Nearly forty years ago, Justice Brennan recognized that new technological advancements posed a danger for individual privacy concerns and the necessity of the law to adapt to those dangers writing, "Development of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds. Consequently judicial interpretations of the reach of the constitutional protection of individual privacy must keep pace . . . ."[228] More recently, Justice Sotomayor has echoed this belief and gone as far as to say it may be time to reconsider the idea that individuals do not have a reasonable expectation of privacy in what is disclosed to third parties according to *Smith v. Maryland* and *United States v. Miller*.[229] Justice Sotomayor opined that the third party approach is not well suited to the digital age where individuals reveal a great amount of information to service providers by just going about everyday tasks.[230] Technology has certainly changed a great deal since the 1970s when *Miller* and *Smith* were decided. Rules that were promulgated in the age of pay phones, paper checks, and eight track tapes may need to be adjusted to suit technology that is approaching that appearing on the Jetsons.[231] If this chain of precedent does not change, individual privacy may become a piece of antiquated American tradition.

---

224. Bob Sullivan, *For Many US Households, Bank Account Is a Luxury*, NBC NEWS (Apr. 22, 2013), http://www.cnbc.com/id/100661088.

225. United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

226. *See* Smith v. Maryland, 442 U.S. 735, 749 (1979) (citing Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 95-96 (1974) ("Privacy is not a discrete commodity, possessed absolutely or not at all.") (Marshall, J., dissenting)).

227. *Id.*

228. United States v. Miller, 425 U.S. 435, 451-52 (1976) (citing Burrows v. Superior Court, 529 P.2d 590, 593-97 (Cal. 1974) (Brennan, J., dissenting)).

229. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

230. *Id.*

231. *Id.*

VII. CONCLUSION

Law enforcement is currently engaging in a practice of retrieving both historical and real time location data from service providers without first obtaining a search warrant based on probable cause.[232] It is not the position of this Comment that law enforcement should be kept from this location data altogether because this data is an invaluable resource in their battle against crime. This Comment is simply of the belief that law enforcement should first obtain a warrant based on probable cause before obtaining location data to ensure that individual's privacy interests are not violated.

The United States' Supreme Court has yet to weigh in on the topic, but several appellate level courts have recently addressed the constitutionality of law enforcement retrieving location data without a warrant and have reached different conclusions. The Fifth and Sixth Circuits have upheld the warrantless searches as constitutional but reached this conclusion on slightly different grounds.[233] The Supreme Court of New Jersey, in applying New Jersey law, found that law enforcement obtaining location data absent a warrant to be unconstitutional but, in doing so, they engaged in much of the same analysis as the Fifth and Sixth Circuits.[234]

The constitutionality of a warrantless search is largely determined by applying the two prong test first laid out by Justice Harlan in his concurring opinion in *Katz v. United States* and in the subsequent line of cases applying that test.[235] In applying the *Katz* test to law enforcement obtaining location data from service providers, it is the opinion of this Comment that the Fifth and Sixth Circuits erred in upholding the practice without a warrant. Mobile device users who do not wish to have their whereabouts known by the world or law enforcement should be viewed to have exhibited an expectation of privacy that society is prepared to recognize as reasonable.[236] Further, mobile device users should not be viewed to have knowingly exposed their location to the public, therefore losing Fourth Amendment protections of that information.[237] Additionally, location data obtained without a warrant can reveal intimate information about the interior of one's home that could not be otherwise observed by law enforcement.[238] The Supreme Court has determined that such intimate information about the interior of a home

---

232. *Cell Phone Location Tracking*, *supra* note 3.

233. *In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

234. New Jersey v. Earls, 70 A.3d 630, 645 (N.J. 2013).

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

236. *See id.*

237. *Id.*

238. *See* United States v. Karo, 468 U.S. 705, 715 (1984).

should only be obtained by law enforcement pursuant to a warrant.[239] This precedent should not be deviated from in regards to location data. Finally, Supreme Court precedent holding that information conveyed to a third party—even if confidential and done so for business purposes—is not protected under the Fourth Amendment and should be reconsidered as it is out of touch with the realities of modern society, where ninety-one percent of Americans own a mobile device.[240] If this precedent is not reconsidered, millions of Americans may be said to have no expectation of privacy in their location, simply due to the fact that they purchased a mobile device to keep up with the times and the demands of modern life.[241] Americans should not have to forfeit their privacy as a result of buying a product many likely consider to be essential.[242]

Law enforcement undoubtedly engages in warrantless location data gathering with the best of intentions: the intentions of fighting crime, ensuring national security, and curbing the trade of illegal narcotics. But good intentions do not alleviate the potential for abuse that the Fourth Amendment seeks to protect against. The words of Daniel Webster—a famous American diplomat, senator, and lawyer from well over a century ago—ring equally true today when he said:

> Good intentions will always be pleaded for every assumption of power ; but they cannot justify it, even if we were sure that they existed. It is hardly too strong to say that the Constitution was made to guard the people against the dangers of good intention, real or pretended. . . . There are men in all ages who mean to exercise power usefully ; but who mean to exercise it. They mean to govern well ; but they mean to govern. They promise to be kind masters ; but they mean to be masters.[243]

For now, the only way to be sure your mobile device is not serving as a de facto monitoring device that law enforcement can access without a warrant is to have the device turned off.[244] Before you turn that device back

---

239. *See id.*

240. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

241. *See* United States v. Miller, 425 U.S. 435, 451 (1976) (citing Burrows v. Superior, 529 P.2d 590 (Cal. 1974) (Brennan, J., dissenting)).

242. *Id.*

243. SPEECH DELIVERED BY DANIEL WEBSTER AT NIBLO'S SALOON IN NEW YORK, ON THE 15TH MARCH, 1837, at 17 (New York, Harper and Bros. 1837).

244. *See Cell Phone Location Tracking*, *supra* note 3.

on, be careful where you go because big brother may be looking no matter how hard you try to hide.[245]

245. *Id.*