Note – Alito’s Way: Application of Justice Alito’s Concurring Opinion in United States v. Jones to Cell Phone Location Data

Ryan Birss
Alito’s Way: Application of Justice Alito’s Concurring Opinion in *United States v. Jones* to Cell Phone Location Data

**Ryan Birss**

On January 23, 2012, the Supreme Court issued a landmark decision in *United States v. Jones*, ruling unanimously that the government’s installation of a GPS device on Antoine Jones’s vehicle and the use of that device to monitor the vehicle’s movements constituted a “search” and violated the Fourth Amendment. However, the majority opinion focused solely on the physical trespass of placing a device on a suspect’s car.

Due to advancements in technology such as cell phone location data, physical intrusion is unnecessary for government officials to track an individual. The limitations of the opinion were immediately apparent in cases like *United States v. Skinner*, as government agents circumvented the holding in *Jones* by merely avoiding physical trespass.

This Note argues that by focusing on Justice Alito’s concurrence in *Jones* and his three prongs of analysis (Fourth Amendment jurisprudence, the length of tracking, and the type of offense) and analyzing cell phone location data as something a person has a reasonable expectation of privacy in, courts can protect individuals from unchecked government intrusion.

This Note recaps the three opinions in *Jones*, summarizes the current technology and the procedures used by government agencies to access cell phone location data, and uses the facts of *Skinner* to illustrate how the surveillance process works. This Note then discusses Justice Alito’s concurrence in detail and proposes several modifications to his analysis in order to clarify when the warrantless collection of cell phone data should be deemed constitutional.

* J.D., University of California, Hastings College of the Law, 2013; Articles Editor, Hastings Law Journal. B.S., Political Science and Business Administration, University of Oregon, 2009. I would like to thank the editors of the Hastings Law Journal for their commitment and hard work in preparing my Note for publication. This Note is dedicated to my parents for their unwavering support throughout the Note writing process, law school, and most of all life in general. “If you will it, Dude, it is no dream.”

[899]
Table of Contents

Introduction ................................................................................................ 900

I. PROCEDURAL HISTORY AND THE THREE OPINIONS IN UNITED STATES
   V. JONES .......................................................................................... 903
   A. Facts .......................................................................................... 903
   B. Controlling Opinion .............................................................. 905
   C. Critique ..................................................................................... 905
   D. Alito’s Way .............................................................................. 906

II. OVERVIEW OF THE TECHNOLOGY IN UNITED STATES V. SKINNER.............. 908
   A. Technology: Cell Phone Location Data .................................... 908
   B. Technology: Pinging .................................................................. 910
      Access Location Data .................................................................. 911

III. UNITED STATES V. SKINNER ...................................................................... 914
   A. Facts ........................................................................................... 914
   B. Skinner’s Motion to Suppress and Subsequent Appeal .......... 916
   C. Opinion of the Sixth Circuit Court of Appeals ................... 916

IV. ALITO’S CONCURRENCE AND UNITED STATES V. SKINNER ..................... 918
   A. Existing Doctrine ................................................................. 919
   B. Length-of-Trip and Type-of-Offense .................................. 923

V. JUSTICE SOTOMAYOR: THE FIFTH VOTE? .................................................. 925

VI. REFINING ALITO’S WAY ......................................................................... 926
   A. Refining the Length-of-Trip Prong ..................................... 926
   B. Refining the Type-of-Offense Prong .................................. 927

Conclusion .................................................................................................. 927

Introduction

On January 23, 2012, the Supreme Court issued a landmark decision in United States v. Jones, ruling unanimously that the government’s installation of a global positioning system (“GPS”) device on Antoine Jones’s vehicle and the use of that device to monitor the vehicle’s movements constituted a “search” in violation of the Fourth Amendment. After this decision, the legal landscape regarding the use of GPS tracking devices changed fundamentally, but the Justices’ rationales for why a Fourth Amendment violation had occurred varied wildly. The controlling opinion in Jones, authored by Justice Scalia and joined by Chief Justice Roberts, Justice Kennedy, Justice Thomas, and

Justice Sotomayor, focused on the government’s physical occupation of private property for the purpose of obtaining information and that “such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.” In contrast, Justice Alito, who concurred in judgment and was joined by Justices Ginsburg, Breyer, and Kagan, focused on the *Katz* test and a person’s reasonable expectation of privacy.

*Jones* caused a “sea change” in law enforcement” that led the Federal Bureau of Investigation (“FBI”) to deactivate nearly 3000 GPS devices that were tracking suspects at the time. Andrew Weissmann, general counsel for the FBI, stated that it was not the “majority opinion that caused such turmoil in the bureau, but a concurring opinion written by Justice Samuel Alito.”

Justice Alito applied existing Fourth Amendment doctrine and reasoned that the Court should “ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.” Under this approach, he emphasized two important factors to consider when determining the reasonable expectation of privacy in location data: (1) the length of the monitoring, and (2) the nature of the underlying offense.

Justice Sotomayor filed a separate concurrence because she agreed that the physical intrusion was at a minimum a Fourth Amendment violation, but she also discussed the reasonable expectation of privacy, shifts in technology, and indicated a willingness to revisit the third-party doctrine. However, she expressly agreed that “at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’**

---

4. See id. at 958 (Alito, J., concurring); see also *Katz* v. United States, 389 U.S. 347 (1967) (holding that a search occurs when the government invades a person’s reasonable expectation of privacy). In *Katz*, government agents placed a listening device on a public payphone. *Id.* at 348. The Supreme Court found this to be a Fourth Amendment violation because the defendant did not subjectively believe that his phone conversation was being recorded, and society recognizes this subjective belief as reasonable. *Id.* at 361 (Harlan, J., concurring).
8. *Id.*
9. *Id.* at 954–56 (Sotomayor, J., concurring).
10. *Id.* at 955.
Nevertheless, soon after the landmark ruling, federal prosecutors chose to retry Jones by replacing the type of evidence offered to the court.\textsuperscript{11} The case against Jones remained fairly similar except that the unconstitutional GPS location data had been replaced with his cell phone location data.\textsuperscript{12} As this Note goes to print—in April 2014—Jones continues to sit in federal custody after representing himself and entering a plea bargain prior to his retrial.\textsuperscript{13} Although the Jones majority focused on the physical intrusion of the GPS device, the opinion did not govern cell phone location data because law enforcement did not commit a physical intrusion or trespass by tracking Jones’s cell phone.

In the midst of Jones, the Sixth Circuit Court of Appeals granted review to United States v. Skinner, a case involving warrantless cell phone tracking and cell phone location data.\textsuperscript{14} In Skinner, the Drug Enforcement Agency (“DEA”) used the defendant’s cell phone to track his movements along a three-day, multistate road trip as he transported 1000 pounds of marijuana.\textsuperscript{15} The Sixth Circuit held that there was no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data transmitted by his cell phone.\textsuperscript{16} The Sixth Circuit argued that the holding in Jones—that a Fourth Amendment violation occurs when the government installs a tracking device to monitor a vehicle’s movements—did not apply because the Skinner case lacked a similar physical intrusion.\textsuperscript{17} The Sixth Circuit’s rationale in Skinner illustrates the inherent limitations of Justice Scalia’s property-based majority opinion in Jones.

This Note argues that the Supreme Court should adopt Justice Alito’s concurring opinion as a framework to analyze cases concerning a person’s reasonable expectation of privacy in cell phone data. Based on

\textsuperscript{11} See Defendant’s Motion to Suppress Cell Site Data & Memorandum of Points and Authorities in Support Thereof at 6, United States v. Jones, No. 05-CR-386(1) (D.D.C Mar. 29, 2012), 2012 WL 1576673 (including allegations by Jones’s attorney that “the government seeks to do with cell site data what it cannot do with the suppressed GPS data”); see also Sarah Roberts, Court Says No GPS Tracking? How About Cell Phone Tracking?, ACLU Blog Rts. (Apr. 6, 2012, 12:55 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/court-says-no-gps-tracking-how-about-cell-phone (“[Instead of fixing the way it conducts this kind of invasive surveillance—[the government] has simply set its sights on another way to obtain people’s location information: their cell phones.”).
\textsuperscript{12} Roberts, supra note 11.
\textsuperscript{14} See generally United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), cert. denied, 133 S. Ct. 2851 (2013). For another example, see In re U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (“Cell site data are business records and should be analyzed under that line of Supreme Court precedent.”).
\textsuperscript{15} Skinner, 690 F.3d at 774.
\textsuperscript{16} Id. at 777.
\textsuperscript{17} Id. at 779–80.
her concurrence in Jones, Justice Sotomayor could provide the fifth vote to make this the majority opinion.  

Part II of this Note discusses the three opinions in Jones. Part III summarizes the current technology and the procedures used by government agencies to access cell phone location data. Part IV uses the facts of Skinner to illustrate how the surveillance process works. Part IV elaborates on the shortcomings of Skinner and discusses how Justice Alito’s concurrence in Jones provides a framework of three prongs to overrule it and similar cases. Part V notes that based on her concurrence in Jones, Justice Sotomayor could be the fifth vote to make Justice Alito’s opinion the majority. Finally, Part VI briefly proposes several modifications to Justice Alito’s analysis in order to clarify when the warrantless collection of cell phone data should be deemed unconstitutional.

I. PROCEDURAL HISTORY AND THE THREE OPINIONS IN UNITED STATES V. JONES

A. FACTS

In the fall of 2004, a FBI and the Metropolitan Police Department task force began investigating Antoine Jones, owner and operator of a nightclub in the District of Columbia, for trafficking narcotics. The government obtained a “warrant authorizing the use of an electronic tracking device on a Jeep Grand Cherokee registered to Jones’ wife.” A magistrate judge issued a warrant authorizing the installation of the device within ten days while the vehicle was located in the District of Columbia.

Eleven days after the warrant was signed, government agents surreptitiously installed a GPS device on the undercarriage of Jones’s vehicle while it was in Maryland, outside the District of Columbia. Using the device and signals from multiple satellites, the government tracked the vehicle’s movements for the next twenty-eight days. The device established the vehicle’s location within fifty to one hundred feet and

---

18. For a competing argument that Justice Alito’s concurring opinion is not helpful for future cases see Erin Murphy, Back to the Future: The Curious Case of United States v. Jones, 10 Ohio St. J. Crim. L. 325, 332 (2012) (“The greatest disappointment of the concurring opinion, therefore, is its refusal to even attempt a theory of Fourth Amendment applicability that would have buttressed the same ultimate holding, but with a test that might apply beyond the particular facts of this case.”).
20. Id.
21. Id.
22. Id.
23. Id.
communicated that location to a government computer. Over the next four-week period, the device transmitted more than 2000 pages of data.

After his indictment, Jones moved to suppress the evidence obtained from the warrantless use of the GPS device. Jones argued that the prolonged and constant tracking of his movements over the course of four weeks indicated that the search was unreasonable. On August 10, 2006, the district court denied Jones’s motion to suppress in part and held that the data obtained from the GPS device when Jones traveled on public roads was admissible.

The District Court for the District of Columbia relied on the Supreme Court’s holding in United States v. Knotts, a case involving a beeper device tracking a person traveling in a vehicle on a single trip on public thoroughfares. The court held that Knotts was binding precedent and equated the GPS device with the beeper despite the significant technological advancements since the Knotts holding in 1983. The court found Jones guilty for “conspiracy to distribute and possess with intent to distribute five kilograms or more of cocaine and 50 grams or more of cocaine base” and sentenced him to life in prison.

On August 6, 2010, Judge Douglas H. Ginsburg of the Court of Appeals for the District of Columbia reversed the district court’s decision, holding that the warrantless use of the GPS device on Jones’s vehicle for four weeks constituted a search and Knotts did not control. Judge Ginsburg pointed to the Supreme Court’s language regarding the limited use of the beeper in Knotts and held that it should not apply to the more comprehensive and sustained monitoring of Jones. He also recognized that, in Knotts, the Supreme Court specifically reserved the question of the constitutionality of warrantless twenty-four hour surveillance.

The Supreme Court granted the United States’ Petition for a Writ of Certiorari on June 27, 2011.

24. Id.
25. Id.
26. Id.
33. Id.
34. Id.
B. CONTROLLING OPINION

Justice Scalia authored the controlling opinion in Jones, which focused on the physical occupation of the private property for the purpose of obtaining information and that “such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.” The Court reasoned that Fourth Amendment jurisprudence had always been “tied to common-law trespass, at least until the latter half of the twentieth century.” The Court then shifted its analysis and incorporated the “reasonableness expectation of privacy” argument from Justice Harlan’s concurrence in Katz. Early in the twentieth century, the Court treated property rights as dispositive in determining the scope of the Fourth Amendment. Justice Scalia stated that the “Katz reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.”

Justice Scalia also asserted that the present facts before the Court did not require them to answer the question of whether an unconstitutional invasion of privacy could be achieved through electronic means without an accompanying physical trespass. Acknowledging that its opinion only addressed surveillance that involves a trespass, the majority wrote that “[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis.” Thus, the majority left cell phone tracking for another day, and its opinion is of limited value in analyzing future cases such as United States v. Skinner.

C. CRITIQUE

Legal scholars and, more importantly, Justice Alito, immediately criticized the limitations of the majority’s trespass-based holding for not

37. Id. at 949–50.
38. Id. at 950 (quoting Katz v. United States, 389 U.S. 347, 351 (1967) (Harlan, J., concurring)).
41. Id. at 954.
42. Id. at 953.
addressing the real issue regarding the intersection of privacy rights and advancements in technology. Justice Alito called the holding “unwise” as “[i]t strains the language of the Fourth Amendment; it has little if any support in current Fourth Amendment case law; and it is highly artificial.” He stated that the majority chose to decide this case involving twenty-first century surveillance techniques based on eighteenth-century tort law principals. Justice Alito wrote that it was impossible to imagine eighteenth-century situations that were analogous to the state’s tracking of Jones. Additionally, he compared Justice Scalia’s analysis to the pre-Katz cases and the emphasis that courts had placed on technical trespasses. Justice Alito criticized this approach because it placed a great significance on something that most people would think is a relatively minor aspect of the case: “attaching to the bottom of a car a small object that does not interfere in any way with the car’s operation,” instead of focusing on what was really important in the case—“the use of a GPS device for long-term tracking” and data collection.

D. Alito’s Way

Returning to traditional Fourth Amendment jurisprudence, Justice Alito focused on whether the FBI violated Jones’s reasonable expectation limitless, technologically powered government surveillance?”). But see Fabio Arcila, Jr., GPS Tracking Out of Fourth Amendment Dead Ends: United States v. Jones and the Katz Conundrum, 91 N.C. L. Rev. 1, 16–17 (2012) (stating “it is a mistake to treat the decision as a narrow one”). For a more expansive list of commentaries, see Daniel T. Pesciotta, I’m Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century, 63 Case W. Res. L. Rev. 187, 230–36 (2012).

44. Alito’s various critiques of the majority opinion included: (1) “[d]isharmony with a substantial body of existing case law,” (2) the majority “disregards what is really important,” (3) their approach provides incongruous results (amount of time tracking based on ownership of car), and (4) a variety in Fourth Amendment coverage for individuals in different states based on the community property laws of their home state. Jones, 132 S. Ct. at 961–62 (Alito, J., concurring).

45. Id. at 958.

46. Id. (“Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time in order to monitor the movements of the coach’s owner?”). But see id. at 950 n.3 (majority opinion) (including Justice Scalia’s response: “[I]t is quite irrelevant whether there was an 18th-century analog. Whatever new methods of investigation may be devised, our task, at a minimum, is to decide whether the action in question would have constituted a ‘search’ within the original meaning of the Fourth Amendment”).

47. Id. at 958 (Alito, J., concurring).

48. Id. at 959 (quoting Silverman v. United States, 365 U.S. 505, 509 (1961)) (“In the early electronic surveillance cases, the Court concluded that a Fourth Amendment search occurred when private conversations were monitored as a result of an ‘unauthorized physical penetration into the premises occupied’ by the defendant.”). But see Olmstead v. United States, 277 U.S. 438, 457 (1928) (holding that the Fourth Amendment did not apply because “[t]he taps from house lines were made in the streets near the houses”), and Goldman v. United States, 316 U.S. 129, 135 (1942) (holding that no search occurred where a “detectaphone” was placed on the outer wall of defendant’s office for the purpose of overhearing conversations held within the room).

of privacy.\textsuperscript{50} In \textit{Katz}, FBI agents attached an electronic listening and recording device to the outside of the public telephone booth that the petitioner used to place illegal gambling wagers.\textsuperscript{51} The Court concluded that the petitioner intended to exclude others from listening in on his conversation and that what a person knowingly exposes to the public is not subject to Fourth Amendment protection.\textsuperscript{52} Conversely, what one seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.\textsuperscript{53} Therefore, the government’s actions violated Katz’s reasonable expectation of privacy.\textsuperscript{54}

After \textit{Katz}, an individual’s property rights and a government trespass were no longer dispositive for a Fourth Amendment violation.\textsuperscript{55} Courts have concluded that application of \textit{Katz} to Fourth Amendment violations “depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.”\textsuperscript{56} Since \textit{Katz}, the two-factor analysis examines (1) whether a defendant displays conduct consistent with a subjective expectation of privacy, and (2) whether such subjective expectation is one that society, objectively, is willing to find reasonable to the point it would be adopted.\textsuperscript{57}

In analyzing Jones’s reasonable expectation of privacy, Justice Alito argued that the proper approach is to apply existing Fourth Amendment doctrine and “ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.”\textsuperscript{58} Under this approach, he emphasized the length of the monitoring and the nature of the offense.\textsuperscript{59}

According to Justice Alito, relatively short-term monitoring of a person’s movements on public streets, similar to those upheld in United States \textit{v. Knotts}, is reasonable because it does not involve a “degree of intrusion that a reasonable person would not have anticipated.”\textsuperscript{60} However, he stated that “the use of longer term GPS monitoring in

\textsuperscript{50} Jones, 132 S. Ct. at 958 (Alito, J., concurring).
\textsuperscript{51} 389 U.S. 347, 348 (1967).
\textsuperscript{52} Id. at 351–52.
\textsuperscript{53} Id.
\textsuperscript{54} Id. at 353.
\textsuperscript{55} See United States \textit{v. Jones}, 132 S. Ct 945, 960 (2012) (Alito, J., concurring) (quoting Oliver \textit{v. United States}, 466 U.S. 170, 183 (1984)) (“The existence of a property right is but one element in determining whether expectations of privacy are legitimate. The premise that property interests control the right of the Government to search and seize has been discredited.”); \textit{see also id} (quoting \textit{Kyllo v. United States}, 533 U.S. 27, 32 (2001)) (“We have since decoupled violation of a person’s Fourth Amendment rights from trespassory violation of his property.”).
\textsuperscript{56} Id. (quoting \textit{Rakas v. Illinois}, 439 U.S. 128, 143 (1978)).
\textsuperscript{57} \textit{Katz}, 389 U.S. at 361 (1967) (Harlan, J., concurring).
\textsuperscript{58} Jones, 132 S. Ct. at 964 (Alito, J., concurring).
\textsuperscript{59} Id.
\textsuperscript{60} Id. (citing United States \textit{v. Knotts}, 460 U.S. 276, 281–82 (1983)).
investigations of most offenses impinges on expectations of privacy.\textsuperscript{61} For these types of offenses, “society’s expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual’s car for a very long period.”\textsuperscript{62} Justice Alito did not conclude how long is too long, but that the surveillance “surely” became unconstitutional before the four-week mark.\textsuperscript{63} One scholar has called Justice Alito’s approach “revolutionary” for adding two new criteria to the Court’s analysis of an objective privacy expectation: (1) a “temporal limit on surveillance,” and (2) an “offense-specific distinction.”\textsuperscript{64}

Additionally, Justice Alito did not consider “whether prolonged GPS monitoring in the context of investigations involving extraordinary offenses would similarly intrude on a constitutionally protected sphere of privacy.”\textsuperscript{65} In extraordinary cases, Justice Alito stated that “long-term tracking might have been mounted using previously available techniques.”\textsuperscript{66} An offense-specific standard “provides an exception to Justice Alito’s temporal limit.”\textsuperscript{67}

While analyzing an expectation of privacy, Justice Alito focused on how technology can change those expectations and how “dramatic technological change may lead to periods in which popular expectations” are unsettled, resulting in “significant changes in popular attitudes” about privacy.\textsuperscript{68} He stated that one of the most significant technological changes was that “cell phones and other wireless devices now permit wireless carriers to track and record the location of users.”\textsuperscript{69} The DEA took advantage of Justice Alito’s concern about technological changes as they tracked suspects like Skinner without warrants.

II. Overview of the Technology in \textit{United States v. Skinner}

A. Technology: Cell Phone Location Data

Due to advancements in technology, the government does not need to physically intrude on a person’s property to track a person’s location.\textsuperscript{70} At the time of \textit{Jones}, there were more than 322 million wireless devices

\textsuperscript{61} \textit{Id.}
\textsuperscript{62} \textit{Id.}
\textsuperscript{63} \textit{Id.}
\textsuperscript{64} Arcila, Jr., supra note 43, at 42.
\textsuperscript{65} \textit{Jones}, 132 S. Ct. at 964 (Alito, J., concurring).
\textsuperscript{66} \textit{Id.}
\textsuperscript{67} For a critique of the offense-based analysis, see Arcila, Jr., supra note 43, at 66.
\textsuperscript{68} \textit{Jones}, 132 S. Ct. at 962 (Alito, J., concurring).
\textsuperscript{69} \textit{Id.} at 963.
in use in the United States.\(^{71}\) Network tracking has become increasingly precise due to congressional mandates to develop wireless location technology in order to enhance the nation’s emergency response system.\(^{72}\) For example, the Federal Communications Commission mandated that, as of September 11, 2012, “network-based tracking for 911 calls must be accurate to within 100 meters for 67 percent of calls and 300 meters for 90 percent of calls.”\(^{73}\)

At the time of Jones, almost thirty-six percent of households were “wireless only,” meaning they had no landline.\(^{74}\) One court stated that the “inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year.”\(^{75}\) Cell site data is “simply data sent from a cellular phone to the cellular provider’s computers.”\(^{76}\) Cell phones transmit radio signals to cell towers or cell sites when they are turned on so the radio signal data is cell site data.\(^{77}\) The modern state of this technology was examined in In re U.S. for Historical Cell Site Data.\(^{78}\) According to that court:

[Cell site data for a typical adult user will reveal between 20 and 55 location points a day. This data is sufficient to plot the target’s movements hour by hour for the duration of the . . . period covered by the government’s request. . . . If registration data were also collected by the provider and made available, as the Government has requested, such records would track the user on a minute by minute basis, compiling a continuous log of his life, awake and asleep, for [the] . . . period.]

As such, “the data can be utilized to ascertain the location of a cell phone and the user’s physical location if the user possesses the phone and the phone is turned on.”\(^{79}\) Thus, the government does not need to physically intrude on a person’s property to track their location because they can

---

73. Aaron Blank, The Limitations and Admissibility of Using Historical Cellular Site Data to Track the Location of a Cellular Phone, 18 Rich. J.L. & Tech., Fall 2011, at 1, 10 (referring to 911 Service, 47 C.F.R. § 20.18(h)(1) (2011)).
74. Wireless Quick Facts, supra note 71.
79. In re U.S. for Historical Cell Site Data, 747 F. Supp. 2d. at 835.
merely monitor a person’s movements by analyzing their cell phone location data.

In order for a cell phone to make and receive calls or transmit data, it must be in constant connection with the cellular network and nearby cellular towers. The proximity of cell towers varies by provider, by location, and over time. Additionally, the use of triangulation can enable analysts to achieve much greater precision and reduce the area in which a target is generated to improve accuracy of the technology. Additionally, the production of triangulation data cannot be disabled. As such, since the government rarely has to make a physical intrusion to gain access to this information, Jones provides no protection for this type of surveillance.

B. TECHNOLOGY: PINGING

Ping technology is routinely used by law enforcement officials to investigate and track suspects without the use of a search warrant. Ping occurs when the government calls the target’s cell phone in a manner that is undetectable to the cell phone user. By calling the phone, the government officers make the phone search for nearby cell towers so that the location of the phone can be recorded in the location data. As one court has explained:

Cellular service providers typically do not maintain records of the GPS coordinates of cellular telephones operating on their network, but the provider may generate such location data at any time by sending a signal directing the built-in satellite receiver in a particular cellular telephone to calculate its location and transmit the location data back to the service provider.

Ping is another example of technology not covered by Scalia’s property-based holding in Jones, as there is no physical trespass. However, Alito’s concurring opinion would likely give citizens some form of protection from this type of unchecked government intrusion. One

82. Susan Freiwald, Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact, 70 Md. L. REV. 681, 710 (2011) (citing Paul Bedell, Wireless Crash Course 28–31 (2d ed. 2005)).
83. Id. at 712.
84. Id. In addition to cell towers, there is the growing concern over the government’s use of “Stingray” technology, which “act[] as fake cell-phone tower[s] small enough to fit in a van [and] allow[[] for the government to collect cell information. See Hanni Fakhoury, When a Secretive Stingray Cell Phone Tracking “Warrant” Isn’t a Warrant, ELEC. FRONTIER FOUND. (Mar. 28, 2013), https://www.eff.org/deeplinks/2013/03/when-stingray-warrant-ist-warrant.
86. Freiwald, supra note 82, at 704.
87. Id. at 702.
example is Sprint Nextel’s history of providing law enforcement agencies with customer location data more than eight million times between September 2008 and October 2009. They provided law enforcement with a web portal to conduct automated “pings” to track users, which allowed government agents to simply type in a suspect’s phone number and obtain the GPS coordinates of the phone.


The Communications Assistance for Law Enforcement Act (“CALEA”) requires telecommunications providers to assist law enforcement officials in isolating certain “call-identifying” information, defined to include “dialing or signaling information that identifies the origin, direction, destination, or termination of a communication.” The major wireless carriers received more than 1.3 million requests from law enforcement in 2011 alone.

CALEA precludes the government from acquiring location information about the subscriber solely pursuant to pen register and trap and trace device statutes. However, CALEA provides an exception when the location may be determined from the telephone number itself, for example a landline that has an ascertainable address. To gain access to this location data, law enforcement agents must comply with the Electronic Communications Privacy Act of 1986 (“ECPA”).

“Title II of the ECPA created a new chapter of the criminal code dealing with access to stored communications and transaction records.” This portion of the statute is commonly referred to as the Stored Communications Act (“SCA”), and 18 U.S.C. § 2703 is

---

90. Id.
93. CARR & BELLIA, supra note 91, § 4:84.
94. Id.
essential to phone location data.\textsuperscript{98} “The SCA reflects Congress’s judgment that users have a legitimate interest in the confidentiality of electronic communications stored on third-party servers.”\textsuperscript{99} Section 2703 authorizes government access to stored communications or transaction records in the hands of third-party service providers.\textsuperscript{100} It covers content information, such as text messages and e-mails, and non-content information, such as logs made by a networker server and cell phone records.\textsuperscript{101}

For content, a distinction is made at the 180-day mark of storage. If the information has been stored for less than 180 days, then a warrant is required.\textsuperscript{102} The law triggers a different process (discussed below) if the information is stored for more than 180 days.\textsuperscript{103} The court order under this statute, “often referred to as a ‘2703(d)’ order or simply a ‘d’ order, is something like a mix between a subpoena and a search warrant.”\textsuperscript{104} These “d” orders can be used to gain access to cell phone location data.\textsuperscript{105}

Location data from cell phones is considered non-content. Courts have held that location data from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination that warrants require.\textsuperscript{106}

\begin{itemize}
\item \textsuperscript{98} Id.; 18 U.S.C. § 2703 (2014).
\item \textsuperscript{100} Id. at 581–82.
\item \textsuperscript{102} “A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures.” 18 U.S.C. § 2703(a) (emphasis added).
\item \textsuperscript{103} 18 U.S.C. § 2703(d).
\item \textsuperscript{104} Kerr, supra note 101, at 1219. For a chart organizing the differences in a clear way, see id. at 1223.
\item \textsuperscript{105} Id. at 1218.
\item \textsuperscript{106} In re Application of U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to Gov’t, 620 F.3d 304, 313 (3d Cir. 2010). Other courts have also concluded that a warrant is not needed for cell site location data, interpreting the Stored Communications Act (the “SCA”) as requiring only an administrative subpoena or a showing of reasonable grounds to obtain a court order for the disclosure. See e.g., In re U.S. for an Order Authorizing Release of Historical Cell-Site Info., No. 11-MC-0113, 2011 WL 679925 at *2 (E.D. N.Y. Feb. 16, 2011), abrogated by In re Smartphone Geolocation Data Application, No. 13-MJ-242, 2013 WL 5583711 (E.D.N.Y. May 1, 2013) (abrogated by Magistrate Orenstein, who had denied a similar request); United States v. Dye, No. 1:10-221, 2011 WL 1592555 at *9 (N.D. Ohio Apr. 27, 2011) (finding no reasonable expectation of privacy in cell phone records), aff’d, No. 11-3934, 2013 WL 4712733 (Sept. 3, 2013); United States v. Benford, No. 2:09-86, 2010 WL 1266597 at *3 (N.D. Ind. Mar. 26, 2010); In re U.S. for an Order Authorizing the Use of Two Pen Register & Trap and Trace Devices, 632 F. Supp. 2d 202, 211 (E.D.N.Y. 2008) (authorizing pen register trap and trace devices divulging cell site data only at the beginning and end of specific calls); United States v. Suarez-Blanca, No. CR-0023, 2008 WL 4200156 at *10 (N.D. Ga. Apr. 21, 2008). See generally Crim. Prac. Guide, supra note 78.
\end{itemize}
A court order . . . 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.\(^{107}\)

Hence, the government’s burden of proof has been lowered and only requires a “specific and articulable facts” standard.\(^{108}\) Under this standard, “the government may seek any information that is materially relevant to an ongoing investigation. . . . [including] acquisition of location data that will not yield evidence of crime but that instead will yield information that will aid the investigation.”\(^{109}\) The Judge will sign the order if she determines that a factual showing has been made.\(^{110}\) The Judge’s signed order is then served like an ordinary subpoena and a government investigator brings or faxes the Judge’s order to the telephone company, which produces the requested information.\(^{111}\)

However, under the SCA, any communication from a “tracking device” is excluded from the definition of “electronic communication.”\(^{112}\) Tracking devices are governed by 18 U.S.C. § 3117 and a warrant based on probable cause is required.\(^{113}\) Unfortunately, there is no clear standard and courts are split as to whether or not a cell phone can be considered a tracking device. A tracking device is defined as “an electronic or mechanical device which permits the tracking of the movement of a person or object.”\(^{114}\) Therefore, if the “electronic communication” sought under § 2703 is information derived from a device which “permits the tracking of movement of a person or object” that electronic communication cannot be obtained under § 2703.\(^{115}\) In contrast, if a cell phone is not a tracking device, the government can gather the information. Courts are split as to whether or not a warrant is required.\(^{116}\)

As no physical intrusion exists with these types of government


\(^{109}\) Freiwald, supra note 82, at 696–97.

\(^{110}\) Id.

\(^{111}\) Id.


\(^{114}\) Id.


\(^{116}\) For cases where warrant was required, see In re Application of U.S. for Orders Authorizing the Installation & Use of Pen Registers, 416 F. Supp. 2d 390, 397 (D. Md. 2006); In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756 (S.D. Tex. 2005); In re Application of U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. and/or Cell Site Info., 396 F. Supp. 2d 294, 304 (E.D.N.Y. 2005).
surveillance techniques, the Jones majority decision provides little protection. The application of these surveillance techniques is illustrated below as applied to Skinner.

III. United States v. Skinner

The limitations of the majority’s holding became apparent soon after Jones. The majority’s holding cannot reach cell phone location data, pinging, or “d” orders because no physical trespass takes place. The facts of Skinner show, however, that the government can essentially do the same type of surveillance that was held unconstitutional in Jones by replacing the GPS device with these nonphysical intrusion techniques.

A. Facts

In January 2006, the DEA began investigating a large-scale drug distribution network run by James Michael West for which Melvin Skinner worked as a courier.\(^\text{117}\) The investigation began after authorities pulled over another courier, Christopher S. Shearer, in Flagstaff, Arizona with $362,000.\(^\text{118}\) Police intercepted Shearer immediately before he attempted to deliver money to Philip Apodaca, West’s marijuana supplier.\(^\text{119}\) Shearer became a confidential informant and told the authorities how West operated his drug conspiracy.\(^\text{120}\)

The DEA learned that West purchased “pay-as-you-go” cell phones for the members of his network to facilitate safe communication.\(^\text{121}\) He provided false names and addresses for the phone subscriber information that were then programmed with contact information and given to the couriers to maintain communication.\(^\text{122}\) Skinner acted as a courier, delivering money to Arizona and then returning to Tennessee with hundreds of pounds of marijuana.\(^\text{123}\)

In June 2006, authorities determined that Skinner was using one of the “pay-as-you-go” cell phones to communicate with West.\(^\text{124}\) Authorities obtained a section 2703 order\(^\text{125}\) from a federal magistrate judge on July 12, 2006, “authorizing the phone company to release subscriber information, cell-site information, GPS real-time location, and ‘ping’ data” for the phone in order to learn Skinner’s location while he was transporting the


\(^{118}\) Id.

\(^{119}\) Id.

\(^{120}\) Id. For specifics, see Affidavit attached to Court Order, available at https://docs.google.com/file/d/1gr1bcSXbq7pXlj7GxaM5ywgsUg-hblBeuodjaSL5KcZtBQVbPbnKlr5Y/edit (last visited Mar. 12, 2014) [hereinafter Skinner Order].

\(^{121}\) Skinner, 690 F.3d at 775.

\(^{122}\) Id.

\(^{123}\) Id. at 775–76.

\(^{124}\) Id. at 775.

\(^{125}\) See supra Part II.B.
April 2014 |  

**CELL PHONE LOCATION DATA**

marijuana. The confidential informant provided most of the specific and articulable facts in an affidavit. The authorities asked for thirty days of historical data and sixty days real-time location and “ping” data. When it turned out that the first cell phone number was still in West’s possession in North Carolina, authorities then sought and obtained a second order from the magistrate judge to “ping” the second cell phone number and locate Skinner.

This information revealed that the cell phone was located near Flagstaff, Arizona. By continuously “pinging” the phone, the DEA learned that Skinner had departed Tucson, Arizona on Friday, July 14, 2006, and traveled on Interstate 40 across Texas. The agents did not follow the vehicle or conduct any type of visual surveillance at any time. With the magistrate judge’s authorization under the § 2703 order, the government agents received location information from the cell phone company to track the exact location of the vehicle that was carrying the load of marijuana. The information obtained from Skinner’s cell phone led the DEA agents to locate Skinner at a rest stop inside a motor home filled with more than 1100 pounds of marijuana.

DEA agents arrested Skinner and subsequently charged him with conspiracy to distribute and possession with intent to distribute in excess of 1000 kilograms of marijuana, conspiracy to commit money laundering, and aiding and abetting the attempt to distribute in excess of 100 kilograms of marijuana. After a ten-day trial, the jury found Skinner guilty on all counts.

---

126. *Skinner*, 690 F.3d at 776. See, e.g., *Skinner Order*, supra note 120; see also Jennifer Granick, *UPDATED: Sixth Circuit Cell Tracking Case Travels Down the Wrong Road*, CTR. FOR INTERNET & SOC’y (Aug. 14, 2012 9:24 PM), http://cyberlaw.stanford.edu/blog/2012/08/updated-sixth-circuit-cell-tracking-case-travels-down-the-wrong-road (“The orders show that the court authorized pinging and GPS tracking on a real time basis under 18 USC 2703(c)(1)(B) and 2703(d). ‘Whoa’, you are saying to yourselves. ‘You mean, the court authorized real time tracking based on a provision of the Stored Communications Act, without even a reference to the Pen Register statute or CALEA? That can’t be right.’ Well, its not right, but that’s what the Court did.”).


128. Id. at 2.

129. *Skinner*, 690 F.3d at 776.

130. Id.

131. See supra Part II.A.

132. *Skinner*, 690 F.3d at 776.

133. Id.

134. Id. at 779.

135. Id. at 774.


137. Id. at 777.
B. Skinner’s Motion to Suppress and Subsequent Appeal

Skinner moved to suppress the search of the motorhome pursuant to a violation of the Fourth Amendment, arguing that the government agents’ use of GPS location information was a warrantless and unconstitutional search. At an evidentiary hearing, the magistrate judge:

[O]pined that because the cell phone was utilized on public thoroughfares and was ‘bought by a drug supplier and provided to . . . Skinner as part and parcel of his drug trafficking enterprise,’ Skinner did not have a legitimate expectation of privacy in the phone or in the motorhome that was driven on public roads.

Furthermore, the magistrate judge recommended that Skinner’s motion be rejected because he lacked standing for not subscribing to the cell phone plan in his own name.

On appeal to the Sixth Circuit, Skinner argued that:

[The government’s request for cell site location information, along with real time GPS data and ‘ping’ data . . . in regard to the cellular telephone in Skinner’s possession was based on the Stored Communications Act found at 18 U.S.C. § 2701 et seq. This type of information is considered prospective, as opposed to historical; and is not subject to disclosure pursuant to 18 U.S.C. § 2703.

Rather, Skinner proposed that the monitoring of cell site location information, GPS data, and ping data are types of electronic surveillance, and searching such information requires a warrant pursuant to the Fourth Amendment.

C. Opinion of the Sixth Circuit Court of Appeals

The Sixth Circuit rejected Skinner’s appeal of the district court’s denial of the motion to suppress. The Sixth Circuit held that there was no Fourth Amendment violation because “Skinner did not have a reasonable expectation of privacy in the data” transmitted by his voluntarily procured pay-as-you-go cell phone. Thus, the court held that “suppression was not warranted and the district court correctly denied Mr. Skinner’s motion to suppress.” Additionally, the court reasoned that a criminal cannot be “entitled to rely on the expected

138. Id. at 776.
139. Id.
142. Skinner, 690 F.3d at 777.
143. Id.
144. Id. at 781.
untrackability of his tools.” The court stated that if a device used to transport contraband gives off a signal that can be tracked for location, the police can track the signal.

The court stated that its opinion was consistent with United States v. Knotts. Similar to Knotts, Skinner “travel[ed] on a public road before he stopped at a public rest stop.” Although the cell site information aided the police in determining Skinner’s location, that same information could have been obtained through visual surveillance. The court stated:

Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen. The recent nature of cell phone location technology does not change this. It follows that Skinner had no expectation of privacy in the context of this case, just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car’s paint.

The court also emphasized that it stayed consistent with Fourth Amendment jurisprudence, as “the government never had physical contact with Skinner’s cell phone; he obtained the phone, GPS technology and all, and could not object to its presence.”

Also, the court reasoned that because the cell site data is simply a substitution for Skinner’s visually observable location, he had “no legitimate expectation of privacy in his movements along public highways” and “the Supreme Court’s decision in Knotts is controlling.”

The court went on to discuss United States v. Jones and distinguished the case on two grounds. First, discussed in Part II, the Jones majority based its decision on the fact that the police had to “physically occup[y] private property for the purpose of obtaining information,” which was not present in this case. Second, the Sixth Circuit distinguished the case

145. Id. at 777. But see Gelb, supra note 85, at 30 (“Ironically, it appears the Sixth Circuit perceived the defendant’s use of a prepaid or “pay-as-you-go” cell phone as evidence of defendant’s subjective intent not to be followed.”).
146. Skinner, 690 F.3d at 777.
147. Id. (citing United States v. Knotts, 460 U.S. 276 (1983)).
148. Id. at 778.
149. Id. at 778-79.
150. Id. at 777; cf. Recent Cases, Criminal Procedure—Fourth Amendment—Sixth Circuit Holds that “Pinging” a Target’s Cell Phone to Obtain Gps Data Is Not a Search Subject to the Warrant Requirement—United States v. Skinner, 126 Harv. L. Rev. 802, 806 (2013) [hereinafter Recent Cases] (“To revise one of the Sixth Circuit’s analogies, it was as if the police could somehow remotely force an otherwise odorless suspect to create a scent for the dogs to follow.”).
151. Skinner, 690 F.3d at 781.
152. Id. at 779 (quoting United States v. Forest, 355 F.3d 942, 951–52 (6th Cir. 2004), vacated, 543 U.S. 1100 (2005)).
153. Id.
154. Id. at 780 (quoting United States v. Jones, 132 S. Ct. 945, 949 (2012)).
from Justice Alito’s concurrence as “Jones involved intensive monitoring over a 28-day period, here the DEA agents only tracked Skinner’s cell phone for three days.” The Skinner Court analyzed Justice Alito’s opinion and stated that there was no “extreme comprehensive tracking” in the case before them. Therefore, the Sixth Circuit held that the Jones holding did not apply.

IV. Alito’s Concurrence and United States v. Skinner
Before analyzing Justice Alito’s opinion, it is important to review the text of the Fourth Amendment:

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.

As the Supreme Court once wrote, “the familiar history of the Amendment need not be recounted here, we should remember that it reflects a choice that our society should be one in which citizens ‘dwell in reasonable security and freedom from surveillance.’”

As the Supreme Court has also noted that “[t]he point of the Fourth Amendment, which often is not grasped by zealous officers, is not that it denies law enforcement the support of the usual inferences which reasonable men can draw from evidence.” Rather, the Fourth Amendment “require[s] that those inferences be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the often competitive enterprise of ferreting out crime.” Furthermore, citizens like Jones, Skinner, and others suspected of drug offenses are no less entitled to Fourth Amendment protections than those suspected of non-drug offenses.

In analyzing Skinner’s reasonable expectation of privacy—and other cases involving cell phone location data—Justice Alito would apply existing Fourth Amendment doctrine and “ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.” He would also consider the length of the monitoring and the nature of the suspect’s underlying

155. Id.
156. Id.
157. Id. at 780–81.
158. U.S. Const. amend. IV.
161. Id. at 14.
After analyzing these three prongs of Justice Alito’s concurrence in Jones, this Note asserts that he would hold that the type of surveillance in Skinner violates a suspect’s reasonable expectation of privacy.

A. EXISTING DOCTRINE

Justice Alito focuses on the Katz test when discussing existing Fourth Amendment doctrine. This Note asserts that the Skinner court incorrectly applied the Katz test, which has been modified and refined by cases like United States v. Knotts, and ignored United States v. Kyllo entirely.

In Katz, the Supreme Court held that the Fourth Amendment "protects people, not places." Further elucidating this concept, Justice Harlan’s concurrence set forth a two-part test to determine whether an individual has a reasonable expectation of privacy. First, a person must have “exhibited an actual . . . expectation of privacy and, second, the expectation must be one that society is prepared to recognize as reasonable.”

Subsequently, the Court applied and refined the Katz test when it held that “a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another” because he voluntarily has shown his progress and route to anyone that wants to look. In Knotts, the police placed a beeper in a container and monitored its movements along a single drive by Knott’s co-conspirator from the chemical factory to Knott’s home. The Court acknowledged the government’s limited use of this particular beeper. The Court reasoned that a police car following at distance throughout the co-conspirator’s journey “could have observed him leaving the public highway and arriving at the cabin owned by

164. Id.
165. Id. at 960.
167. 533 U.S. 27 (2001) (holding that a Fourth Amendment violation occurs when the government gains access to a constitutionally protected area by using a device or technology that is not available to the common public). In Kyllo, government agents used a thermal imaging device to detect high levels of infrared radiation inside defendant’s home. Id. at 31. The agent inferred that the defendant was using halide lights to grow marijuana. Id. The government then used the information obtained from the thermal imaging device to secure a warrant and subsequently prosecuted the defendant for manufacturing marijuana. Id.
169. Id. at 361 (Harlan, J., concurring).
170. Id.
172. Id. at 278.
173. Id. at 284–85.
respondent, with the drum of chloroform still in the car.” As such, the defendant did not have a reasonable expectation of privacy because his public movements were potentially observable.

The *Skinner* court tried to analogize its facts with those of *Knotts*. *Skinner* was immediately criticized as a “good example of how legal precedent, although ever-evolving, is not necessarily progressing in lock step with technology and the realities of the ways in which it is being embraced by modern society.” It was also critiqued as a “troubling development” in post-Jones jurisprudence. For example, the court stated that because of the criminal nature of Skinner’s activities, he “had no expectation of privacy . . . just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car’s paint.” But “[t]his analysis neglects the objective prong of the reasonable-expectation-of-privacy test—whether society would accept as reasonable the fugitive’s and getaway driver’s purported beliefs that they had ‘gotten away unseen.’” This lack of analyzing the objectivity prong contrasts with Justice Alito’s approach of relying on existing Fourth Amendment doctrine.

The court then stated that *Knotts* supported this rationale because “[s]imilar to the circumstances in *Knotts*, Skinner was traveling on a public road before he stopped at a public rest stop.” The court argued that these situations were parallel because the cell site information that aided the police in determining Skinner’s location could have been obtained through visual surveillance. The timing of the government’s use of surveillance in its investigation is one important distinction between *Knotts* and *Skinner*. In Skinner’s case:

> [P]olice had not and could not establish visual contact with Skinner without utilizing electronic surveillance because they had not yet identified the target of their search. Authorities did not know the identity of their suspect, the specific make and model of the vehicle he would be driving, or the particular route by which he would be traveling.

---

174. *Id.* at 285.
175. *Id.*
179. *Skinner*, 690 F.3d at 777.
182. *Id.*
183. *Id.* at 786 (Donald, Circuit Justice, concurring).
This is in sharp contrast to the investigation in *Knotts*, as the police watched the defendant make a purchase, followed his car in which the contraband had been placed, and maintained contact by using both visual surveillance and the tracking device. \(^\text{184}\)

The type of technology used is another distinction between the surveillance in *Knotts* and *Skinner*. The Sixth Circuit in *Skinner* erroneously equated modern day cell location data with a police beeper. Courts should not equate cell phone location data with beepers due to the advancements in technology discussed in Part III. The prolonged collection of cell location data is much more advanced than the *Knotts* beeper. In *United States v. Karo*, the Supreme Court explained that the beeper technology is not even accurate enough to determine in which storage locker the suspect had stored the bugged drum.\(^\text{185}\) Additionally, the Court noted in *Knotts* that the beeper provided limited information and the signals were periodically lost.\(^\text{186}\)

[The beepers used in *Knotts* and *Karo* were simple radio transmitters of limited range that forced the agents tracking the device to stay in close physical proximity to the device. In contrast, the functionality of the cell phone data is essentially unlimited by any distance between device and agent. Additionally, the beeper device only provides low-resolution directional information, including the approximate angle between the receiver and the beeper and the approximate distance as judged by signal strength.\(^\text{187}\)

Another distinction between cell phone data and the information collected from a beeper is the amount of detail that these devices can accumulate.\(^\text{188}\)

Location information reveals everything from daily habits like stopping at the same coffee shop on the way to work, to associations with other people, to visits to locales that reveal much more about a person’s particular characteristics, affiliations or beliefs—such as a gay bar, a doctor’s office, HIV testing facility, or abortion clinic; a certain church,

---


\(^{186}\) Knotts, 460 U.S. at 278.


\(^{188}\) See infra note 220. This is commonly referred to as the “mosaic theory.” See Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 Mich. L. Rev. 311, 320 (2012) (“The mosaic theory requires courts to apply the Fourth Amendment search doctrine to government conduct as a collective whole rather than in isolated steps. Instead of asking if a particular act is a search, the mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group. The mosaic theory is therefore premised on aggregation: it considers whether a set of nonsearches aggregated together amount to a search because their collection and subsequent analysis creates a revealing mosaic.”)
synagogue, or mosque; a strip club; or various political and civic organizations.  

The *Knotts* and *Karo* beepers did not have the capacity to collect such details or save data that could later be analyzed by government agents.  

The *Knotts* Court acknowledged that the use of beepers is limited, primarily because it only assisted the agents in tracking the suspect during a single trip.  

The Court explicitly did not address whether surveillance such as “twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision” was constitutional.  

The *Knotts* Court held that, if long-term surveillance should eventually occur, there would be enough time to determine whether different constitutional principles may be applicable.  

The Court dismissed the respondent’s concern that its decision would lead to the endorsement of warrantless twenty-four hour tracking of individuals.  

This is much different than the DEA agents who had to sit back and “ping” Skinner’s phone to gather information because they never had to physically follow him. Also, *Knotts* involved a shorter trip than Skinner’s three-day journey from Arizona to Texas.  

Furthermore, although the *Jones* Court never discussed *Kyllo*, “opinions like *Skinner* appear to be in conflict with those like *Kyllo*.”  

This Note suggests that Justice Alito’s analysis would lead to the conclusion that *Skinner* is inconsistent with the Supreme Court precedent established in *Kyllo*.  

In *Kyllo*, the government used a thermal-imaging device to look inside a house to determine if marijuana grow lamps were giving off heat.  

There, the Court held that a search occurred when sense-enhancing technology revealed “any information regarding the home’s interior that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’ . . . at least where . . . the technology in question is not in general public use.”  

In *Skinner*, mining for location data was not a method of observation available to members of the public, unlike a camera used for

---

192. *Id.* at 283–84.  
193. *Id.*  
194. *Id.*  
196. *Id.* at 31. *Cf.* Arcila, Jr., *supra* note 43, at 72–73. (“The dramatic impact that this Kyllo factor would have had—combined with its complete failure to make any appearance whatsoever—potentially calls into question its continued viability.”).  
198. *Id.* at 34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).
aerial mapping. As such, it is important to craft a rule that does not leave U.S. citizens “at the mercy of advancing technology . . . that could discern all human activity.” Unbridled access to cell location data has the potential to discern a significant portion of a person’s activities.

Citizens do not have access to other people’s cell location data. The SCA states that entities in possession of this type of data shall not disclose it to anyone without meeting an enumerated exception outlined in the statute. As such, “no random member of the public could” have requested and received Skinner’s cell data from his “cell phone company for the right to track [his] location.” Members of the general public could not even subpoena the phone companies to get this type of data. Only government agents can use orders under section 2703 of the SCA to request this information. The Sixth Circuit should have considered that the general public does not have access to cell phone location data when determining Skinner’s reasonable expectation to privacy.

B. Length-of-Trip and Type-of-Offense

According to Justice Alito’s analysis, “relatively short-term monitoring of a person’s movements on public streets,” similar to those upheld in Knoits, is reasonable. However, Justice Alito wrote that “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.” For these types of offenses, “society’s expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual’s car for a very long period.” He did not conclude how
long is too long, but that the surveillance surely became unconstitutional before the four-week mark.209 “Justice Alito’s temporal limit frees ‘relatively short-term monitoring’ from Fourth Amendment oversight but extends Fourth Amendment protections to ‘longer term GPS monitoring.’”210 Prior to Jones, many lower courts also struggled with GPS monitoring and how long the monitoring must last before it becomes unreasonable.211

However, courts will likely continue to struggle with Jones because Justice Alito’s concurrence unfortunately provides little guidance “about how to resolve Fourth Amendment privacy claims apart from its crucial distinction between brief and prolonged GPS tracking.”212 Some have even said that his analysis is not helpful because “it offered only a single paragraph of analysis in determining that four weeks was too long.”213 Similarly, the Skinner Court found Justice Alito’s concurrence inapplicable because the Jones case “involved intensive monitoring over a 28-day period . . . [as opposed to] the DEA agents [who] only tracked Skinner’s cell phone for three days.”214

Despite the flaw of establishing no clear line between brief and prolonged tracking, Justice Alito could consider other factors of the surveillance in Skinner to determine that the tracking was too long. He could take into account factors such as the distance of the surveillance, whether it was around the clock, and whether it crossed different jurisdictions.215 Justice Scalia’s property-based rationale is silent in regard to these additional factors as they are irrelevant to physical trespass. In contrast, Justice Alito’s analysis leaves open the possibility to include these factors when examining a person’s reasonable expectation of privacy in their cell phone location data.

Besides the length of the offense, Justice Alito considers the type of underlying offense. Jones and Skinner’s offenses are similar because they both involve drug conspiracies. As such, Skinner’s offense would not fit into Justice Alito’s exception involving investigating extraordinary

---

209. Id.
210. Arcila, Jr., supra note 43, at 44.
211. See, e.g., United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010) (holding that twenty-eight days was too much), aff’d in part sub nom. United States v. Jones, 132 S. Ct. 945 (2012). But see United States v. Cuevas-Perez, 640 F.3d 272, 274 (7th Cir. 2011) (holding that sixty hours was not enough), vacated, 132 S. Ct. 1534 (2012); United States v. Hernandez, 647 F.3d 216, 221 (5th Cir. 2011) (raising a theoretical concern about GPS monitoring, but distinguishing itself from Maynard based on the length of the trip and the surveillance not being around the clock).
212. Arcila, Jr., supra note 43, at 45.
214. United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012), cert. denied, 133 S. Ct. 2851 (2013). However, length of trip is not the only factor and Justice Alito’s analysis would not change solely on the trip lasting three days.
215. See infra Part VI.A.
April 2014

CELL PHONE LOCATION DATA

925

offenses. In extraordinary cases, Justice Alito stated “long-term tracking
might have been mounted using previously available techniques.”
Furthermore, in Justice Sotomayor’s “statement of agreement with Justice
Alito that long term monitoring impinges expectations of privacy, Justice
Sotomayor qualified her statement as applicable to ‘most offenses.’”
However, Justice Alito’s concurrence would still be applicable because
_Skinner_ does not deal with an extraordinary offense.

V. JUSTICE SOTOMAYOR–THE FIFTH VOTE

For “Alito’s Way” to become a majority opinion, he needs one
more vote, as four Justices have already signed on to his concurrence.
Justice Sotomayor is the most likely fifth vote because her concurring
opinion has a much broader interpretation of an individual’s reasonable
expectation to privacy. There is a much stronger chance to overturn the
Sixth Circuit with Justice Alito’s framework because there is no guarantee
a majority of the current Justices would adopt Justice Sotomayor’s ideas,
especially revisiting the third-party doctrine. Justice Sotomayor agreed
that the physical intrusion is a Fourth Amendment violation at a
minimum but also discussed the reasonable expectation of privacy, shifts
in technology, and a willingness to revisit the third-party doctrine, as that
approach is ill-suited to the digital age. She also alluded to the
adaptation of the mosaic theory of a reasonable expectation of privacy
when discussing GPS surveillance because it “generates a precise,
comprehensive record of a person’s public movements that reflects a
wealth of detail about her familial, political, professional, religious, and
sexual associations.” However, she expressly agreed that, “at the very

216. _Jones_, 132 S. Ct. at 964 (Alito, J., concurring).
217. Murphy, _supra_ note 18, at 337 (quoting _Jones_, 132 S. Ct. at 954 (Sotomayor, J., concurring)).
218. For general critical discussions of the third-party doctrine, see Katherine J. Strandburg,
_Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change_, 70 Mil.
219. _Jones_, 132 S. Ct. at 957 (Sotomayor, J., concurring).
220. _Id._ at 955. (Sotomayor, J., concurring). This is commonly referred to as the “mosaic theory.”
least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy’” and would agree with Justice Alito’s interpretation.221

VI. REFINING ALITO’S WAY

Justice Alito’s concurrence has prompted two common critiques: that it (1) does not define what period of surveillance is too long, and (2) does not define which types of offenses are extraordinary.222 This Part briefly refines these two elements223 and provides suggestions to future courts that employ Justice Alito’s opinion to determine when the collection of warrantless cell phone location data becomes unconstitutional.

A. REFINING THE LENGTH-OF-TRIP PRONG

Justice Alito focused on the number of days to determine when surveillance lasts too long. This Note proposes that courts should adopt a multi-factor test and look at the totality of the circumstances surrounding the surveillance in dispute. Based on the language of Justice Alito’s opinion, the number of days would be the most important factor. A court should also strongly consider Justice Alito’s language that the surveillance should be similar to the type upheld in Knotts and ask: Did the government agents ever have any visual contact? This is an important factor because it concerns allocation of government resources and provides guidance as to his thinking because he had earlier emphasized that, prior to technological advances, practical resource constraints had limited the amount and intrusiveness of governmental searches, with the government choosing to make special efforts only in rare and significant cases.”224 Courts could also consider factors such as the distance of the surveillance, whether it was around the clock, and whether it crossed jurisdictions.

In Skinner’s case, Justice Alito could consider the fact that the DEA never conducted any visual surveillance.225 Also, he could take into account the overall distance. In this case, the DEA monitored Skinner as he drove from Tucson, Arizona, to Abilene, Texas.226 This warrantless tracking lasted for more than 760 miles.227 A final fact to consider is that the tracking crossed state lines. When considering these various factors,

---

221. Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring).
222. See supra notes 18, 196.
223. See supra Parts V.B–C.
226. Id.
227. See Driving Distance from Tucson, AZ., to Abilene, TX., TRAVEL.MATH, http://www.travelmath.com (Use “Travel Calculator” on homepage; then search “Get” for “driving distance”, search “From” for “Tucson, AZ” and search “To” for “Abilene, TX”; then follow “Calculate” hyperlink).
the tracking in *Skinner* would likely satisfy the “length-of-trip” prong of Justice Alito’s concurrence.

**B. Refining the Type-of-Offense Prong**

As discussed in Subpart VI.C, Jones and Skinner had committed similar offenses involving drug trafficking conspiracies. This Note proposes that Justice Alito’s “extraordinary offenses” would rarely include the surveillance of criminal enterprises in the smuggling and trafficking of contraband such as drugs, weapons, or counterfeit goods.

*Jones* and *Skinner* illustrate this proposal. In *Jones*, although the agents applied for a warrant, they did not follow the magistrate judge’s guidelines. Both of these cases involved ongoing investigations with multiple parties that most likely took a substantial amount of time to thoroughly investigate. In this regard, there was ample opportunity for the government agents to make a probable cause showing and for determinations to access Skinner’s cell phone location data “be drawn by a neutral and detached magistrate instead of being judged by the officer engaged in the ‘often competitive enterprise of ferreting out crime.’” Justice Alito would likely require a warrant in these circumstances.

In contrast, this Note hypothesizes that courts would find that the definition of an extraordinary offense includes exigent circumstances. One example would be the kidnapping of a child. If there was an “Amber Alert” issued after a child had been kidnapped and the police had a suspect, the police should be able to immediately request the suspect’s cell phone location data to help track the suspect. One scholar has also argued that terrorism would fit into Justice Alito’s extraordinary offense analysis as well. As the *Skinner* case does not include these types of facts, his alleged crimes would not be extraordinary offenses and Skinner would have a reasonable expectation of privacy in his cell phone location data.

**Conclusion**

The Sixth Circuit’s rationale in *Skinner* illustrates the inherent limitations of Justice Scalia’s property-based holding in *Jones*. As this Note has discussed, technologies like pinging and cell phone location data make it unnecessary for government officials to place a GPS on a suspect’s car if they want to track the suspect. By focusing on Justice Alito’s concurrence and his three prongs of analysis (Fourth Amendment jurisprudence, the length of tracking, and the type of offense), courts can protect individuals like Skinner and Jones from unchecked government intrusion.

---

228. See supra Part I.A.
229. See supra Part III.A.
231. Arcila, Jr., supra note 43, at 68.
intrusion. Although the majority opinion may ultimately be of limited value in protecting the privacy interests of Americans as technology such as cell phone location data makes physical intrusions obsolete, courts can correct this by using “Alito’s Way” to hold that individuals have a reasonable expectation of privacy in their cell location data.

232 Phillip Smith & Clarence Walker, How Can a Man Who Won an Appeal, and a Major Supreme Court Case, Still be Locked Up for Life?, ALTERNET (Mar. 6, 2012), http://www.alternet.org/story/154394/how_can_a_man_who_won_an_appeal_and_a_major_supreme_court_case_still_be_locked_up_for_life (reporting that Jones said after his victory at the Supreme Court, “I am very happy with the Supreme Court decision and I hope the decision helps millions of Americans preserve their right to have reasonable expectation of privacy”).