### University of Cincinnati Law Review

Volume 82 | Issue 1 Article 5

September 2014

# GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis

Marc McAllister

Follow this and additional works at: https://scholarship.law.uc.edu/uclr

#### **Recommended Citation**

Marc McAllister, *GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis*, 82 U. Cin. L. Rev. (2014)

Available at: https://scholarship.law.uc.edu/uclr/vol82/iss1/5

This Article is brought to you for free and open access by University of Cincinnati College of Law Scholarship and Publications. It has been accepted for inclusion in University of Cincinnati Law Review by an authorized editor of University of Cincinnati College of Law Scholarship and Publications. For more information, please contact ronald.jones@uc.edu.

## GPS AND CELL PHONE TRACKING: A CONSTITUTIONAL AND EMPIRICAL ANALYSIS

#### Marc McAllister\*

I. Introduction	207
II. Supreme Court Cases on GPS and Electronic Tracking	
A. The Law of Electronic Tracking Pre-Jones	214
B. United States v. Jones	216
III. Lower Court GPS Tracking Cases Post-Jones	221
A. GPS Tracking Accomplished by Way of Trespass	221
B. GPS Tracking Accomplished Without Trespass: Cell	
Phone Tracking	224
IV. Survey Results	235
A. Overall Survey Design	
B. GPS Tracking Survey	237
1. Variations Based on the Type of Suspect	238
2. Variations on the Permissible Length of	
Surveillance	240
C. Cell Phone Tracking Survey	242
1. Survey Results	243
2. Conclusions	246
V. A Sliding Scale Framework for Cell Phone and GPS Tracking	247
A. Proposal Details	250
1. Those Suspected of Severe Crimes	250
2. Those Suspected of Minor Crimes	252
3. Those Not Suspected of Any Crime	252
B. Support for this Proposal	253
VI. Conclusion	256

#### I. INTRODUCTION

In *United States v. Jones*,<sup>1</sup> the United States Supreme Court ruled that the Fourth Amendment is violated when police, without a warrant, attach a Global–Positioning–System (GPS) device to a suspect's vehicle and use that device to monitor the vehicle's movements,<sup>2</sup> a ruling which

 $<sup>\</sup>ast$  Marc McAllister is a 2003 graduate of Notre Dame Law School, and is the author of ten publications. The author dedicates this article to his faithful and loving wife, Candy.

<sup>1.</sup> United States v. Jones, 132 S. Ct. 945 (2012).

<sup>2.</sup> More specifically, *Jones* ruled that the Government's installation of a GPS tracking device on a suspect's vehicle, and its subsequent use of that device to monitor the vehicle's movements, constitutes a Fourth Amendment "search," *id.* at 949, a ruling which effectively imposes Fourth Amendment protections upon this form of investigation.

has significantly restrained law enforcement's ability to utilize this method of investigation.<sup>3</sup> Prior to *Jones*, warrantless GPS tracking had been common, and most courts were unwilling to extend Fourth Amendment protection to this investigative technique.<sup>4</sup> In unanimously rejecting these decisions, the *Jones* ruling was surprising<sup>5</sup> and reveals a Court concerned by the potential for mass surveillance inherent in this form of investigation.<sup>6</sup> Perhaps more importantly, the Justices in *Jones* employed distinct rationales, with the majority returning to a trespass-based analysis unused since the 1960's, <sup>7</sup> a potentially groundbreaking

<sup>3.</sup> In response to *Jones*, the FBI turned off about 3,000 GPS tracking devices that were in use. *See* Julia Angwin, *FBI Turns Off Thousands of GPS Devices After Supreme Court Ruling*, THE WALL STREET JOURNAL (Feb. 25, 2012, 3:36 PM), http://blogs.wsj.com/digits/2012/02/25/fbi-turns-off-thousands-of-gps-devices-after-supreme-court-ruling/.

<sup>4.</sup> Prior to *Jones*, most lower courts had ruled that when police use a GPS device to monitor a vehicle's movements in public, no "search" occurs under the principle that it is not reasonable to expect privacy in one's movements in public. *See, e.g.*, United States v. Pineda-Moreno, 591 F.3d 1212, 1216–17 (9th Cir. 2010) (invoking *Knotts* and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search); United States v. Garcia, 474 F.3d 994, 996–97 (7th Cir. 2007) (relying on *Knotts* and holding that GPS tracking is not a search); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) ("[w]]hen police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time"). *See also* United States v. Cuevas-Perez, 640 F.3d 272, 276 (7th Cir. 2011) (Flaum, J., concurring) ("The practice of using [GPS tracking] devices to monitor movements on public roads falls squarely within the [Supreme] Court's consistent teaching that people do not have a legitimate expectation of privacy in that which they reveal to third parties or leave open to view by others.").

<sup>5.</sup> See, e.g., United States v. Rose, 914 F. Supp. 2d 15, 21 (D. Mass. 2012) (describing *Jones* "as a surprise to many" in light of the lower courts' many rulings to the contrary).

<sup>6.</sup> The potential for mass surveillance that concerned the *Jones* Court included the potential to investigate the law-abiding citizen, as well as those suspected of criminal activity, on no suspicion of wrongdoing. Several Justices voiced this concern during oral argument. For example, Chief Justice Roberts inquired: "You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?" Transcript of Oral Argument at 9, United States v. Jones, 132 S. Ct. 945, *available at* http://www.supremecourt.gov/oral\_arguments/argument\_transcripts/10-1259.pdf. Reacting to the same concern, Justice Ginsburg inquired: "I think you answered the question that the government's position would mean that any of us could be monitored whenever we leave our homes. So, the only thing secure is the home. Is—I mean, that is—that is the end point of your argument, that an electronic device, as long as it's not used inside the house, is okay." *Id.* at 12.

<sup>7.</sup> To determine whether a particular form of investigation constitutes a Fourth Amendment "search," thereby triggering the Fourth Amendment's protections, most courts over the past forty-five years have applied the *Katz* test, under which a "search" occurs when "the government['s] [conduct] violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001). *See also* Smith v. Maryland, 442 U.S. 735, 739 (1979) ("In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is *Katz v. United States*."). Rather than apply the *Katz* test, the *Jones* majority applied the pre-*Katz* physical trespass doctrine; in doing so, the Court clarified that the *Katz* test governs only those "search" questions that do not involve an actual physical trespass. *See* United States v. Jones, 132 S. Ct. 945, 952 ("the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test").

move in Fourth Amendment jurisprudence.8

While the *Jones* majority's return to a trespass-based approach leaves many questions unanswered, perhaps the most important, unresolved aspect of *Jones* is whether a Fourth Amendment "search" would occur in the event the same type of monitoring could be accomplished in the absence of a trespass —most notably, where a suspect's location is determined through a GPS-enabled cell phone. 11

According to all nine Justices in *Jones*, instances of GPS tracking that do not require a trespass will be governed by the more traditional *Katz* test, <sup>12</sup> under which a "search" occurs when "the government['s]

<sup>8.</sup> See United States v. Figueroa-Cruz, 914 F. Supp. 2d 1250, 1261 (N.D. Ala. 2012) (describing the *Katz* test as "the predominant approach to Fourth Amendment jurisprudence since the 1960s," and stating that the *Jones* Court's "property-based trespass analysis alters the matrix most frequently applied in the assessment of Fourth Amendment issues because questions of ownership or the existence of a legally cognizable property interest have not generally been considered of controlling analytical importance [under the *Katz* test]") The potential to apply *Jones*'s trespass approach to Fourth Amendment "search" issues more broadly has already begun to alter Fourth Amendment jurisprudence. Indeed, recent courts have employed the *Jones* majority's trespass-based analysis in cases going beyond GPS tracking, such as, for example, public camera monitoring. *See, e.g.*, United States v. Nowka, No. 5:11-cr-00474-VEH-HGD, 2012 WL 2862139, at \*4 (N.D. Ala. May 14, 2012) (rejecting defendant's argument that a pole camera installed outside defendant's residence and trained on this driveway was a "search" under *Jones* because no trespass on Nowka's property occurred in the installation of the pole camera)

<sup>9.</sup> See Rose, 914 F. Supp. 2d at 22 ("the Jones decision left a number of issues unresolved, among them 1) whether the government must obtain a warrant to install and use a GPS tracking device, 2) if not, what quantum of suspicion is required (e.g., probable cause, reasonable suspicion), 3) if the Fourth Amendment is violated, whether the exclusionary rule requires suppression, and 4) if so, what evidence must be suppressed"). See generally Benjamin J. Priester, Five Answers and Three Questions After United States v. Jones (2012), the Fourth Amendment "GPS case", 65 OKLA. L. REV. 491 (2013) (identifying and discussing critical questions that follow in the wake of Jones).

<sup>10.</sup> The *Jones* majority deemed it dispositive that "Jones... possessed the Jeep at the time the Government trespassorily inserted the [GPS] device," distinguishing him from someone who takes possession of property upon which such a device has already been installed. United States v. Jones, 132 S. Ct. 945, 952. The majority distinguished *Karo* on these grounds because in that case, "Karo accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to monitor the container's location" in much the same way as modern-day GPS. *Id.* Noting the potentially broader impact of the Court's trespass-based rationale, some courts post-*Jones* have described *Jones* as signaling "a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') [the Fourth Amendment] enumerates." *Figueroa-Cruz*, 914 F.Supp.2d at 1260.

<sup>11.</sup> See, e.g., United States v. Skinner, 690 F.3d 772, 779–80 (6th Cir. 2012) (In a case where law enforcement "pinged" a suspect's phone to determine its location, the court distinguished *Jones* on the grounds that "[n]o such physical intrusion [of the suspect's phone] occurred in [this] case. [The suspect] himself obtained the cell phone for the purpose of communication, and that phone included the GPS technology used to track the phone's whereabouts.") (internal citations omitted).

<sup>12.</sup> See Jones, 132 S. Ct. at 953 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."). See also id. at 955 (Sotomayor, J., concurring) ("But '[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."); id. at 959–61 (Alito, J., concurring) (arguing that the *Jones* majority erred in reviving the trespass test because "the *Katz* Court repudiated the old [trespass] doctrine," and suggesting that any and all "search" questions should be governed exclusively by *Katz*).

[conduct] violates a subjective expectation of privacy that society recognizes as reasonable." While four Justices in *Jones* did not specifically address the constitutionality of GPS tracking under the *Katz* test, five concurring Justices did. Given that a majority of Justices have already applied *Katz* to analyze a GPS tracking issue, and given that the underlying rationale employed by these Justices would naturally extend to similar forms of tracking by way of GPS-enabled cell phones, the views of the concurring Justices in *Jones* will undoubtedly influence these unresolved issues.

According to those five concurring Justices, <sup>17</sup> tracking the suspect's vehicle for twenty-eight days constituted a search under the *Katz* test. <sup>18</sup> These Justices did not identify the precise point at which the tracking became a search, but simply declared that "the line was surely crossed before the 4-week mark." <sup>19</sup> In light of this opinion, a suspect like Antoine Jones can claim a reasonable expectation of privacy in his movements in public where those movements are tracked for twenty-eight days or longer. <sup>20</sup> At the other end of the spectrum, the Court's

<sup>13.</sup> Kyllo v. United States, 533 U.S. 27, 33 (2001). *See also* Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring) ("there is a twofold requirement, first 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.'").

<sup>14.</sup> See United States v. Hanna, No. 11-20678-CR, 2012 WL 279435, at \*4 (S.D. Fla. Jan. 30, 2012) ("[F]ive members of the [Jones] Court concluded that [the majority's] trespass theory did not form a sufficiently comprehensive analysis of the Fourth Amendment implications of GPS monitoring and argued that GPS monitoring should also (in the case of Justice Sotomayor) or only (in the case of Justice Alito) be analyzed to determine whether it has invaded a reasonable expectation of privacy.").

<sup>15.</sup> As argued below, despite a potential distinction between GPS tracking and cell phone tracking, location information obtained by way of GPS-enabled cell phone enables the Government to obtain essentially the same location information as that provided by the surreptitiously-installed GPS device utilized in *Jones*, thereby implicating the same length of surveillance concerns of the *Jones* concurring Justices. *See infra* notes 154–161 and accompanying text.

<sup>16.</sup> See, e.g., State v. Estrella, 286 P.3d 150, 157 (Ariz. Ct. App. 2012) (Eckerstrom, J., dissenting) ("My colleagues maintain that our result in this case is compelled by the Court's reasoning in [United States v. Knotts, 460 U.S. 276 (1983),] that a person has 'no reasonable expectation of privacy in his movements' on public roads. But, in the context we address today—the GPS tracking of a person's movements on public roads—five [J]ustices of the Court have implicitly declined to adopt that part of *Knotts*'s reasoning. I, therefore, cannot agree that this aspect of *Knotts* must control our reasoning in this case.").

<sup>17.</sup> Justice Alito's concurring opinion, which was signed by three additional Justices, described the issue as "[w]hether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." United States v. Jones, 132 S. Ct. 945, 958 (Alito, J., concurring).

<sup>18.</sup> Id. at 964.

<sup>19.</sup> *Id. See also id.* at 955 (Sotomayor, J., concurring) (agreeing with the Alito concurrence that "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

<sup>20.</sup> At least for the particular type of suspect at issue in *Jones*, a suspected drug dealer. *See id.* at 948 (describing the suspect, Antoine Jones, as someone who the police suspected was "trafficking in narcotics").

prior holding in *United States v. Knotts*<sup>21</sup> suggests that a person traveling on public roads for just a few hours cannot reasonably expect privacy in those movements,<sup>22</sup> a decision *Jones* was careful not to overrule.<sup>23</sup> The line between these two points remains unclear.<sup>24</sup>

Complicating matters, the concurring Justices in *Jones* suggested that a twenty-eight day monitoring would not constitute a search where the investigation involved a more serious offense than that in *Jones*, <sup>25</sup> and the remaining Justices conceded that "[w]e may have to grapple with these 'vexing problems' in some future case where a classic trespassory search is not involved and resort must be had to *Katz* analysis."

This article examines these "vexing problems"<sup>27</sup> in depth. Since *Jones* was decided in January 2012, courts in GPS tracking cases have already begun making distinctions based upon the type of suspect and length of surveillance.<sup>28</sup> Through empirical studies, I set out to explore

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

211

<sup>21.</sup> United States v. Knotts, 460 U.S. 276 (1983).

<sup>22.</sup> In *Knotts* the Court upheld the warrantless use of a beeper to track a drum of chloroform from the defendant's point of purchase to a cabin about 100 miles away. According to the Court, the use of the beeper did not constitute a "search" because the beeper did not provide any information police could not have obtained through visual surveillance along the vehicle's route. Just one year after *Knotts*, the Court in *United States v. Karo*, 468 U.S. 705 (1984), examined a similar case and reached the opposite result as in *Knotts*, primarily because the beeper in that case was used to track a can of ether inside a private residence.

<sup>23.</sup> See Jones, 132 S. Ct. 945, 952 (distinguishing *Knotts* as a case where the Court's trespass concerns did not apply because "[t]he beeper had been placed in the container before it came into Knotts' possession, with the consent of the then-owner"). See also U.S. v. Figueroa-Cruz, 914 F.Supp.2d 1250, 1268 (N.D. Ala. 2012) (noting that *Jones* did not overrule *Knotts*, but rather distinguished it based on "the ownership or exclusivity of the use of the chattel" at issue).

<sup>24.</sup> See, e.g., United States v. Skinner, 690 F.3d 772, 780 (6th Cir. 2012) ("Justice Alito's concurrence and the majority in *Jones* both recognized that there is little precedent for what constitutes a level of comprehensive tracking that would violate the Fourth Amendment.").

<sup>25.</sup> Writing on behalf of Justices Ginsburg, Breyer, and Kagan, Justice Alito wrote: "[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable. But the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such 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." Jones, 132 S. Ct. at 964 (Alito, J., concurring). Writing separately, Justice Sotomayor appeared to ratify Justice Alito's suggestion when she wrote: "I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Id. at 955 (Sotomayor, J., concurring) (emphasis added). With the addition of Justice Sotomayor, five Justices in Jones appear willing to vary Fourth Amendment protections based upon not only the length of surveillance, but also the type of suspect at issue.

<sup>26.</sup> Jones, 132 S. Ct. at 954.

<sup>27.</sup> Perhaps these are "vexing problems" for the Court because if Justice Alito's approach were taken literally, the Fourth Amendment would no longer protect all American citizens equally. Rather, the suspected criminals, the "bad guys" if you will, would enjoy fewer Fourth Amendment protections than the purely "innocent," law-abiding citizens would enjoy.

<sup>28.</sup> See infra notes 162-204 and accompanying text.

whether society is likewise ready to embrace such distinctions.<sup>29</sup>

In the months following *Jones*, I administered two surveys designed to test this hypothesis; each professionally designed and inspired by similar instruments administered by Fourth Amendment scholar Christopher Slobogin.<sup>31</sup>

My first survey poses a series of questions involving GPS tracking of seven different types of suspects, including: individuals not suspected of any crime, individuals suspected of minor crimes, and individuals suspected of relatively severe crimes. My essential hypothesis was that society would be willing to permit police to engage in warrantless GPS tracking for a longer period of time when investigating the most serious offenses.

After collecting over 230 survey responses, this hypothesis was seemingly verified. For example, only 10.9% of survey respondents (25 of 230), would have permitted police to attach a GPS tracking device to the vehicle of an innocent suspect<sup>32</sup> and monitor that vehicle's movements without first obtaining a warrant. By contrast, 67.3% of survey respondents would have permitted a suspected terrorist's vehicle to be tracked with no warrant, and those individuals were generally willing to permit a much lengthier period of surveillance for the suspected terrorist as compared to those suspected of less severe crimes.<sup>33</sup> This evidence appears to validate the notion that Fourth Amendment protections with respect to GPS tracking should vary based upon the nature of the crime under investigation, with one of those variations being the permissible length of warrantless surveillance.

To specifically examine the constitutionality of cell phone tracking, I conducted a second survey posing questions relating to both GPS

<sup>29.</sup> Society's views are arguably relevant under the *Katz* standard because the *Katz* test itself, taken literally, anticipates examination of society's actual expectations of privacy. *See* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 505–08 (2012) (arguing in support of the empirical approach).

<sup>30.</sup> I designed each survey with the help of an instructional design consultant, Dr. Raoul A. Arreola. Dr. Arreola retired from the University of Tennessee Health Science Center in 2009 with the rank of professor emeritus. He holds a doctorate in educational psychology, specializing in research design, measurement, and evaluation, as well as an undergraduate degree in mathematics and physical sciences. Over the last forty-two years, he has worked primarily in the areas of instructional evaluation and development, faculty evaluation and development, and the use of technology in the teaching and learning process.

<sup>31.</sup> See infra notes 208–219 and accompanying text.

<sup>32.</sup> As used here, the term "innocent suspect" refers to an individual who has not previously been convicted of a crime and who is not currently suspected of committing any crime.

<sup>33.</sup> For example, when asked whether a suspected terrorist could be tracked without a warrant, 89 of 226 survey respondents, or 39.4%, would have permitted such an individual to be tracked without a warrant for twenty-one days or longer. By contrast, when asked whether a suspected drug dealer could be tracked without a warrant, only 20.6% of respondents, or 46 of 223, would have permitted such an individual to be tracked without a warrant for twenty-one days or longer.

tracking by physical trespass upon a suspect's vehicle, approximating the issue in *Jones*; and the monitoring of a suspect's movements by GPS-enabled cell phone, an issue currently unresolved by the Supreme Court.<sup>34</sup>

213

In this second survey, respondents were given two distinct series of questions. In the first series of questions, respondents were asked to assume that police had attached a GPS tracking device to a suspect's vehicle by way of trespass and had used that device to monitor the suspect's movements for a period of time. In the second series of questions, identical to the first in most respects,<sup>35</sup> respondents were instead asked to assume that police were able to monitor an individual's movements by way of cell phone.

The results of this second survey, summarized in Part V, suggest several important conclusions for the future of warrantless cell phone tracking. First, as a general matter, society deems electronically-stored information presumptively protected by the Fourth Amendment, regardless of whether that data is obtained surreptitiously by the police or obtained directly from a cell phone provider. Second, as with the first survey, society appears willing to vary Fourth Amendment protections in regards to GPS tracking based upon the nature of the crime under investigation, with length of surveillance as one of those variations. Finally, and perhaps most importantly, society believed that tracking an individual by cell phone should receive somewhat greater Fourth Amendment protection than tracking an individual in the manner employed in *Jones*. This particular finding suggests that cell phone tracking, despite its currently limited protection, should be subject to at least the same constraints as those imposed in *Jones*. In combination,

<sup>34.</sup> See Jones v. United States, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring) ("With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory—or owner—installed vehicle tracking devices or GPS-enabled smartphones."); see also id. at 963 (Alito, J., concurring) (describing the ability of cell phones to track a person's movements).

<sup>35.</sup> Emphasizing the parallel to GPS tracking, the lead-in language for the second series of questions was as follows: "Cell phone technology, coupled with the widespread use of smart phones among American citizens, has enabled police to determine a person's movements with nearly as much accuracy as a GPS device mounted on that person's vehicle. Cell phone data, for example, is often used to reveal where a cell phone was located at a particular point in time by identifying which cell tower communicated with the cell phone while the phone was utilized to make a call. Cell location data makes it possible to determine a person's movements with precision, and can operate successfully even when the phone is simply turned on, regardless of whether a call has been made or not. Cell phone companies maintain accurate records of cell phone location information for all of its customers, making it possible for police to obtain a suspect's location information by a simple request to a cell phone provider, such as AT&T or Verizon. Please answer the following questions related to this emerging form of police investigation."

<sup>36.</sup> See United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("[P]hysical intrusion is now unnecessary to many forms of surveillance. With increasing regularity, the

these findings point to a proposal, set forth in Part V, that treats all forms of GPS and cell phone tracking alike for purposes of the Fourth Amendment and that alters the level of suspicion required by the Fourth Amendment based upon the length of surveillance and type of crime under investigation.

Part II of this article summarizes the major United States Supreme Court cases that impact the developing law of GPS tracking. Part III highlights the two primary lines of GPS tracking cases that exist today: those, like *Jones*, that involve the trespassory attachment of a GPS device to a suspect's vehicle; and those, numerous among the lower courts, that address the tracking of a suspect's movements by GPS-enabled smart phone. Part IV sets forth the detailed results of each of my surveys. Part V addresses how my survey results impact the constitutionality of monitoring a suspect's movements by cell phone.<sup>37</sup> Part VI concludes.

#### II. SUPREME COURT CASES ON GPS AND ELECTRONIC TRACKING

#### A. The Law of Electronic Tracking Pre-Jones

In the years preceding *Jones*, police departments around the country were utilizing GPS tracking devices to monitor the movements of criminal suspects without warrants.<sup>38</sup> When suspects challenged the

Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory—or owner—installed vehicle tracking devices or GPS-enabled smartphones. In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance.") (internal citations omitted).

<sup>37.</sup> While tracking a suspect's movements by cell phone is the most likely method of tracking to follow in the wake of *Jones*, post-*Jones* courts have upheld the warrantless attachment of a GPS tracking device to a target vehicle by finding an insufficient property interest in the vehicle at issue on the part of the particular defendant. *See, e.g.*, U.S. v. Figueroa-Cruz, 914 F. Supp. 2d 1250, 1262–64 (N.D. Ala. 2012).

<sup>38.</sup> See, e.g., United States v. White, 484 F.3d 267, 281 (4th Cir. 2007) (detailing an extensive federal drug investigation in Maryland involving various investigative techniques, including GPS trackers); United States v. Mayberry, 540 F.3d 506, 511 (6th Cir. 2008) (noting that, as part of their investigation into robberies, police in Michigan "secretly placed a GPS tracking device on the [defendant's] rental car" while it was parked at an apartment complex); United States v. Santiago, 560 F.3d 62, 64–65 (1st Cir. 2009) (detailing "a year-long investigation into a large-scale heroin distribution operation" that occurred in 2003 and 2004 in Massachusetts, in which "agents tracked [defendant's] van with a GPS unit and conducted visual surveillance of it; conducted court authorized wiretaps of cell phones of the defendants; [and] tracked and observed transactions among the defendants revealed by cell phone conversations"); United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (noting that "over a four-month period, [DEA] agents [in Oregon] repeatedly monitored Pineda-Moreno's Jeep using various types of mobile tracking devices," and that agents installed the devices on seven different occasions); United States v. Marquez, 605 F.3d 604, 607 (8th Cir. 2010) (recounting how DEA and Iowa state officers placed a GPS tracking device on the bumper of a Ford while it was parked in a Walmart parking lot in Des Moines, Iowa, and subsequently used the device to monitor the vehicle's

constitutionality of that warrantless police conduct, most courts had concluded that the Fourth Amendment did not apply to this method of investigation under the simple logic that no person can reasonably expect privacy in his movements in public.<sup>39</sup> To support that result, courts analogized GPS tracking to one of two Supreme Court cases from the 1980's, each involving the tracking of a vehicle by electronic beeper.

215

In *United States v. Knotts*, <sup>40</sup> the Court upheld the warrantless use of a beeper to track a drum of chloroform from the defendant's point of purchase to a cabin about 100 miles away. According to *Knotts*, the use of the beeper did not constitute a "search" because the beeper did not provide any information police could not have obtained through visual surveillance along the vehicle's route. 42

Just one year after Knotts, the Court in United States v. Karo<sup>43</sup> examined a similar case and reached the opposite result, primarily because the beeper in that case was used to track a can of ether inside a private residence. 44 Distinguishing the public surveillance in *Knotts*, the Court reasoned that "indiscriminate monitoring of property that has been

2010) (per curiam) (describing an investigation in Florida in which police installed a GPS device on the truck of a person suspected of trafficking marijuana); United States v. Cuevas-Perez, 640 F.3d 272, 272-73 (7th Cir. 2011) (describing an investigation in which Arizona police attached a GPS tracking device to the suspect's Jeep which was programmed to send text message updates of the Jeep's location every four minutes, then tracked the Jeep's movements into several states, eventually leading to the suspect's arrest in Illinois).

- 39. See, e.g., Pineda-Moreno, 591 F.3d at 1216-17 (invoking Knotts and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search); United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) (relying on Knotts and holding that GPS tracking is not a search); Marquez, 605 F.3d at 610 ("[w]hen police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time"). See also Cuevas-Perez, 640 F.3d at 276 (7th Cir. 2011) (Flaum, J., concurring) ("The practice of using [GPS tracking] devices to monitor movements on public roads falls squarely within the [Supreme] Court's consistent teaching that people do not have a legitimate expectation of privacy in that which they reveal to third parties or leave open to view by others.").
  - 40. United States v. Knotts, 460 U.S. 276 (1983).
- 41. Having suspected Knotts of manufacturing drugs, federal officers, without a warrant, had installed a beeper in a chemical drum they knew would be sold to Knotts. With the beeper's assistance, officers followed Knotts's vehicle to where it stopped outside a certain cabin. Based on this information, the police secured a warrant to search the cabin, and uncovered incriminating evidence inside. Id. at 278-79.
- 42. According to the Knotts Court, "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and the "use of the beeper to signal the presence of [the vehicle] . . . does not alter the situation." Id. at 281-282.
  - 43. United States v. Karo, 468 U.S. 705 (1984).
- 44. Because the beeper in Karo was used to monitor the can's movements within a private residence, see id. at 714, the Court described the issue as follows, "whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." Id. at 714.

movements back and forth to Colorado); United States v. Smith, 387 Fed. App'x. 918, 919 (11th Cir.

withdrawn from public view" must remain subject to Fourth Amendment oversight.<sup>45</sup>

Invoking *Knotts* and distinguishing *Karo*, pre-*Jones* GPS tracking cases typically concluded that when a GPS tracking device is used to monitor a suspect's movements on public roads, no "search" occurs because the suspect cannot reasonably expect privacy in those movements. Applying the *Knotts/Karo* distinction, most courts analyzing the constitutionality of warrantless GPS tracking prior to *Jones* reasoned that tracking a vehicle's movements in public is more akin to "non-search" forms of surveillance, such as an officer physically trailing a suspicious vehicle. However, some pre-*Jones* courts refused to apply this rationale, on the grounds that it fails to account for inherent differences between tracking a vehicle for a few hours by beeper and tracking that same vehicle for a substantially longer period of time by the more sophisticated GPS. The Supreme Court granted certiorari in *Jones* to resolve the split.

#### B. United States v. Jones

In *Jones*, the United States Supreme Court unanimously struck down one instance of GPS tracking in which a suspect's vehicle was

<sup>45.</sup> As the Court explained, "[Karo] is thus not like Knotts, for there the beeper told the authorities nothing about the interior of Knotts' cabin.... [H]ere, [by contrast] the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified [by the police from outside the house]," id. at 715, and one that "the Government is extremely interested in knowing." Id.

<sup>46.</sup> See, e.g., United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010) (invoking Knotts and holding that the GPS tracking of an individual's movements in his vehicle over a prolonged period is not a search); United States v. Garcia, 474 F.3d 994 (7th Cir. 2007) (same); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) (stating in dicta that "when police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time").

<sup>47.</sup> In one such case, the United States Court of Appeals for the Seventh Circuit viewed GPS tracking as more akin to hypothetical practices it assumed are not searches, such as tracking a car "by means of cameras mounted on lampposts or satellite imaging." *See* United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007) ("[I]f police follow a car around, or observe its route by means of cameras mounted on lampposts or of satellite imaging as in Google Earth, there is no search.").

<sup>48.</sup> See, e.g., United States v. Maynard, 615 F.3d 544, 555–68 (D.C. Cir. 2010) (holding that the use of a GPS tracking device to monitor an individual's movements over a four-week period is a search, and rejecting the Government's argument, based on an attempted extension of *Knotts*, that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another" even in such extended instances of GPS tracking); People v. Weaver, 12 N.Y.3d 433, 440–44 (2009) (distinguishing *Knotts*, and declaring: "At first blush, it would appear that *Knotts* does not bode well for Mr. Weaver, for in his case, as in *Knotts*, the surveillance technology was utilized for the purpose of tracking the progress of a vehicle over ... predominantly public roads and, as in *Knotts*, these movements were at least in theory exposed to 'anyone who wanted to look.' This, however, is where the similarity ends.").

<sup>49.</sup> United States v. Jones, 131 S. Ct. 3064 (2011).

monitored on public streets for twenty-eight days.<sup>50</sup>

In *Jones*, without a valid warrant,<sup>51</sup> officers installed a GPS tracking device on suspect Antoine Jones's jeep while it was parked in a public parking lot.<sup>52</sup> Over the next twenty-eight days, officers used the device to track the movements of Jones's vehicle.<sup>53</sup> The resulting GPS data connected Jones to a structure that contained large amounts of cash and cocaine, evidence that was used to bring criminal charges against Jones.<sup>54</sup>

Before trial, Jones unsuccessfully moved to suppress the evidence obtained through the GPS tracking device. Following most prior GPS tracking decisions, the trial court reasoned that, just as in *Knotts*, "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."

On appeal, the Supreme Court's majority opinion (consisting of Justices Scalia, Roberts, Kennedy, Thomas, and Sotomayor<sup>58</sup>) considered "whether the attachment of a Global–Positioning–System (GPS) tracking device to an individual's vehicle, and subsequent use of that device to monitor the vehicle's movements on public streets, constitutes a search or seizure within the meaning of the Fourth Amendment."<sup>59</sup>

In its phrasing of the issue, the *Jones* majority limited its analysis to the movements of Jones's vehicle "on public streets," <sup>60</sup> rather than

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

<sup>50.</sup> See United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search,'" thereby presumptively requiring a warrant). See also id. at 964 (Alito, J., concurring) (concluding on behalf of Justices Alito, Ginsburg, Breyer, and Kagan that the lengthy GPS monitoring that occurred in that case constituted a Fourth Amendment "search," thereby presumptively requiring a warrant); id. at 954 (Sotomayor, J., concurring) (agreeing with the majority that "a search within the meaning of the Fourth Amendment occurs, at a minimum, 'where, as here, the Government obtains information by physically intruding on a constitutionally protected area").

<sup>51.</sup> Although the officers had obtained a warrant authorizing installation of the device, the device was installed after the warrant had expired and outside the jurisdiction specified in the warrant. *Id.* at 948.

<sup>52.</sup> Id

<sup>53.</sup> *Id.* The device relayed more than 2,000 pages of data regarding the vehicle's movements over the four week period. *Id.* 

<sup>54.</sup> Id. at 949.

<sup>55.</sup> The District Court granted the motion in part, suppressing only the data obtained while the vehicle was parked in the garage adjoining Jones's residence. United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006).

<sup>56.</sup> See supra note 4.

<sup>57.</sup> Jones, 451 F. Supp. 2d at 88 (citing United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

<sup>58.</sup> Jones, 132 S. Ct. at 948.

<sup>59.</sup> *Id*.

<sup>60.</sup> Id.

within private spaces,<sup>61</sup> potentially triggering the rationale underlying *Knotts* that one cannot reasonably expect privacy in his movements in public. Effectively rejecting the principle underlying *Knotts*, the majority held that a "search" had occurred;<sup>62</sup> since no warrant justified the search, the evidentiary fruits of that search had to be suppressed.<sup>63</sup>

While all nine Justices in *Jones* agreed that this particular instance of GPS tracking triggered the protections of the Fourth Amendment,<sup>64</sup> the Justices were split in their rationale. Instead of applying the *Katz* test, the majority applied the pre-*Katz* physical trespass doctrine.<sup>65</sup> Under this test, the majority reasoned that "a vehicle is an 'effect' as that term is used in the [Fourth] Amendment;"<sup>66</sup> and in this case, the Government physically trespassed upon Jones's vehicle by attaching the device as it was parked in public.<sup>67</sup> According to the majority, "the Government's installation of a GPS device on a target's vehicle, and its use of that

<sup>61.</sup> In limiting the issue to the movements of Jones's vehicle "on public streets," the *Jones* majority seemingly accepted the District Court's suppression of the GPS tracking data obtained while the vehicle was parked in the garage adjoining Jones's residence. *See id.* at 948.

<sup>62.</sup> According to the majority, "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search." *Id.* at 949. In its brief in *Jones*, the Government argued that individuals have no reasonable expectation of privacy in information that is knowingly exposed to public view, and that Antoine Jones himself had no reasonable expectation of privacy in the movements of his vehicle on public streets because that information was exposed to public view. *See* Reply Brief for the United States at 18, 38, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5094951. Invoking *Knotts*, the Government argued that "[t]his case, like *Knotts*, involves movements of a vehicle on public streets," which is unprotected by the Fourth Amendment. *Id.* at 22. In ruling for Jones, the majority effectively rejected the Government's *Knotts*-based argument.

<sup>63.</sup> See Jones, 132 S. Ct. at 954 (affirming the lower court's judgment that admission of the evidence obtained by use of the GPS device violated the Fourth Amendment, and refusing to address the Government's argument that the warrantless "search" that occurred in this case was made reasonable, despite no valid warrant, by the reasonable suspicion or probable cause the officers had obtained before using the device).

<sup>64.</sup> See id. at 949 (holding that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search," thereby presumptively requiring a warrant). See also id. at 964 (Alito, J., concurring) (concluding on behalf of Justices Alito, Ginsburg, Breyer, and Kagan that the lengthy GPS monitoring that occurred in that case constituted a Fourth Amendment "search," thereby presumptively requiring a warrant); id. at 954 (Sotomayor, J., concurring) (agreeing with the majority that "a search within the meaning of the Fourth Amendment occurs, at a minimum, 'where, as here, the Government obtains information by physically intruding on a constitutionally protected area"").

<sup>65.</sup> See id. at 949–52. According to the majority, Katz did not repudiate the understanding that the Fourth Amendment embodies a particular concern for government trespass upon the areas it enumerates. See id. at 950. Rather, "[t]he Katz reasonable-expectation-of-privacy test has been added to, but not substituted for, the common-law trespassory test." Id. at 947. Thus, as the majority saw it, "Jones's Fourth Amendment rights do not rise or fall with the Katz formulation." Id. at 950. However, as the majority clarified, "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis." Id. at 953.

<sup>66.</sup> Id. at 949.

<sup>67.</sup> According to the majority, "[b]y attaching the device to the Jeep, officers encroached on a protected area." *Id.* at 952.

device to monitor the vehicle's movements, constitutes a 'search,'".68 and a presumptively unreasonable one in the absence of a valid warrant.

219

Criticizing the majority's trespass-based analysis, Justice Alito's concurring opinion, joined by Justices Ginsburg, Breyer, and Kagan, instead employed the *Katz* test. Emphasizing the length of surveillance as the most important factor, the concurring Justices declared that the majority's trespass-based analysis "largely disregards what is really important (the use of a GPS for long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."<sup>71</sup> According to these four Justices, "the lengthy monitoring that occurred in this case [twenty-eight days] constituted a search under the Fourth Amendment,"<sup>72</sup> further noting that "the line [of Fourth Amendment protection] was surely crossed before the 4-week mark."<sup>73</sup>

Justice Sotomayor wrote separately to voice her agreement with both the majority and the Alito concurrence. According to Justice Sotomayor, the majority's trespass-based analysis was sufficient to resolve the case because "[t]he Government usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded . . . Fourth Amendment protection."

Despite agreeing with the majority, Justice Sotomayor went on to declare that "the Fourth Amendment is not concerned only with trespassory intrusions on property;" rather, even in the absence of a trespass, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." Employing this test, Justice Sotomayor agreed with the other four concurring Justices that "at the very least, 'longer term GPS

<sup>68.</sup> *Id.* at 949. In a similar passage, the majority declared: "The Government physically occupied private property [i.e., Jones's vehicle] for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* 

<sup>69.</sup> See id. at 954.

<sup>70.</sup> Emphasizing the length of surveillance as the critical factor, Justice Alito's concurrence described the issue as "[w]hether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." *Id.* at 958 (Alito, J., concurring).

<sup>71.</sup> *Id.* at 961.

<sup>72.</sup> Id. at 964.

<sup>73.</sup> *Id*.

<sup>74.</sup> See id. at 954-55 (Sotomayor, J., concurring).

<sup>75.</sup> Id. at 955.

<sup>76.</sup> Id. at 954.

<sup>77.</sup> *Id*.

<sup>78.</sup> Id. at 954–55.

monitoring in investigations of most offenses impinges on expectations of privacy." 79

As the dust of *Jones* settles, we know that there are currently two ways in which a particular instance of GPS tracking may constitute a Fourth Amendment "search." First, as the *Jones* holding makes clear, a "search" occurs when the Government trespassorily installs a GPS tracking device upon a suspect's "effect" and uses that device to monitor the vehicle's movements, even where those movements are monitored only on public streets. When such a trespassory attachment has taken place, a "search" will always have occurred, regardless of the length of surveillance. 83

Alternatively, when the government installs a GPS tracking device on or within a piece of property at a time when the particular suspect at issue has no legal interest in the property, the installation of the device is not a "trespass" and is therefore not a "search" for purposes of the trespassory test. His result applies as well when a suspect takes possession of an item that contains a factory-installed GPS device, as in the case of most modern cell phone purchases. In the event of no

<sup>79.</sup> Id. at 955.

<sup>80.</sup> See United States v. Cowan, 674 F.3d 947, 955 (8th Cir. 2012) ("An individual may challenge a search under the Fourth Amendment if it violates the individual's 'reasonable expectation of privacy,' or involves an unreasonable 'physical intrusion of a constitutionally protected area."") (citing United States v. Jones, 132 S. Ct. 945, 950–53 (2012)); United States v. Johnson, 871 F. Supp. 2d 539, 546 (W.D. La. 2012) ("Jones established, or perhaps reiterated, that there are two ways to analyze [whether a Fourth Amendment "search" has occurred]: a traditional common-law property rights test and the Katz/reasonable-expectation-of-privacy test."). See also Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013) (utilizing the same two-part "search" framework set forth in Jones).

<sup>81.</sup> In other words, at a time when the defendant has a legal interest in the property. *See Jones*, 132 S. Ct. at 949 n.2 (refusing to consider Jones's status in relation to the vehicle at issue because the Government acknowledged, and did not challenge, that Jones was "the exclusive driver").

<sup>82.</sup> See id. at 949 ("We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"); id. at 952 ("By attaching the device to the Jeep, officers encroached on a protected area"). See also Free Speech Coalition, Inc. v. Attorney Gen. of the United States, 677 F.3d 519, 542–43 (3d Cir. 2012).

<sup>83.</sup> In such instances, *Jones* creates a bright-line rule, one that does not depend upon factors that would be relevant under a traditional *Katz* analysis. *See Jones*, 132 S. Ct. at 961 (Alito, J., concurring) ("If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies.").

<sup>84.</sup> The *Jones* majority deemed it dispositive that "Jones... possessed the Jeep at the time the Government trespassorily inserted the [GPS] device," distinguishing him from someone who takes possession of property upon which such a device has already been installed. *Id.* at 952. The majority distinguished *Karo* on these grounds because in that case, "Karo accepted the container as it came to him, beeper and all, and therefore was not entitled to object to the beeper's presence, even though it was used to monitor the container's location" in much the same way as modern-day GPS. *Id.* 

<sup>85.</sup> Here again, the same reasoning would apply because when a person purchases a GPS-enabled cell phone, that person has likewise "accepted the [phone] as it [comes] to him, [GPS] and all, and therefore [i]s not entitled to object to the [GPS device's] presence, even [if] it [i]s used to monitor the [phone]'s location." *Id*.

trespass, a Fourth Amendment "search" could only occur if the *Katz* test is satisfied. To satisfy the *Katz* test, the person invoking Fourth Amendment protection must demonstrate a reasonable or legitimate expectation of privacy that has been invaded by government action, an analysis which is necessarily fact specific. Under *Katz*, factors such as the length of surveillance, the nature of the suspected crime, and the location of the vehicle become critical, but as a totality of circumstances inquiry, the factors may be important as well.

221

#### III. LOWER COURT GPS TRACKING CASES POST-JONES

#### A. GPS Tracking Accomplished by Way of Trespass

Consistent with the explicit holding of *Jones*, post-*Jones* courts have held that when law enforcement officers attach a GPS tracking device to a suspect's vehicle and use that device to monitor the vehicle's movements, a Fourth Amendment "search" occurs (without regard to the types of factors that might be relevant under a *Katz*-based analysis, such as length of surveillance). <sup>90</sup>

United States v. Lee<sup>91</sup> is illustrative. In Lee, DEA agents received a tip that defendant Robert Dale Lee had at one time obtained marijuana

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

<sup>86.</sup> *Id.* at 953 ("Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis.").

<sup>87.</sup> Free Speech Coalition, Inc., 677 F.3d 542-43.

<sup>88.</sup> In the Fourth Amendment context, the Supreme Court has consistently voiced a preference for a case-by-case approach. In 1931, the Court declared: "There is no formula for the determination of reasonableness. Each case is to be decided on its own facts and circumstances." Go-Bart Co. v. United States, 282 U.S. 344, 357 (1931). The Court in Sibron v. New York similarly declared, "[t]he constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case." 392 U.S. 40, 59 (1968). And, just recently, Justice Alito's concurring opinion in Jones declared, "[t]he best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated." See United States v. Jones, 132 S. Ct. 945, 964 (Alito, J., concurring) (emphasis added).

<sup>89.</sup> As one court put it, when a defendant takes possession of a piece of property on which a GPS device has already been installed, the continued monitoring of the device would not be a "search" of that particular defendant under the trespassory test, but may constitute a "search" of the defendant under the *Katz* reasonable-expectation-of-privacy test. That analysis, however, would depend on the specific facts of the case. United States v. Barraza-Maldonado, 879 F. Supp. 2d 1022, 1028 (D. Minn. 2012). *Compare* United States v. Knotts, 460 U.S. 276, 285 (1983) (finding no reasonable expectation of privacy in a very short monitoring of a suspect's location on public streets), *with* United States v. Karo, 468 U.S. 705, 714–15 (1984) (finding a reasonable expectation of privacy in location in a private residence).

<sup>90.</sup> See e.g., Kelly v. State, 56 A.3d 523, 538 (Md. Ct. Spec. App. 2012) ("In the case before us, there was a physical trespass, and therefore, placement of the GPS device [on the defendant's vehicle] constituted a search, without need to address [defendant's] reasonable expectation of privacy and whether the facts in this case, distinguishable from the facts in *Jones*, would pass muster.").

<sup>91.</sup> United States v. Lee, 862 F. Supp. 2d 560 (E.D. Ky. 2012).

from Chicago and transported it to eastern Kentucky in his car. Several months later, Lee, who had been in prison on similar charges, reported to the United States Probation Office in London, Kentucky, for the last day of his supervised release. While Lee met with his probation officer, DEA Task Force Officer Brian Metzger secretly installed a GPS tracking device on Lee's car. The tracking device, which had not been authorized by a judge, transmitted the location of Lee's vehicle to DEA agents in real time.

Three days after installing the device, DEA agents noticed that Lee had driven to Chicago. The next day, the agents observed Lee's vehicle moving back towards Kentucky. Suspecting that Lee had again driven to Chicago to obtain marijuana, Officer Metzger contacted Kentucky State Trooper Matt Hutti, told him that the vehicle "probably" contained marijuana, and told him that he "would have to obtain his own PC, probable cause, for a traffic stop." When Lee reached the area where Hutti was stationed to intercept him, Hutti observed that Lee was not wearing a seatbelt as he drove past. Consequently, Hutti pulled Lee over for the seatbelt violation. Soon thereafter, two drug-sniffing dogs alerted to the presence of illegal narcotics within the car. Officers then searched the car and found approximately 150 pounds of marijuana.

Lee later moved to suppress the marijuana found in his vehicle. On March 22, 2012, about two months after *Jones* was decided, Magistrate Judge Ingram recommended granting the motion to suppress. Judge Amul R. Thapar of the United States District Court for the Eastern District of Kentucky agreed. According to Judge Thapar, "[u]nder even the narrowest reading of *Jones*, 'when the government physically

<sup>92.</sup> Id. at 562.

<sup>93.</sup> Id.

<sup>94.</sup> Id.

<sup>95.</sup> Id.

<sup>96.</sup> Id.

<sup>97.</sup> Id.

<sup>98.</sup> Id. at 562.

<sup>99.</sup> Id. at 563.

<sup>100.</sup> Id.

<sup>101.</sup> Id.

<sup>102.</sup> Id.

<sup>103.</sup> *Id*.

<sup>104.</sup> Given the rather clear *Jones* holding, both Lee and the United States agreed that the DEA agents performed an illegal search when they installed a GPS device on Lee's car without Lee's knowledge or consent. *Id.* at 564. The parties therefore centered their arguments on possible exceptions to the exclusionary rule, including the good-faith exception and the attenuation doctrine. *See id.* at 564–71 (analyzing the issues).

#### 2013] GPS AND CELL PHONE TRACKING

invades personal property to gather information, a search occurs."<sup>105</sup> Applying this rule, Judge Thapar found "no[] dispute that [Officer Metzger] physically invaded Lee's property when he placed the GPS tracker on Lee's car."<sup>106</sup> According to Judge Thapar, "[t]hat physical invasion was a trespass, and that trespass continued while the device transmitted information to the DEA agents."<sup>107</sup> Under a simple application of *Jones*, Judge Thapar thus concluded "that the DEA agents performed an illegal search when they installed a GPS tracking device on Lee's car without a warrant."<sup>108</sup>

While post-Jones courts have consistently held that a "search" occurs when law enforcement officers attach a GPS tracking device to a suspect's vehicle and use that device to monitor the vehicle's movements (pursuant to the explicit holding of *Jones*), most of these courts have ultimately refused to suppress the evidence obtained as a result of that tracking by employing one of the exceptions to the exclusionary rule. For example, in *United States v. Ford*, <sup>109</sup> a federal District Court ruled that "law enforcement must obtain a warrant to place a GPS device on a suspect's vehicle," and held that "[h]ere, [the investigating officer] did not obtain a warrant and he therefore violated Defendant's Fourth Amendment rights." 110 Despite that ruling, the Ford court upheld the admissibility of the evidence obtained as a result of this Fourth Amendment violation under the exclusionary rule's goodfaith exception outlined in Davis v. United States, 111 which creates an exception to exclusion "when the police act with an 'objectively reasonable good-faith belief that their conduct is lawful."112 Application of the Davis good-faith exception is a common theme among the post-Jones GPS tracking cases, effectively preventing suppression in those cases where warrantless, trespassory GPS tracking was conducted prior to *Jones* and in reasonable reliance upon existing case law at the time. 113

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

<sup>105.</sup> Id. at 570-71.

<sup>106.</sup> Id. at 571.

<sup>107.</sup> *Id*.

<sup>108.</sup> *Id.* Moreover, Judge Thapar noted that "[e]ven though the DEA agents could have determined Lee's location through cell phone data under [the jurisdiction's case precedent], they could not obtain that same information through an illegally placed GPS device under *Jones.*" *Id.* at 571.

 $<sup>109. \ \</sup> United \ States \ v. \ Ford, \ No. \ 1:11-CR-42, \ 2012 \ \ WL \ 5366049 \ (E.D. \ Tenn. \ Oct. \ 30, \ 2012).$ 

<sup>110.</sup> Id. at \*8.

<sup>111.</sup> Davis v. United States, 131 S. Ct. 2419 (2011). Despite the lack of binding circuit court precedent at the time of the officer's action, the *Ford* court concluded that the officer's reliance on non-binding precedent from "three out of four federal circuits to hear the GPS tracking device issue" prior to *Jones* was reasonable. *Ford*, 2012 WL 5366049, at \*11.

<sup>112.</sup> Davis, 131 S. Ct. at 2427.

<sup>113.</sup> See, e.g., United States v. Rose, 914 F. Supp. 2d 15, 22–24 (D. Mass. 2012) (noting no dispute "that the installation of and use of GPS tracking devices, post-*Jones*, constitutes a 'search' under

#### B. GPS Tracking Accomplished Without Trespass: Cell Phone Tracking

Law enforcement is often able to duplicate the type of tracking that occurred in *Jones* by monitoring the location of a suspect's cell phone. Given that no trespass is required to monitor the location of a suspect's cell phone, this method of investigation is currently subject to fewer constitutional constraints. As a result, police agencies are utilizing this form of tracking more frequently. Indeed, the number of requests to cell carriers for location information has grown "exponentially" over the past several years, with major wireless carriers now receiving thousands of requests each month. 114

Cell phone tracking by law enforcement comes in two primary forms. In the most precise form of tracking, cell phone providers are able to monitor a cell phone's location, and subsequently transmit that information to law enforcement anytime a user activates the GPS on such a phone. This method of tracking is used by law enforcement thousands of times each year and is becoming more common. 116

United States v. Jones 117 illustrates how this form of cell phone tracking may be used. In Jones, agents obtained a search warrant authorizing them to receive "pings" with the location of a suspect's cell phone for a thirty-day period. 118 Thereafter, Sprint provided information to an officer via e-mails sent directly to the officer's phone. 119 The e-mails contained longitudinal and latitudinal coordinates and a link to a map indicating the phone's exact location, accurate to

224

the Fourth Amendment," but ultimately ruling that the government's failure to get a warrant to authorize its use of GPS tracking devices does not require suppression of evidence due to the Davis good-faith exception); Kelly v. State, 56 A.3d 523, 538-41 (Md. Ct. Spec. App. 2012) (holding that the installation and use of GPS tracking device on defendant's vehicle involved a physical "trespass," thus constituting a Fourth Amendment "search;" but that evidence obtained from the GPS device was admissible under the good-faith exception); United States v. Hardrick, 2012 WL 4883666, at \*5 (E.D. La. Oct. 15, 2012) (refusing to decide the constitutionality of acquiring cell-site location information because the goodfaith exception applied and was dispositive of the defendant's motion to suppress). See also Kelly, 56

A.3d at 540-41 (summarizing similar cases).

<sup>114.</sup> Stephanie K. Pell & Christopher Soghoian, Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data that Congress Could Enact, 27 Berkeley Tech. L.J. 117, 121 (2012) (citing Michael Isikoff, The Snitch in Your Pocket, NEWSWEEK (Feb. 18, 2010, 7:00 PM), http://www.newsweek.com/2010/02/18/the-snitch-in-your-pocket.html).

<sup>115.</sup> United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

<sup>116.</sup> Jeremy H. Rothstein, Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest, 81 FORDHAM L. REV. 489, 491 (2012). According to Rothstein, all cell phones sold since 2003 are GPS-enabled, making most phones today at least potentially trackable. However, a user can disable her phone's GPS. Moreover, whether a phone transmits GPS data may depend on the network and on the phone's applications. *Id.* at 493.

<sup>117. 2012</sup> WL 2568200 (M.D. Ala. June 15, 2012).

<sup>118.</sup> Id. at \*1.

<sup>119.</sup> Id. at \*1 n.2.

within just a few meters.<sup>120</sup> Using this data, officers were able to determine the suspect's location, initiate a traffic stop, and eventually discover large amounts of illegal narcotics in the suspect's vehicle.<sup>121</sup> As this case exemplifies, pinging a cell phone in this manner allows law enforcement to remotely obtain the precise location of a suspect's cell phone in real time, information that may later lead to the discovery of incriminating evidence.<sup>122</sup>

225

In another, similar form of cell phone tracking, police are able to obtain cell phone location data by identifying which cell tower communicated with the cell phone while the phone was either turned on or utilized to make a call. Using this technique, a suspect's location can often be determined through methods of triangulation from various cell towers, 124 although the precision of cell site data may depend on the distance between cell towers in the user's vicinity, 125 especially where triangulation is not employed. Cell phone companies maintain records of this information 127—usually when a phone sends and receives text messages and at the beginning and end of each call 128—making it possible for law enforcement to request either "real time" cell site information or "historical" cell site information.

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

<sup>120.</sup> *Id.* Ultimately, this investigative technique was declared constitutional because it had been authorized by a valid warrant. *See id.* at \*4.

<sup>121.</sup> See id. at \*2.

<sup>122.</sup> See also United States v. Orbegoso, 2013 WL 161194 (D. Ariz. Jan. 15, 2013) (describing an investigation where law enforcement employed both surreptitiously installed GPS tracking devices and cell phone tracking).

<sup>123.</sup> United States v. Benford, 2010 WL 1266507, at \*1 (N.D. Ind. Mar. 26, 2010). Moreover, as Justice Alito notes in *Jones*, "phone-location-tracking services are offered as 'social' tools, allowing consumers to find (or to avoid) others who enroll in these services." United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

<sup>124.</sup> United States v. Suarez-Blanca, 2008 WL 4200156, at \*10 (N.D. Ga. Apr. 21, 2008). *See also In re* Applications of the United States, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) ("[C]ell site information coupled with a basic knowledge of trigonometry makes it possible to identify with reasonable certainty the location from which a call was made.").

<sup>125.</sup> See United States v. Hardrick, 2012 WL 4883666, at \*3 (E.D. La. Oct. 15, 2012) (noting that "the more cell-site tower locations in a given area, the more precise the location information can be for a user's particular call" and that "densely populated regions are equipped with more cell-site towers").

<sup>126.</sup> As one court has noted, cell towers can be up to ten or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas. *See In re* Application of the United States, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005).

<sup>127.</sup> See In re Application of the United States, 809 F. Supp. 2d 113, 115 (E.D.N.Y. 2011) ("If a user's cell phone has communicated with a particular cell-site, this strongly suggests that the user has physically been within the particular cell-site's geographical range. By technical and practical necessity, cell-phone service providers keep historical records of which cell-sites each of their users' cell phones have communicated. The implication of these facts is that cellular service providers have records of the geographic location of almost every American at almost every time of day and night.").

<sup>128.</sup> Rothstein, supra note 116, at 494.

<sup>129.</sup> See In re Application of the United States, 405 F. Supp. 2d at 437 ("As a cell phone user moves from place to place, the cell phone automatically switches to the tower that provides the best

site information, law enforcement may request all such data accumulated over a period of time in the past; by contrast, with real-time data, law enforcement may seek to obtain this information on a real-time basis into the future. The tracking of a cell phone in this manner does not require the installation of any device, hence no trespass; rather, the phone itself does the work.

As technology evolves, cell site location information is becoming just as accurate, and in some instances even more so, than alternative forms of GPS tracking, a development that supports my proposal to treat all forms of electronic monitoring alike for purposes of the Fourth Amendment. This evolution has two primary causes. First, due to the massive increase in the use of data by cell phone users in recent years (AT&T, for example, experienced an 8,000 percent increase in data traffic from 2007 to 2010), <sup>132</sup> carriers have been forced to deploy new cell sites and reduce the coverage area of existing cell towers, which, in turn, makes cell site data more accurate. 133 Second, new technologies including microcell, picocell, and femtocell technology <sup>134</sup>—have the potential to make cell site location information more accurate than GPS. Because these technologies often broadcast a signal no farther than a subscriber's home, single cell site location data can in some cases be more accurate than GPS. 135 For example, in urban areas where microcell technology is used, a cell phone's location can be identified on an individual floor or room within a building. 136

In striking down the warrantless use of a GPS tracking device in *Jones*, the majority based its decision on the physical trespass that was required to monitor the vehicle's movements. <sup>137</sup> *Jones* did not address the constitutionality of obtaining similar tracking information in the absence of a trespass, including location information obtained directly

reception," which in turn enables the Government to obtain "cell-site information concerning the physical location of the antenna towers associated with the beginning and termination of calls to and from a particular cellphone."). See also id. at 447 (noting the distinction between requests for "historical versus real time data").

<sup>130.</sup> See United States v. Jones, 908 F. Supp. 2d 203, 207 (D.D.C. 2012).

<sup>131.</sup> In re Application of the United States, 809 F. Supp. 2d at 81 n.11.

<sup>132.</sup> Pell & Soghoian, supra note 114, at 132.

<sup>133.</sup> Id. at 132-33.

<sup>134.</sup> For a description of this technology, see id. at 132.

<sup>135.</sup> See id.

<sup>136.</sup> Id. at 137.

<sup>137.</sup> According to the majority, "the Government's *installation* of a GPS device on a target's vehicle, *and its use* of that device to monitor the vehicle's movements, constitutes a 'search.'" United States v. Jones, 132 S. Ct. 945, 951. Crucial to the majority's analysis is the fact that "Jones... possessed the Jeep at the time the Government trespassorily inserted the [GPS] device." *Id.* at 952.

from a suspect's cell phone provider. According to *Jones*, the constitutionality of non-trespassory forms of GPS tracking, like cell phone tracking, would be governed by *Katz*.

Under the *Katz* framework, obtaining tracking information directly from a third-party provider is arguably not a "search" under the Supreme Court's assumption of risk rationale, which posits that one cannot reasonably expect privacy in certain types of "addressing information" knowingly disclosed to a third party, <sup>139</sup> such as a telephone company. <sup>140</sup> Indeed, many courts have likened this form of evidence to company business records, which are generally unprotected by the Fourth Amendment. <sup>141</sup> If this rationale is applied to instances of cell phone tracking, this method of investigation would fall outside the Fourth Amendment's protections altogether, regardless of the volume of data requested or the length of surveillance. *United States v. Graham*, <sup>142</sup> decided just a few weeks after *Jones*,

United States v. Graham, <sup>142</sup> decided just a few weeks after Jones, illustrates the potential application of the assumption of risk rationale to the warrantless gathering of historical cell site location information (CSLI). In Graham, a federal District Court ruled that the government does not need probable cause or a warrant to obtain more than seven months of CSLI from a cell phone provider. <sup>143</sup> In that case, two defendants were thought to have conducted a series of armed robberies, and a key piece of evidence linking them to each robbery was data about the movements of their cell phones. <sup>144</sup> The defendants sought to

<sup>138.</sup> *Id.* at 954 (Sotomayor, J., concurring). *See also* People v. Weaver, 12 N.Y.3d 433, 442 (2009) ("[W]ith GPS becoming an increasingly routine feature in cars and cell phones, it will be possible to tell from the technology with ever increasing precision who we are and are not with, when we are and are not with them, and what we do and do not carry on our persons—to mention just a few of the highly feasible empirical configurations.").

<sup>139.</sup> See Smith v. Maryland, 442 U.S. 735, 741–43 (1979) (distinguishing the content of communications, which are protected by the Fourth Amendment, and the addressing information associated with those communications, which are not, and reasoning: "[t]elephone users . . . typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. . . . [I]t is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.").

<sup>140.</sup> The government advanced this argument in *United States v. Graham*, 846 F. Supp. 2d 384 (D. Md. 2012), a case decided less than two months after *Jones. See id.* at 388.

<sup>141.</sup> See, e.g., id. at 398 ("Like the bank records at issue in Miller [which are not protected by the Fourth Amendment], the historical cell site location records in this case are not the 'private papers' of the Defendants—instead, they are the 'business records' of the cellular providers... and are not protected by the Fourth Amendment.").

<sup>142.</sup> *Id*.

<sup>143.</sup> Id. at 394-95.

<sup>144.</sup> On March 25, 2011, the government applied for an order from a magistrate judge pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701–2712, "which ordered Sprint/Nextel, Inc. to disclose to the government 'the identification and address of cellular towers (cell site locations) related

suppress this evidence because the government did not obtain a warrant authorizing its acquisition. Rejecting the defendant's argument, the court ruled that the defendants "[lacked] a legitimate expectation of privacy in the historical cell site location records acquired by the government." According to the court, "[l]ike the dialed telephone numbers in *Smith*, the [d]efendants in this case voluntarily transmitted signals to cellular towers in order for their calls to be connected," and "[t]he cellular provider then created internal records of that data for its own business purposes." 148

In reaching this result, the *Graham* court described *Jones* as "relevant but not controlling in this case." The court distinguished *Jones* on the grounds that historical cell site location data exposes only historical evidence of a suspect's past locations, whereas GPS technology reveals the location and movements of a suspect in real time and is "far more precise than the historical cell site location data at issue here." <sup>151</sup>

Like *Graham*, a majority of courts to have considered the constitutionality of acquiring historical cell site location information have invoked *Smith*'s assumption of risk rationale, effectively eliminating Fourth Amendment protection, regardless of the volume of

to the use of the [Defendants' cellular telephones]." *Id.* at 386. The government sought cell site location data for the periods of August 10–15, 2010; September 18–20, 2010; January 21–23, 2011; and February 4–5, 2011. *Id.* In its application, the government alleged that the information sought was relevant to an ongoing investigation of robberies the defendants were suspected of committing. *Id.* "By identifying the location of cellular towers accessed by the defendants' phones during the relevant time periods, the government sought to more conclusively link the defendants with the prior robberies." *Id.* The magistrate judge issued the order under the reasonable suspicion standard utilized by the Stored Communications Act. *Id.* In a second order, the Government sought cell site location data for the periods July 1, 2010 through February 6, 2011. This order was granted by a separate magistrate judge under the same reasonable suspicion standard. *Id.* The government's request resulted in the release of almost 22,000 individual cell site location data points. *Id.* at 387.

145. *Id.* The *Graham* defendants did not argue that the Stored Communications Act is unconstitutional on its face, but instead argued that the length of time and extent of the cellular phone monitoring conducted in their particular case intruded on their expectation of privacy and was therefore unconstitutional. *Id.* 

146. Id. at 389.

147. *Id*.

148. *Id. See also id.* at 399 ("Like the bank records at issue in *Miller*, [and] the telephone numbers dialed in *Smith*..., historical cell site location records are records created and kept by third parties that are voluntarily conveyed to those third parties by their customers. As part of the ordinary course of business, cellular phone companies collect information that identifies the cellular towers through which a person's calls are routed.").

149. Id. at 406 n.2.

150. While this may be a plausible distinction of *Jones*, the distinction would not apply in those instances in which the government seeks "real time" cell site information. *See In re* Application of the United States, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (noting the distinction between requests for "historical versus real time data").

151. Graham, 846 F. Supp. 2d at 392.

information obtained.<sup>152</sup> However, not all courts have chosen to follow *Graham*'s approach, especially for larger volumes of data acquired over lengthier periods of time.<sup>153</sup>

229

Given the concurring Justices' opinions in *Jones*, this complex issue should not be resolved by such a simple application of the assumption of risk doctrine, especially when one considers the inability of that doctrine to account for the realities of the digital age. Cell site location information enables the Government to obtain nearly the same type and volume of location information provided by the surreptitiously-installed GPS device utilized in *Jones*, especially if a suspect is a frequent phone user, thereby implicating the very concerns of the five Justices who concurred in *Jones* regarding the aggregation of various bits of private information. According to Justice Sotomayor's opinion, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," all highly private and intimate matters. Moreover, the longer that an individual is tracked by GPS, the more data that can be accumulated, naturally

<sup>152.</sup> See, e.g., United States v. Dye, No. 1:10CR221, 2011 WL 1595255, at \*9 (N.D. Ohio Apr. 27, 2011); United States v. Velasquez, No. CR 08-0730 WHA, 2010 WL 4286276, at \*5 (N.D. Cal. Oct. 22, 2010); United States v. Benford, No. 2:09 CR 86, 2010 WL 1266507, at \*3 (N.D. Ind. Mar. 26, 2010); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 WL 4200156, at \*8-11 (N.D. Ga. Apr. 21, 2008); In re Applications of the United States, 509 F. Supp. 2d 76, 80-81 (D. Mass. 2007).

<sup>153.</sup> See, e.g., In re Application of the United States, 809 F. Supp. 2d 113, 118–19 (E.D.N.Y. 2011) ("Here, the Government has requested... at least 113 days of constant surveillance of an individual.... [T]he application seeks information that is protected by the Fourth Amendment.... The cell-site-location records sought here captures enough of the user's location information for a long enough time period—significantly longer than the four weeks in Maynard—to depict a sufficiently detailed and intimate picture of his movements to trigger the same constitutional concerns as the GPS data in Maynard.").

<sup>154.</sup> See United States v. Jones, 132 S. Ct. 945, 955–57 (2012) (Sotomayor, J., concurring) (agreeing with Justice Alito that long-term GPS monitoring "impinges on expectations of privacy" with or without a physical intrusion, and noting that individuals often have no choice but to reveal private information to third parties (e.g., calls and texts to and from cell phones, internet browsing history) and yet still would be offended by government monitoring of the very same data). See also McAllister, supra note 29, at 520–21 (2012).

<sup>155.</sup> See Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring) (expressing her concern that, "[w]ith increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting . . . GPS-enabled smartphones"). Perhaps the primary factor noted by the concurring Justices in Jones was the length of surveillance. See id. at 961 (Alito, J., concurring) ("the Court's reasoning largely disregards what is really important (the use of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)"). See also In re Application of the United States, 809 F. Supp. 2d at 118–19.

<sup>156.</sup> Jones, 132 S. Ct. at 955 (Sotomayor, J., concurring).

<sup>157.</sup> See id. (Sotomayor, J., concurring) (describing "GPS monitoring" as "making available at a relatively low cost...a substantial quantum of intimate information about any person whom the Government...chooses to track").

leading to a greater invasion of privacy. These concerns apply to both GPS tracking in the manner employed in *Jones* and GPS tracking accomplished via cell phone. In her *Jones* opinion, Justice Sotomayor further reasoned, "[a]wareness that the Government may be watching chills associational and expressive freedoms." Again, this is true of both GPS tracking in the manner employed in *Jones* and GPS tracking accomplished via cell phone—perhaps even more so with respect to cell phone tracking given the inherently tighter connection between a person's phone and her First Amendment rights. Finally, in neither case does the suspect know his location is being tracked by government agents. With very little difference between the types of information provided by both forms of investigation, and very little difference in the manner in which the information is conveyed to police, acquisition of this type of information should be more carefully analyzed by taking into account the opinions of the *Jones* concurring Justices.

In cases that have rejected or failed to employ the assumption of risk doctrine, leading to a more precise *Katz*-based analysis, courts have begun to draw lines based upon the factors noted by Justice Alito—most notably, the length of surveillance. Employing *Katz*, several post-*Jones* courts have ruled that tracking a suspect for only a few days, whether through cell phone tracking or through more traditional forms of GPS tracking, does not constitute a Fourth Amendment "search."

For example, in *United States v. Skinner*, <sup>162</sup> the United States Court of Appeals for the Sixth Circuit examined whether the tracking of a cell phone for three days constituted a "search" under *Katz*. In that case, DEA agents discovered a large-scale drug-trafficking operation after arresting one of its participants, Christopher Shearer, who then divulged information about the scheme. <sup>163</sup> According to Shearer, the operation's marijuana supplier, Philip Apodaca, used couriers to send marijuana from his home in Arizona to another participant, James Michael West, in Tennessee. <sup>164</sup> The defendant, Melvin Skinner, was one of those couriers. Agents also learned from Shearer that Apodaca purchased

<sup>158.</sup> According to Justice Sotomayor, "[t]he Government can store such records and efficiently mine them for information years into the future." *Id.* at 955.

<sup>159.</sup> Id. (Sotomayor, J., concurring).

<sup>160.</sup> Rothstein, *supra* note 116, at 495 (2012) (noting that judicial orders authorizing cell phone tracking are usually accompanied by a gag order preventing the service provider from notifying consumers that the government is accessing their location information, and that associated records are usually placed under indefinite seal).

<sup>161.</sup> See supra notes 70–79 and accompanying text. As the *Jones* majority noted, the inside/outside distinction between *Knotts* and *Karo* is also potentially relevant here. See supra notes 59–63 and accompanying text.

<sup>162.</sup> United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

<sup>163.</sup> Id. at 775.

<sup>164.</sup> *Id*.

pay-as-you-go cell phones that he programmed with contact information and then gave to the couriers to maintain communication. Apodaca was unaware that these phones were equipped with GPS technology. <sup>165</sup>

In late June 2006, agents learned that Skinner would meet Apodaca in Arizona on July 11 to pick up approximately 900 pounds of marijuana for transport to Tennessee on July 13. In the meantime, agents obtained an order from a magistrate judge on July 12 authorizing the phone company to release subscriber information, cell site information, GPS real-time location, and "ping" data for the cell phone thought to be used by Skinner. That same day, agents "pinged" this particular cell phone and discovered that it was then located near West's primary residence. Agents subsequently determined that West, rather than Skinner, was using this particular phone.

Agents then obtained a second judicial order authorizing release of the same information for the phone actually being used by Skinner, which revealed that the phone was located near Flagstaff, Arizona. By continuously "pinging" the second phone, authorities learned that Skinner left Arizona on July 14 and was traveling across Texas. At no point did agents follow the vehicle or conduct any type of visual surveillance. 169

At around 2:00 a.m. on July 16, the GPS indicated that Skinner's phone had stopped near Abilene, Texas. DEA agents in that area were then dispatched to a nearby truck stop, where they discovered Skinner's vehicle. After a dog sniff alerted to the presence of narcotics, officers searched the vehicle and discovered over 1,100 pounds of marijuana. 170

Prior to trial, Skinner sought to suppress the evidence obtained from his vehicle, arguing that the agents' use of GPS location information emitted from his cell phone was a warrantless search that violated the Fourth Amendment. The trial court, however, denied his motion. In affirming that decision, the Sixth Circuit analogized the case to *Knotts* and distinguished it from *Jones*.

<sup>165.</sup> *Id.* After some time, the drug conspirators would discard their pay-as-you-go phones and get new ones with different telephone numbers and fictitious names. *Id.* 

<sup>166.</sup> Id. at 775-76.

<sup>167.</sup> Id.

<sup>168.</sup> Id.

<sup>169.</sup> Id.

<sup>170.</sup> *Id.* Skinner was subsequently charged with conspiracy to distribute and possess with intent to distribute in excess of 1,000 kilograms of marijuana, in violation of 21 U.S.C. §§ 846, 841(a)(1), and 841(b)(1)(A), conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h), and aiding and abetting the attempt to distribute in excess of 100 kilograms of marijuana, in violation of 21 U.S.C. §§ 846, 841(a)(1), 841(b)(1)(B), and 18 U.S.C. § 2. *Id.* 

<sup>171.</sup> Id.

<sup>172.</sup> See id. at 777 (describing the lower court proceedings).

According to the *Skinner* court, as in *Knotts*, Skinner was traveling on public roads throughout his journey. <sup>173</sup> As such, "[w]hile the cell site information aided the police in determining Skinner's location, that same information could have been obtained through visual surveillance" along Skinner's public route. <sup>174</sup>

In distinguishing *Jones*, the *Skinner* court first reasoned that, unlike in *Jones* where police physically intruded upon a constitutionally-protected area by attaching the GPS tracking device to Jones's vehicle, "[n]o such physical intrusion occurred in [this] case." Rather, "Skinner['s]... phone included the GPS technology used to track the phone's whereabouts," thereby rendering the *Jones* majority's trespass concerns inapplicable.

Responding to Justice Alito's concerns regarding the comprehensive tracking of a suspect's movements, the *Skinner* court further declared that "[n]o such extreme comprehensive tracking is present . . . [where] the DEA agents only tracked Skinner's cell phone for three days." According to the court, such "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable." This is because, as the court declared, "the monitoring of the . . . vehicle as it crossed the country is no more of a comprehensively invasive search than if instead the car was identified in Arizona and then tracked visually, and the search handed off from one local authority to another as the vehicles progressed," thereby eliminating any expectation of privacy Skinner may have had in his location. In *State v. Estrella*, 181 a case similar to *Jones*, in that agents

In State v. Estrella, or a case similar to Jones, in that agents trespassorily attached a GPS tracking device to a suspect's vehicle, the Court of Appeals of Arizona deemed any trespass-based argument from Jones to have been waived and therefore analyzed the issue under

<sup>173.</sup> *Id*.

<sup>174.</sup> Id.

<sup>175.</sup> Id. at 779-80.

<sup>176.</sup> *Id.* at 780. Later, invoking the *Jones* Court's discussion of *Karo*, the *Skinner* court reasoned, "the Government never had physical contact with Skinner's cell phone; he obtained it, GPS technology and all, and could not object to its presence." *Id.* at 781.

<sup>177.</sup> Id. at 780.

<sup>178.</sup> Id. (citations omitted).

<sup>179.</sup> Id.

<sup>180.</sup> *Id.* at 781. The court declared that no Fourth Amendment violation would have occurred even if the agents had not obtained court orders authorizing the GPS tracking of Skinner's cell phone. *See id.* at 779 ("Although not necessary to find that there was no Fourth Amendment violation in this case, the Government's argument is strengthened by the fact that the authorities sought court orders to obtain information on Skinner's location from the GPS capabilities of his cell phone.").

<sup>181.</sup> State v. Estrella, 286 P.3d 150 (Ariz. Ct. App. 2012).

Katz. 182 In Estrella, DEA agents, acting without a warrant, placed a GPS tracking device on a van after discovering that the van was being used to transport illegal drugs. 183 Similar to *Jones*, agents attached the device while the van was parked in a public parking lot. 184 Also similar to *Jones*, agents then used the device to monitor the van's movements. 185

233

After the GPS device indicated the van was traveling in a direction that corresponded with allegations of illegal drug distribution, agents then contacted Arizona state police and informed them that the van might be transporting marijuana. In response, Arizona police located the van and pulled it over. Upon discovering that the driver, defendant Estrella, had an outstanding arrest warrant, agents arrested Estrella and searched the van, which yielded bundles of marijuana.

Estrella later moved to suppress the marijuana, alleging that the warrantless placement and use of the GPS device violated his Fourth Amendment rights. The trial court, however, denied the motion. On appeal, the court found Estrella to have waived any argument under the trespass theory espoused in *Jones* and instead addressed whether Estrella could assert a successful *Katz* claim.

In rejecting Estrella's claim, the court presented two, intertwined rationales. Most importantly, the court declared that, "generally '[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another," and that "[t]his is true particularly where the government's monitoring is short-term." Given the limited use of the GPS device,

```
182. Id. at 152-53.
```

<sup>183.</sup> Id. at 151.

<sup>184.</sup> Id.

<sup>185.</sup> Id.

<sup>186.</sup> *Id*.

<sup>187.</sup> *Id*.

<sup>188.</sup> *Id*.

<sup>189.</sup> Id. at 151-52.

<sup>190.</sup> Estrella was later convicted. Id. at 152.

<sup>191.</sup> Id.

<sup>192.</sup> Id. at 152-53.

<sup>193.</sup> Id. at 153.

<sup>194.</sup> The first rationale was based on the defendant's lack of standing. According to the court, "Estrella provided no evidence he had permission to drive the van or otherwise had any interest in it when the device was attached to the vehicle in a public parking lot," presumably defeating his claim to an expectation of privacy in that vehicle. *Id.* at 154.

<sup>195.</sup> Id. at 153 (citing United States v. Knotts, 460 U.S. 276, 281 (1983)).

<sup>196.</sup> *Id.* (quoting United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (short-term monitoring of person's movements in public "accords with expectations of privacy that our society has recognized as reasonable")). According to the court, this is particularly true where "the driver has borrowed another's vehicle without any knowledge of whether it is being tracked by a GPS device"

the court refused to address "the hypothetical situation Justice Sotomayor's observation suggests, in which GPS tracking is used to aggregate large amounts of personal data for a much longer period of time, or on a purely arbitrary basis." 197

In a similar case, *United States v. Luna-Santillanes*, <sup>198</sup> where agents installed multiple GPS tracking devices on vehicles driven by three suspects, <sup>199</sup> the court rejected *Jones*'s trespass approach and held that a one-day track of a suspect's vehicle was not a "search" under *Katz*. In the relevant portion of the opinion, the court analyzed whether a Fourth Amendment violation occurred when police attached a GPS tracking device to a red Lincoln Aviator and used that device to monitor the Aviator's movements for one day. <sup>200</sup> According to the court, the two defendants who objected to this monitoring, neither of whom were present at the time the Aviator was searched, did not have standing to object to that action, <sup>201</sup> making *Jones*'s trespass rationale inapplicable.

Next, and more significantly, the court applied the *Katz* test and concluded that "even if Defendants could establish that they had standing to challenge the . . . search and seizure of the red Lincoln Aviator, the one-day monitoring of that vehicle" was not a Fourth

because "[f]rom the reasonable borrower's perspective, it is entirely possible the owner has permitted the installation of such a device." *Id.* at 153–54.

<sup>197.</sup> *Id.* at 154. According to the court, "[t]he determination of whether that type of surveillance may intrude on a person's reasonable expectations of privacy, and accordingly run afoul of constitutional standards, must wait until the issue is presented." *Id.* 

<sup>198.</sup> United States v. Luna-Santillanes, No. 11-20492, 2012 WL 1019601 (E.D. Mich. Mar. 26, 2012).

<sup>199.</sup> See id. at \*2–3 (describing the warrantless attachment and subsequent monitoring of GPS tracking devices to three vehicles being driven by defendants, a red Lincoln Aviator, a silver Chrysler Sebring, and a black Mazda).

<sup>200.</sup> According to the facts as described by the *Luna-Santillanes* court, DEA agents installed a GPS device on the red Lincoln Aviator on April 13, 2011. *See id.* at \*2. On April 14, 2011, DEA agents used the GPS device on the Aviator to monitor its movements, through which agents were able to determine that the Aviator had traveled to Chicago and was on its way back to the Detroit area. At that point, DEA agents requested assistance by the Michigan State Police to conduct a traffic stop of the Aviator. *Id.* Once the vehicle was stopped, the driver and sole occupant consented to a search of the vehicle, which produced two kilograms of heroin. *Id.* After this search, the GPS tracking device was removed within hours, *id.* at \*7, such that the GPS device was on the Aviator "for two days at the most." *Id.* at \*7 n.4.

<sup>201.</sup> *Id.* at \*6. According to the court, unlike the defendant in *Jones*, neither defendant at issue could establish that they were the "exclusive driver" of the vehicle, and the vehicle was not registered to either defendant. *Id.* 

<sup>202.</sup> See id. at \*6 (reasoning that, due to the lack of standing in the vehicle at issue, "unlike the defendant in Jones, D-1 and D-2 cannot persuasively argue that '[t]he Government usurped [their] property for the purpose of conducting surveillance on [them], thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection."") (quoting United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring)).

Amendment violation.<sup>203</sup> With little discussion of this issue, the court simply reasoned that "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable."<sup>204</sup>

235

As *Skinner*, *Estrella*, and *Luna-Santillanes* make clear, tracking a suspect's vehicle by GPS for only a few days likely does not constitute a "search" under a *Katz*-based analysis. Thus, while the opinions of the five concurring Justices in *Jones* indicate that a suspect similar to Antoine Jones can reasonably expect privacy in his movements in public where those movements are tracked for twenty-eight days or longer, these more recent decisions indicate that a person traveling on public roads over a few days cannot reasonably expect privacy in those movements. Exactly where the line of protection begins between these two points remains unclear.

#### IV. SURVEY RESULTS

As recent GPS tracking cases illustrate, tracking a suspect by GPS for only a few days likely does not constitute a "search" under the *Katz* test, an approach that seemingly complies with Justice Alito's opinion in *Jones*. However, tracking a suspect for a lengthier period of time likely does constitute a "search" under the *Katz* test. As Justice Alito noted in *Jones*, however, the result in such cases might depend on the actual crime under investigation. In the months following *Jones*, I administered two surveys designed to test Justice Alito's suggestion. I designed each survey with the help of an instructional design consultant, who ensured the validity of each survey instrument. This section sets forth the detailed results of each of these surveys.

#### A. Overall Survey Design

A court analyzing a "search" issue under *Katz* must consider whether "society is prepared to recognize [a defendant's asserted expectation of privacy] as reasonable." Taken literally, the *Katz* inquiry anticipates at least some assessment of society's actual expectations of privacy, as

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

<sup>203.</sup> United States v. Luna-Santillanes, No. 11-20492, 2012 WL 1019601, at \*7 (E.D. Mich. Mar. 26, 2012).

<sup>204.</sup> Id. (quoting Jones, 132 S. Ct. at 964 (Alito, J., concurring)).

<sup>205.</sup> See Jones, 132 S. Ct. at 964 (Alito, J., concurring).

<sup>206.</sup> See supra note 30.

<sup>207.</sup> See Katz v. United States, 389 U.S. 347, 360 (Harlan, J., concurring) ("there is a twofold requirement, first 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.").

opposed to an analysis that entirely disregards society's views.<sup>208</sup>

According to Fourth Amendment scholar Christopher Slobogin, there are at least two ways to determine societal attitudes about privacy. The first is to examine property, contract, and tort doctrine for clues as to what society believes is private. For example, in the context of GPS tracking, the California legislature has made it unlawful for private citizens to "use an electronic tracking device to determine the location or movement of a person" and has specifically declared that "electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy."

A second method is to simply pose the question to society.<sup>211</sup> This form of empirical analysis is gaining acceptance among legal scholars, particularly under the Fourth Amendment, where scholars have employed the empirical approach to analyze various Fourth Amendment "search" issues.<sup>212</sup> My surveys follow in the footsteps of similar surveys conducted by Christopher Slobogin and Joseph Schumacher.

In 1993, Slobogin and Schumacher conducted a survey, completed by 217 individuals, which included fifty scenarios involving various forms of police investigation. Several years later, Slobogin conducted a second survey, completed by 190 people, which contained twenty police investigation scenarios. 190 people, which contained twenty police investigation scenarios.

In each of these studies, the subjects were asked to rate each investigative method in terms of "intrusiveness" on a scale of 1 to 100, with 1 representing "not intrusive" and 100 representing "very

<sup>208.</sup> Scholars agree. See, e.g., CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 33 (University of Chicago Press 2007) (arguing that "some assessment of societal attitudes about the relative intrusiveness of police actions should inform the analysis" under Katz and noting that "the Court has pretty much ignored this precept, with predictably anomalous results"); Stephen E. Henderson, Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34 PEPP. L. REV. 975, 1000 (2007) ("I part with the High Court . . . on its refusal to determine those expectations [of privacy] in any rational manner. Rather than grapple with the complications of surveys or other evidence, the Court has been content to declare societal expectations without any foundation or support. . . . Either courts should look to academic empirical studies like those done by Professor Slobogin (in which case we need more like them), or litigants should prepare relevant surveys" of their own.).

<sup>209.</sup> SLOBOGIN, supra note 208, at 33.

<sup>210.</sup> Cal. Penal Code § 637.7. Other states have enacted similar legislation. *See, e.g.*, Utah Code Ann. §§ 77-23a-4, 77-23a-7, 77-23a-15.5; Minn. Stat. §§ 626A.37, 626A.35; Fla. Stat. § 934.42; S.C. Code Ann. § 17-30-140; Okla. Stat. tit. 13, §§ 176.6, 177.6; Haw. Rev. Stat. §§ 803-42, 803-44.7; 18 Pa. Cons. Stat. § 5761.

<sup>211.</sup> SLOBOGIN, supra note 208, at 33.

<sup>212.</sup> See, e.g., SLOBOGIN, supra note 208, at 112, 184 (tables reporting empirical data).

<sup>213.</sup> Christopher Slobogin & Joseph E. Schumacher, Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society", 42 DUKE L.J. 727 (1993).

<sup>214.</sup> See SLOBOGIN, supra note 208, at 110–11 (describing survey design).

intrusive."<sup>215</sup> Slobogin and Schumacher hypothesized that "many of the Court's conclusions about expectations of privacy and autonomy do not correlate with actual understandings of innocent members of society."<sup>216</sup> As Slobogin and Schumacher demonstrated, judicial conclusions about expectations of privacy do not always correlate with actual expectations of privacy among society.<sup>217</sup>

237

My surveys are similar to the Slobogin and Schumacher surveys but contain key differences. Most significantly, unlike the Slobogin and Schumacher surveys, in which survey participants were instructed to numerically assess the extent to which they considered each method "an invasion of privacy or autonomy," my surveys simply ask respondents to indicate whether they believe police should have to obtain a search warrant before undertaking each type of activity identified by the survey instrument. Thus, my survey employs a simple "yes" or "no" option, rather than a 100-point scale of invasiveness. This binary method more closely follows the analysis required by *Katz*, which effectively requires a reviewing court to determine whether society does, or does not, expect privacy in the particular case at hand.

#### B. GPS Tracking Survey

My first survey focuses exclusively on GPS tracking of the type that occurred in *Jones*—i.e., where officers surreptitiously attach a GPS tracking device to a suspect's vehicle and subsequently use that device to monitor the vehicle's movements for a period of time. This survey poses a series of questions involving GPS tracking of seven different types of suspects, including: individuals not suspected of any crime,

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

<sup>215.</sup> *Id.* at 111. *See also* Slobogin & Schumacher, *supra* note 213, at 735–36. According to Slobogin and Schumacher, "[w]ith respect to searches, we wanted to discover [society's] expectations of privacy in the searched area." *Id.* at 733. To uncover those expectations, Slobogin and Schumacher sought evidence regarding "how society perceives the 'intrusiveness' of government investigative methods." *Id.* According to the researchers, "[u]sing the single word 'intrusiveness' is less cumbersome than speaking about the impact of government conduct on reasonable expectations of privacy.... At the same time, 'intrusiveness' captures the core of the construct we sought to investigate...." *Id.* 

<sup>216.</sup> Id. at 733-34.

<sup>217.</sup> See id.

<sup>218.</sup> Among other differences, my survey examines particular "search" issues not examined by Slobogin and Schumacher. For example, my survey includes questions relating to police access of computer files and records, including the issues presented in *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2007), ones not included in Slobogin's surveys.

<sup>219.</sup> Slobogin & Schumacher, supra note 213, at 735–36.

<sup>220.</sup> Note, however, that the GPS tracking questions contain three overall options as to whether GPS tracking should be allowed in the absence of a warrant: (1) "Yes, indefinitely," (2) "No," and (3) "Yes, but only for a limited time." If a respondent selects choice (3), she is then presented with an additional question asking her to specify the acceptable length of warrantless tracking.

individuals suspected of minor crimes, and individuals suspected of relatively more severe crimes.

This survey considered the following suspects: (1) a person who has not been convicted of a previous crime and who is currently not suspected of committing any crime (i.e., an "innocent suspect"); (2) a person who has not been convicted of a previous crime but who is currently suspected of having committed an unspecified crime; (3) a person who is a convicted felon, but who is not currently suspected of committing another crime; (4) a person who is a convicted felon, and who is currently suspected of committing another, unspecified crime; (5) a suspected terrorist; (6) a suspected drug dealer; and (7) a suspected serial killer.

Tracking Justice Alito's suggestion in *Jones*, which highlights the type of crime under investigation and the length of surveillance as potential factors under *Katz*, my first hypothesis was that society would generally believe that Fourth Amendment protections should vary based upon the nature of the crime under investigation. Examining the other factor noted by Justice Alito, I further hypothesized that most people would be willing to vary Fourth Amendment protections based upon the length of surveillance. Combining the two, my basic hypothesis was that society would agree that Fourth Amendment protections should vary based upon the nature of the crime under investigation, and most people would permit police to engage in warrantless GPS tracking for a longer period of time when investigating the most serious offenses.

#### 1. Variations Based on the Type of Suspect

After collecting over 230 survey responses, I was able to verify my first hypothesis. For example, only 10.9% of survey respondents (25 of 230), would have permitted police to attach a GPS tracking device to the vehicle of an innocent suspect<sup>221</sup> and monitor that vehicle's movements without first obtaining a warrant. By contrast, when asked whether police should be permitted to monitor a suspected drug dealer's<sup>222</sup> vehicle by way of surreptitiously installed GPS, nearly half of all survey respondents, 47.1%, would have permitted this individual to be tracked without a warrant. Finally, when asked the same question regarding the tracking of a suspected terrorist, 67.3% of survey respondents would

<sup>221.</sup> As used here, the term "innocent suspect" refers to an individual who has not previously been convicted of a crime and who is not currently suspected of committing any crime.

<sup>222.</sup> Among the seven different types of suspects hypothesized by my survey, the *suspected drug dealer* represents the type of suspect that most closely approximates the suspect in *Jones*.

<sup>223.</sup> On this question, 20.6% of survey respondents would have permitted warrantless GPS tracking to extend twenty-one days or longer.

#### 2013] GPS AND CELL PHONE TRACKING

have permitted warrantless tracking.<sup>224</sup>

These trends were observed across all seven different types of suspects identified in this survey. Examining the seven suspect types, three distinct groups of suspects emerge. Group One includes innocent suspects who are not suspected of committing any crime, which encompasses Suspect Types 1 and 3. Group Two includes individuals who are either suspected of committing a minor crime or whose suspected crime was left unspecified, including Suspect Types 2, 4, and 6. Group Three includes suspects who are suspected of committing a severe crime, Suspect Types 5 and 7.

Group One includes the suspects who were presumed to be innocent. For Suspect Type 1, the innocent suspect not suspected of committing a crime, only 10.9% of survey respondents (25 of 230), would have permitted police to attach a GPS tracking device to the vehicle of this particular suspect and monitor that vehicle's movements without first obtaining a warrant. Similarly, for Suspect Type 3, the convicted felon who is not currently suspected of committing a crime, only 26.3% of survey respondents (60 of 228), would have permitted police to attach a GPS tracking device to this particular suspect's vehicle and monitor that vehicle's movements without first obtaining a warrant. Given these small percentages, society appears generally unwilling to permit warrantless GPS tracking of an innocent suspect.

By contrast, when we examine the results of the Group Three suspects, those suspected of committing a severe crime, society's views appear to flip. For Suspect Type 5, the suspected terrorist, 67.3% of survey respondents (152 of 226) would have permitted this individual to be tracked without a warrant. Likewise, for Suspect Type 7, the suspected serial killer, 64.8% of survey respondents (142 of 219) would have permitted this individual to be tracked without a warrant.

The Group Two suspects are in the middle, and they include those individuals who are either suspected of committing a minor crime or whose suspected crime was left unspecified: Suspect Types 2, 4, and 6.

For Suspect Type 2, a person who has not been convicted of a previous crime but who is currently suspected of having committed an unspecified crime, only 45.6% of survey respondents (103 of 226) would have permitted this individual to be tracked without a warrant, whereas 54.4% of respondents (123 of 226) would have required a

<sup>224.</sup> Of those respondents who would have permitted the tracking of a suspected terrorist in the absence of a warrant, 89 of 226 respondents, or 39.4%, would have permitted such an individual to be tracked without a warrant for twenty-one days or longer.

<sup>225.</sup> Among the entire cohort, almost 40% of respondents (90 of 226), would have permitted *the suspected terrorist* to be tracked without a warrant for a relatively lengthy period of time—i.e., twenty-one days or longer.

[VOL. 82

search warrant authorizing such tracking.

240

For Suspect Type 4, a person who is a convicted felon and currently suspected of committing an unspecified crime, 68.0% of survey respondents (153 of 225) would have permitted this individual to be tracked without a warrant, whereas only 32.0% of respondents (72 of 225) would have required a search warrant to do so.

Finally, for Suspect Type 6, a suspected drug dealer, 47.1% of survey respondents (105 of 223) would have permitted this individual to be tracked without a warrant, whereas 52.9% (118 of 223) believed police should have to obtain a warrant. Notably, for the suspected drug dealer, only about 1 in 5 respondents would have permitted warrantless GPS tracking to extend twenty-one days or longer, a result which lends strong empirical support for the Court's holding in *Jones*, where the Court unanimously invalidated the tracking of a suspected drug dealer for twenty-eight days without a valid warrant.<sup>226</sup>

#### 2. Variations on the Permissible Length of Surveillance

Regarding the permissible length of warrantless GPS tracking, the results of the first survey appeared to verify my second hypothesis that society would be willing to allow warrantless GPS tracking for a longer period of time when investigating the most serious offenses.

Beginning with the Group One suspects, society appeared unwilling to permit warrantless GPS tracking of an innocent suspect for any period of time. For Suspect Type 1, the innocent suspect not suspected of committing a crime, only 10.9% of survey respondents (25 of 230), would have permitted police to attach a GPS tracking device to the vehicle of this particular suspect and monitor that vehicle's movements without first obtaining a warrant. Of those 25 individuals, 22 of them would have permitted warrantless GPS tracking for only a few days. Across all 230 respondents, only three would have permitted this individual to be tracked without a warrant for twenty-one days or longer.

<sup>226.</sup> Here, only 46 of the 223 respondents, or 20.6%, would permit warrantless GPS tracking to extend twenty-one days or longer. Given that only 1 in 5 respondents would permit warrantless GPS tracking to extend twenty-one days or longer for a suspect similar to Antoine Jones, the Government's analogy to visual observation of a vehicle in public, as argued in *Jones*, a case involving a twenty-eight day warrantless GPS tracking, simply fails to adequately resolve the issue. In its *Jones* brief, the United States argued that individuals have no reasonable expectation of privacy in information knowingly exposed to public view, which directly applied to Jones. See Petitioner's Brief on the Merits at 18, 38, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5094951.

<sup>227.</sup> Four of these 22 survey respondents selected "less than 1 day" as the length of time police would be permitted to track this individual without a warrant; 3 selected one day, 1 selected two days; 9 selected 3–5 days; 5 selected 6–10 days; and no respondents selected 11–20 days. Accordingly, of these 22 respondents, 8 would have permitted such warrantless tracking for only two days or less; and 9 would have allowed such tracking to extend 3–5 days without a warrant.

Similar results appear for Suspect Type 3, the convicted felon who is not currently suspected of committing a crime. Here, only 26.3% of survey respondents (60 of 228), would have permitted police to attach a GPS tracking device to the vehicle of this particular suspect and monitor that vehicle's movements without a warrant. Of the 60 respondents who would permit warrantless tracking, 10 selected either "less than 1 day" or "1 day" as the permissible length of surveillance; eight selected "3–5 days"; nine selected "6–10 days"; and 32 would have permitted warrantless tracking for twenty-one days or longer.

241

Although society seems willing to permit a convicted felon (who is not currently suspected of committing a crime) to be tracked for a lengthier period of time than the innocent suspect, the overriding sentiment is that police should never be permitted to attach a GPS tracking device to the vehicle of an innocent suspect and monitor that vehicle's movements in the absence of a warrant.

By contrast, when we examine the results of the Group Three suspects, those suspected of committing a severe crime, society appears generally willing to permit warrantless GPS tracking. For Suspect Type 5, the suspected terrorist, 67.3% of survey respondents (152 of 226) would have permitted this individual to be tracked without a warrant, whereas only 32.7% of respondents (74 of 226) would have required a warrant to do so. Among the entire cohort, almost 40% of respondents (90 of 226), would have permitted the suspected terrorist to be tracked without a warrant for a relatively lengthy period of time—i.e., twenty-one days or longer. Nearly half of all respondents (107 of 226) would have permitted the suspected terrorist to be tracked without a warrant for eleven days or longer, and a majority of all respondents (124 of 226) would have permitted the suspected terrorist to be tracked without a warrant for six days or longer.

Similar results appear for Suspect Type 7, the suspected serial killer. For the suspected serial killer, 64.8% of survey respondents (142 of 219) would have permitted this individual to be tracked without a warrant, whereas only 35.2% of respondents (77 of 219) would have required a search warrant to do so. Among the entire cohort, almost 40% of all respondents (86 of 219), would have permitted the suspected serial killer to be tracked without a warrant for twenty-one days or longer, and almost 50% of respondents (109 of 219) would have permitted the suspected serial killer to be tracked without a warrant for six days or longer.

As a whole, these results suggest that society is willing to permit law enforcement to track by GPS those suspected of the most extreme

<sup>228.</sup> The remaining respondent selected "11–20 days" as the permissible length of surveillance.

crimes for at least several days without prior judicial approval. When compared to the innocent suspects, society seemingly agrees that police should have greater freedom to investigate the most serious offenses by way of GPS.

## C. Cell Phone Tracking Survey

To further refine my research, I conducted a second survey posing a similar set of questions relating to both GPS tracking by way of physical trespass, approximating the issue in *Jones*; and GPS tracking accomplished in the absence of a physical trespass by way of a GPS-enabled smart phone, an issue that currently remains unresolved. This second survey sought to determine whether society meaningfully distinguishes between these two methods of tracking. To determine whether a trespass upon an effect should, or should not, be dispositive, this survey seeks to determine whether society expects the same, more, or less privacy in the tracking of cell phones, which are presumably known to contain GPS devices upon purchase, vis-à-vis tracking by way of GPS device surreptitiously attached to a suspect's vehicle.

In this second survey, respondents were given two series of questions. In the first series of questions, respondents were asked to assume that police had attached a GPS tracking device to a suspect's vehicle by way of trespass and had used that device to monitor the suspect's movements for a period of time (as in *Jones*). In the second series of questions, identical to the first in most respects, respondents were instead asked to assume that police were able to monitor an individual's movements by obtaining location information directly from the suspect's cell phone provider.

This second survey had only two basic questions. First, the survey asked whether police should be required to obtain a search warrant before they may attach a GPS device to a suspect's vehicle and subsequently monitor that vehicle's movements. Second, the survey asked whether police should be required to obtain a search warrant in

<sup>229.</sup> Emphasizing the parallel to GPS tracking, the lead-in language for the second series of questions was as follows: "Cell phone technology, coupled with the widespread use of smart phones among American citizens, has enabled police to determine a person's movements with nearly as much accuracy as a GPS device mounted on that person's vehicle. Cell phone data, for example, is often used to reveal where a cell phone was located at a particular point in time by identifying which cell tower communicated with the cell phone while the phone was utilized to make a call. Cell location data makes it possible to determine a person's movements with precision, and can operate successfully even when the phone is simply turned on, regardless of whether a call has been made or not. Cell phone companies maintain accurate records of cell phone location information for all of its customers, making it possible for police to obtain a suspect's location information by a simple request to a cell phone provider, such as AT&T or Verizon. Please answer the following questions related to this emerging form of police investigation."

order to acquire a suspect's cell phone location information directly from a cell phone provider. Each of these questions contained three initial answer choices: (1) "Yes, the police should have to get a warrant regardless of the nature of the crime being investigated;" (2) "No, the police shouldn't have to get a warrant to do this;" and (3) "It depends on the nature of the crime the police are investigating."

243

For those respondents who picked answer choices (1) or (2), no additional questions were asked. However, respondents who selected answer choice (3) were then asked to specify permissible lengths of surveillance for the following different types of suspects: (i) a person who has not been convicted of a crime and who is not suspected of committing any crime; (ii) a person who is not suspected of a crime and who has not been accused of committing any crime; (iii) a convicted felon who is not suspected of committing any crime; (iv) a convicted felon who is suspected of committing a crime; (v) a person suspected of planning or engaging in terrorist acts; (vi) a suspected drug dealer involved in a drug-trafficking conspiracy involving large amounts of cash and narcotics; (vii) a suspected serial killer; (viii) an individual suspected of illegally growing marijuana; and (xi) an individual suspected of engaging in a series of bank robberies.

# 1. Survey Results

The results of this survey are significant. Most notably, society saw no statistically significant difference in tracking an individual by means of a GPS tracking device attached to that person's vehicle and tracking that same individual by a GPS-enabled cell phone. Generally speaking, the majority of respondents deemed location information data presumptively protected by the Fourth Amendment, regardless of whether that data is obtained by way of surreptitiously installed GPS or directly from a cell phone provider. Moreover, while the results for each method of tracking were similar, society believed that tracking an individual by a GPS-enabled cell phone should receive somewhat greater Fourth Amendment protection than tracking an individual in the manner employed in *Jones*.

The following chart summarizes these results:

### University of Cincinnati Law Review

[VOL. 82]

244

	GPS Tracking: Should police be required to obtain a search warrant before they may attach a GPS device to a suspect's vehicle?	Cell Phone Tracking: Should police be required to obtain a search warrant in order to obtain a suspect's cell phone location information directly from a cell phone provider?
Yes, the police should have to get a warrant regardless of the nature of the crime being investigated	51.7% (92 of 178)	58.4% (101 of 173)
No, the police shouldn't have to get a warrant to do this	9.0% (16 of 178)	9.8% (17 of 173)
It depends on the nature of the crime the police are investigating	39.3% (70 of 178)	31.8% (55 of 173)

As with my initial survey, the results of this second survey further support the notion that Fourth Amendment protections in regards to GPS tracking should vary depending on the nature of the crime being investigated.

While less than a majority, nearly 40% of all respondents indicated that the nature of the particular crime police are investigating should alter whether police should be required to obtain a warrant before they may attach a GPS device to a suspect's vehicle. Nearly 32% of all respondents selected the same option with respect to obtaining a suspect's cell phone location information directly from a cell phone provider. Respondents who selected this particular answer choice were then given additional questions in which they were asked to specify permissible lengths of surveillance for different types of suspects.

Digging deeper into the data, of the 70 respondents who believed the constitutionality of warrantless GPS tracking should depend on the nature of the crime police are investigating, only six would have allowed the movements of an innocent suspect (Suspect Type (i)) to be monitored without a warrant, whereas 61 would have required a warrant in this situation. By contrast, for the suspected terrorist (Suspect Type (v)), 64 respondents believed police should not be required to

<sup>230.</sup> Three of these 70 respondents did not answer the follow-up questions.

obtain a warrant to monitor this suspect's movements by surreptitiously-installed GPS, whereas only three indicated that police should have to obtain a search warrant to do so. When these distinct types of suspects are compared, this data tends to support the argument that Fourth Amendment protections in regards to GPS tracking should indeed vary depending on the nature of the crime being investigated.

245

When the other suspect types are examined (again, isolating only the 40% of respondents who indicated that the constitutionality of warrantless GPS tracking should depend on the nature of the crime police are investigating) two distinct groups of suspects emerge: those suspected of relatively severe crimes and those suspected of either minor crimes or no crime at all. As set forth in the charts that follow, society appears more willing to permit the warrantless GPS tracking of those suspected of committing relatively severe crimes vis-à-vis those suspected of either minor crimes or no crime at all.

GPS Tracking: Those Suspected of Minor Crimes or of No Crime

CLICDE CT TYDE	NO WARDANIT	WADDANE	
SUSPECT TYPE	NO WARRANT	WARRANT	
	REQUIRED	REQUIRED	
Type (ii): Not suspected	4.6%	95.5%	
nor accused of a crime	(3 of 66)	(63 of 66)	
Type (i): Not convicted	9.0%	91.0%	
nor suspected of a	, , , ,	, -,,,,	
crime	(6 of 67)	(61 of 67)	
	25.00/	64.20/	
Type (viii): Suspected	35.8%	64.2%	
of using illegal drugs	(24 of 67)	(43 of 67)	
Type (x): Suspected of illegally growing marijuana	37.3% (25 of 67)	62.7% (42 of 67)	
Type (iii): Convicted felon not suspected of any crime	43.3% (29 of 67)	56.7% (38 of 67)	

University of Cincinnati Law Review

[VOL. 82

GPS Tracking: Those Suspected of Relatively Severe Crimes

SUSPECT TYPE	NO WARRANT WARRANT	
	REQUIRED	REQUIRED
Type (v): Suspected	95.5%	4.5%
terrorist	(64 of 67)	(3 of 67)
Type (vii): Suspected	91.0%	9.0%
serial killer	(61 of 67)	(6 of 67)
Type (vi): Suspected		
drug dealer involved in	86.6%	13.4%
a large-scale drug-	(58 of 67)	(9 of 67)
trafficking conspiracy		
Type (iv): Convicted		
felon suspected of	82.1%	11.9%
committing an	(59 of 67)	(8 of 67)
unspecified crime		
Type (xi): Suspected of	74.6%	25.4%
bank robberies	(50 of 67)	(17 of 67)
Type (ix): Suspected car	56.7%	43.3%
thief	(38 of 67)	(29 of 67)

Although not reported in detail here, similar results appeared for the 32% of respondents who believed the nature of the particular crime under investigation should determine whether a warrant is required before police may obtain a suspect's cell phone location information directly from a cell phone provider.

### 2. Conclusions

Four important conclusions emerge from the collective responses to this second survey. First, despite the particular method of GPS tracking employed (i.e., trespassorily attaching a GPS device to a suspect's vehicle versus tracking a suspect's movements by means of a GPS-enabled smart phone) there is strong societal support for the overall outcome in *Jones*, which effectively limits the ability of police to obtain GPS tracking information without a warrant. With respect to GPS tracking in the manner employed in *Jones*, 51.7% of survey respondents indicated that police should have to obtain a warrant regardless of the nature of the crime being investigated, and of the 39.3% of respondents who would have made the requirement of a warrant dependent upon the nature of the crime, many of those respondents would have been unwilling to permit warrantless GPS tracking for the type of suspect at issue in *Jones*—the suspected drug dealer.

Second, society appears unwilling to assume the risk that information exposed to cell phone providers (such as the location of their phone during calls) will be shared with law enforcement in the absence of a warrant. Rather, as a general matter, society deems location information data presumptively protected by the Fourth Amendment, regardless of whether that data is obtained surreptitiously by the police or directly from a cell phone provider.

Third, society tends to agree that Fourth Amendment protections relating to GPS tracking should vary depending on the nature of the crime being investigated and on the length of surveillance.

Finally, and perhaps most importantly, society saw no statistically significant difference in tracking an individual by means of a GPS tracking device attached to that person's vehicle and tracking that same individual by smart-phone enabled GPS. If anything, society believed that tracking an individual by smart-phone enabled GPS should receive somewhat greater Fourth Amendment protection than tracking an individual in the manner employed in *Jones*. This particular result is significant in its potential to impact the developing law of cell phone tracking, which remains much more unsettled than the scenario in *Jones*.

#### V. A SLIDING SCALE FRAMEWORK FOR CELL PHONE AND GPS TRACKING

In *Jones*, the Court did not resolve whether a warrant, probable cause, reasonable suspicion, or some other standard would satisfy the Fourth Amendment with respect to the particular method of GPS tracking employed in *Jones*.<sup>231</sup> The Court has also not set forth any standards to govern the acquisition of cell site location information, and courts across the country are imposing different Fourth Amendment requirements in otherwise similar cases.<sup>232</sup> Thus, the question of what would make a particular instance of GPS or cell phone tracking constitutionally "reasonable" remains unresolved, and greater clarity is needed.<sup>233</sup>

Even assuming that the Fourth Amendment would govern all instances of GPS or cell phone tracking, not every Fourth Amendment intrusion requires a warrant or probable cause; rather, as the Supreme Court has declared on a number of occasions, the Fourth Amendment's general restriction against "unreasonable searches and seizures" requires

<sup>231.</sup> United States v. Katzin, No. 11-226, 2012 WL 1646894, at \*4 (E.D. Penn. May 9, 2012).

<sup>232.</sup> See Pell & Soghoian, supra note 114, at 137–139 (noting that in many districts prosecutors may obtain prospective cell site information under a reasonable suspicion standard, whereas some magistrate judges require probable cause before authorizing law enforcement access to any type of prospective cell site data).

<sup>233.</sup> See id. at 121–22 ("determining the proper access standard" for cell phone location information "is anything but clear under current law").

a case-specific analysis as to what is "reasonable." Under this method of Fourth Amendment analysis, "reasonableness" is determined under a balancing test, weighing the government's and individual's interests against each other. In cases where the government's interest is substantial, as in the investigation of the most extreme offenses, and the individual's privacy interest is less so, departures from the usual requirements of a warrant and probable cause may be justified.

With electronic monitoring of a suspect's location, the government's interest in effective crime prevention is heightened when investigating the most serious offenses, particularly those that threaten the national security, such as terrorism investigations. On the other side of the ledger, the electronic monitoring of a person's movements becomes more invasive the longer an individual is tracked. Balancing the competing interests suggests that Fourth Amendment requirements should vary based upon the suspected crime and length of surveillance, an approach that is confirmed by my survey results.

While the notion of varying Fourth Amendment protections based

<sup>234.</sup> See Samson v. California, 547 U.S. 843, 848 (2006). See also Whren v. United States, 517 U.S. 806, 817 (1996) ("It is of course true that in principle every Fourth Amendment case, since it turns upon a 'reasonableness' determination, involves a balancing of all relevant factors."); Graham v. Connor, 490 U.S. 386, 395 (1989) ("all claims that law enforcement officers have used excessive force—deadly or not—in the course of an arrest, investigatory stop, or other 'seizure' of a free citizen should be analyzed under the Fourth Amendment . . . 'reasonableness' standard.").

<sup>235.</sup> Terry v. Ohio, 392 U.S. 1, 21 (1968) ("there is 'no ready test for determining reasonableness other than by balancing the need to search (or seize) against the invasion which the search (or seizure) entails'").

<sup>236.</sup> Under this approach, police may conduct a wide array of less intrusive searches and seizures on the basis of "reasonable suspicion," a lesser standard of cause than "probable cause." The "reasonableness" balancing test of *Terry v. Ohio* has been applied in a number of settings, including: searches of public school students, New Jersey v. T.L.O., 469 U.S. 325, 341–42 (1985) (upholding search of public school student based on reasonable suspicion); probationers, United States v. Knights, 534 U.S. 112 (2001) (upholding search of probationer's home based on reasonable suspicion); and parolees, Samson v. California, 547 U.S. 843 (2006) (individualized suspicion not required for search of parolee's home or person).

<sup>237.</sup> GPS tracking enables the government to track a suspect's movements twenty-four hours a day for extended periods of time. Discovering the whole of one's movements over such a long time is far more invasive of privacy than discovering one's movements during a single journey. Under this type of prolonged surveillance, police can "deduce whether [the suspect] is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." The combination of these observations "tell[s] a story not told by any single visit." United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010). Moreover, it would be incredibly difficult, if not impossible, to replicate the advantages of GPS tracking on a large-scale basis through more traditional forms of surveillance. See People v. Weaver, 12 N.Y.3d 433, 440–44 (2009) ("GPS is a . . . powerful technology that is easily and cheaply deployed and has virtually unlimited and remarkably precise tracking capability . . . . The potential for a similar capture of information or 'seeing' by law enforcement would require . . . millions of additional police officers and cameras on every street lamp.").

<sup>238.</sup> See supra notes 221-231 and accompanying text.

upon the suspected crime and length of surveillance seems empirically justified, Fourth Amendment case law also reflects a similar approach. As *Skinner*, *Estrella*, and *Luna-Santillanes* indicate, tracking a suspect's vehicle by GPS for only a few days should not require a search warrant. By contrast, consistent with the opinions of the five concurring Justices in *Jones*, tracking the movements of a suspect like Antoine Jones, a suspected drug dealer, for twenty-eight days or longer should receive Fourth Amendment protection—presumably the full protection of a warrant.

Jones involved an investigation of cocaine trafficking involving large amounts of drugs, one that ultimately led to severe charges against the suspect and an eventual sentence of life imprisonment. Starting with the type of suspect in Jones, we could begin to fashion a framework for GPS tracking legislation where tracking any suspect for twenty-eight days or longer would always require a search warrant. Because Jones involved a relatively severe offense, this twenty-eight day outer limit would apply regardless of how severe the crime under investigation. On the other hand, due to the less invasive nature of a more limited track, tracking a suspect like Jones for three days or less might not require a warrant, but may instead require a lesser degree of individualized suspicion, perhaps reasonable suspicion. With such a large time gap between these two points, the line where warrants would be required would need to be established.

Consistent with recent, similar proposals, the framework proposed below would not vary Fourth Amendment protections based upon the particular method of electronic tracking.<sup>241</sup> Rather, under my proposal, all forms of electronic tracking would be subject to the same requirements.

This approach not only brings needed consistency to this area, but is also supported by my survey results. As those results indicate, society deems location information data presumptively protected by the Fourth Amendment, regardless of whether that data is obtained surreptitiously by the police or obtained directly from a cell phone provider. Moreover,

<sup>239.</sup> See Brief for Petitioner at 4–5, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5094951.

<sup>240.</sup> As compared to probable cause, the Supreme Court has declared that the "reasonable suspicion" standard is "obviously less demanding than that for probable cause," United States v. Sokolow, 490 U.S. 1, 7 (1989), and requires "considerably less" proof of wrongdoing than proof by a preponderance of evidence. *Id.* Under this standard, police may not act on the basis of an unparticularized suspicion or hunch; rather, an officer must be able to point to "specific and articulable facts" that, along with reasonable inferences from those facts, justify the intrusion. Terry v. Ohio, 392 U.S. 1, 21 (1968).

<sup>241.</sup> See Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013) (proposing the requirement of a warrant for the government to intercept or force service providers to disclose geolocation data of any kind).

as technology continues to evolve, cell site location information is becoming as accurate, in some instances even more so, than GPS tracking, thus triggering the same privacy concerns as those highlighted by the concurring Justices in *Jones*. Given these concerns, my proposal does not vary Fourth Amendment protections based upon the particular method of tracking employed.

# A. Proposal Details

As noted, there is societal support for varying Fourth Amendment protections with respect to GPS tracking based upon the nature of the crime under investigation and length of surveillance. My proposal incorporates this approach by designating three distinct categories of individuals and proposing different standards for each.

## 1. Those Suspected of Severe Crimes

For investigations of relatively severe offenses, my proposal is that police may track an individual by GPS for up to six days without the need for prior judicial approval. Under this proposal, police would need to first establish, and document in advance, reasonable suspicion before they may track an individual by GPS, whether through surreptitiously installed GPS devices or through cell phone tracking; <sup>243</sup> however, police would not need prior judicial approval to do so. If, however, a particular investigation would require lengthier tracking, police would be required to obtain probable cause and a search warrant to continue that monitoring. To obtain such authorization, police must further establish a case-specific need for additional location information extending beyond six days. Moreover, at this time, police would be required to demonstrate the factual basis for their initial finding of reasonable suspicion, which would deter the arbitrary use of this investigative power and which mirrors what a prosecutor must do to defend against a motion to suppress the evidentiary fruits of a *Terry* stop.

The category of relatively severe offenses would include investigations of suspected terrorist activity; large-scale drug trafficking investigations, the type of investigation where the use of GPS tracking devices has been most common; and investigations of those felonies generally recognized by statute as the most extreme, including

<sup>242.</sup> See supra notes 132-136 and accompanying text.

<sup>243.</sup> Under this standard, police would need to document in advance their basis for reasonable suspicion, and be prepared to argue that reasonable suspicion was indeed obtained in advance of such tracking in the event of a motion to suppress any evidence linked to that investigation.

homicides, robbery, burglary, arson, and kidnapping.<sup>244</sup>

This six-day proposal is consistent with my survey results. For example, in my first GPS tracking survey, for the relatively severe offenses such as the suspected terrorist, the tipping point, where a majority of society would require judicial supervision, appears to be 6–10 days of tracking. This is illustrated by the chart that follows. When reviewing this chart, each number in the chart represents the percentage of survey respondents who selected a particular answer choice. For example, the top left-hand corner of the chart indicates that 89.1% of survey respondents believed that warrants are always required to track the movements of an innocent suspect by GPS, whereas the bottom right-hand corner of the chart indicates that 39.4% of survey respondents would permit warrantless tracking of the suspected terrorist to extend for twenty-one days or longer. To make sense of this data, one must identify the tipping point where a majority of society would require judicial supervision.

	Innocent Suspect	Suspected Drug-Dealer	Suspected Terrorist
Warrant always required	89.1%	52.9%	32.7%
Warrantless Tracking Permitted for 1 day or less	3.0%	3.6%	4.0%
Warrantless Tracking Permitted for 2–5 days	4.4%	10.3%	8.4%
Warrantless Tracking Permitted for 6–10 days	2.2%	9.0%	7.5%
Warrantless Tracking Permitted for 11–20 days	0.0%	3.6%	7.5%
Warrantless Tracking Permitted for 21 days or longer	1.3%	20.6%	39.4%

As this chart illustrates, for the suspected terrorist, 45.1% of society (32.7% + 4.0% + 8.4%) would not permit GPS tracking to extend beyond five days without a warrant, and a majority of society, 54.4%,

Published by University of Cincinnati College of Law Scholarship and Publications, 2014

251

<sup>244.</sup> See, e.g., MODEL PENAL CODE § 210.2(1)(b) (designating as sufficient to raise an otherwise unintentional homicide to murder all killings committed during the course of a "robbery, rape or deviate sexual intercourse by force or threat of force, arson, burglary, kidnapping or felonious escape").

would not permit GPS tracking to extend beyond ten days without a warrant. This data, while not perfectly precise, suggests that judicial supervision for the investigation of the most serious offenses should begin somewhere within the 6–10 day range.

In contrast, only 24.2% of survey respondents (3.6% + 20.6%) would permit warrantless GPS tracking to extend beyond ten days for a suspect similar to Antoine Jones, as opposed to the 45.1% who were willing to do so for the suspected terrorist. As set forth more fully below, this data suggests that less severe offenses should generally remain subject to the Fourth Amendment's warrant requirement.

### 2. Those Suspected of Minor Crimes

For all suspected crimes not falling into the category of severe crimes identified above, I propose police be required to establish reasonable suspicion in order to track an individual for up to three days. This proposal is consistent with the holdings in *Knotts*, *Skinner*, *Estrella*, and Luna-Santillanes, in the sense that no prior judicial approval would be necessary to track those suspected of less severe crimes for a relatively short period of time. Moreover, this proposal is consistent with the ability to simply track a suspect turn-by-turn without the need for prior judicial approval. If, however, a particular investigation would require lengthier tracking, police would then be required to obtain a search warrant from a judicial officer to continue that monitoring. Under this proposal, the warrant affidavit must establish the basis for probable cause and must further establish a case-specific need for additional location information extending beyond three days. Moreover, at this time, police would be required to demonstrate the factual basis for their initial finding of reasonable suspicion, a requirement that would again help deter the arbitrary use of this investigative power.

### 3. Those Not Suspected of Any Crime

Finally, consistent with the results of each of my surveys, and consistent with the Fourth Amendment's restriction against general, exploratory searches, an individual who is not suspected of committing any offense could not be tracked by GPS for any period of time, regardless of the method of tracking.

This particular proposal would account for the concerns of the *Jones* Court regarding the possibility of mass surveillance in the absence of individualized suspicion of wrongdoing<sup>245</sup> and would be consistent with

<sup>245.</sup> Indeed, Jones apparently forecloses the possibility of "affixing GPS tracking devices to

society's belief, as expressed in my surveys, that police should never be permitted to obtain data regarding the movements of ordinary, lawabiding citizens in the absence of a particularized showing of wrongdoing. <sup>246</sup>

## B. Support for this Proposal

Despite its ruling on the constitutionality of GPS tracking under the particular circumstances at issue in Jones, the Jones Court did not resolve whether a warrant, probable cause, reasonable suspicion, or some other standard would satisfy the Fourth Amendment where a particular instance of GPS tracking constitutes a Fourth Amendment search.<sup>247</sup> Moreover, the competing interests between law enforcement needs and privacy concerns triggered by this form of investigation suggest the need for flexibility in legal standards, a need the Fourth Amendment's reasonableness approach can accommodate. Because the Fourth Amendment, at its core, simply prohibits "unreasonable searches and seizures," the Supreme Court has declared that "in principle every Amendment case . . . turns upon 'reasonableness' Fourth determination, [which in turn] involves a balancing of all relevant factors."248 This approach to Fourth Amendment analysis, where the government's interests and individual's interests are pitted against each other in any given case, suggests the adoption of a "sliding scale of suspicion"—one that depends on the government's need for, and the level of invasiveness of, any particular instance of tracking. In the realm of electronic tracking, the government's interest in effective crime prevention increases when investigating the most serious offenses, whereas the level of intrusiveness generated by such monitoring increases the longer an individual is tracked. By adopting a "sliding scale of suspicion," one that is calibrated to the particular competing interests of any given case, my proposal is consistent with this reasonableness-based approach to the Fourth Amendment.<sup>249</sup>

On the law enforcement side, this proposal gives police greater

thousands of cars at random," at least where doing so involves a physical trespass upon the vehicle. *See* United States v. Garcia, 474 F.3d 994, 997–98 (7th Cir. 2007) (discussing this possibility in the pre*Jones* world).

<sup>246.</sup> See supra notes 221–226 and accompanying text.

<sup>247.</sup> United States v. Katzin, 2012 WL 1646894, at \*4 (E.D. Penn. May 9, 2012).

<sup>248.</sup> Whren v. United States, 517 U.S. 806, 817 (1996).

<sup>249.</sup> Post-*Jones* courts appear willing to vary Fourth Amendment protections in a "sliding scale" manner. For example, the Seventh Circuit recently declared that its "sliding scale' of suspicion," under which "[h]ow much cause agents need to do something [would] depend[] on how deeply they invade the zone of privacy," "survived *Jones*, which means that the 'sliding scale' approach may allow minimally invasive intrusion on property interests, not merely privacy interests." United States v. Peter, No. 3:11-CR-132 JD, 2012 WL 1900133, at \*15 (N.D. Ind. May 24, 2012).

flexibility in the use of GPS tracking to investigate the most serious offenses. One senior Department of Justice official recently told a Senate Committee that "if an amendment [to existing federal statutes] were to unduly restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost." Similarly, in a recent GPS tracking case, *United States v. Katzin*, <sup>251</sup> a federal district court declared that "the possibly unfettered uses by law enforcement of GPS tracking to gather evidence to . . . establish probable cause in cases of serious crimes like drug trafficking, terrorism, and the like, strongly outweigh the concern about intrusion." I echo these concerns. As the Government argued in *Katzin*.

GPS monitoring of a vehicle, at least for a limited period of time on public roads, is [minimally invasive] in that (1) individuals have a diminished expectation of privacy when traveling on public thoroughfares, (2) the intrusion of the installation of a tracking device is minimal, and (3) the information gathered is less detailed than would be achieved with visual or aural means of surveillance. [Moreover,] the GPS tracker cannot even reveal information such as who is in the car, who is driving the car, or what the occupants do when they arrive at their ostensible destination—all information that would be revealed... by traditional visual surveillance. <sup>253</sup>

Given the arguably reduced privacy concerns inherent in GPS tracking, the case for warrantless GPS tracking of the most serious offenses is much stronger.<sup>254</sup>

Relaxing Fourth Amendment protections in the more extreme cases is further supported by recent Congressional and judicial decisions. For example, in 1986, Congress placed statutory restrictions on the use of

<sup>250.</sup> Pell & Soghoian, *supra* note 114, at 123 (quoting *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) (statement of James A. Baker, Assoc. Deputy Attorney Gen., U.S. Dep't of Justice).

<sup>251.</sup> United States v. Katzin, No. 11-226, 2012 WL 1646894 (E.D. Penn. May 9, 2012).

<sup>252.</sup> Id. at \*5.

<sup>253.</sup> Id.

<sup>254.</sup> Unlike the type of GPS tracking at issue in *Jones*, under which the location of a suspect's vehicle may be tracked continually, simply "pinging" a cell phone periodically to determine its location is far less invasive of privacy than a continual surveillance would be. *Cf.* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) ("[F]or four weeks, law enforcement agents tracked *every movement* that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.") (emphasis added).

### 2013] GPS AND CELL PHONE TRACKING

pen registers by law enforcement.<sup>255</sup> However, as a result of the September 11, 2001, terrorist attacks, Congress granted special powers to the Attorney General to authorize use of pen registers without prior court approval in emergency circumstances relating to international terrorism and foreign intelligence.<sup>256</sup> More recently, the Supreme Court rejected a challenge to a federal law that broadened the government's power to eavesdrop on international phone calls and e-mails, a ruling which exemplifies the Court's willingness to permit relaxed standards in the investigation of the most serious offenses.<sup>257</sup> Thus, the notion that Fourth Amendment protections should vary depending on the nature of the crime being investigated, particularly in the realm of terrorist investigations, is consistent with recent federal statutes and Supreme Court opinions.<sup>258</sup>

Finally, because my proposal could be easily converted into draft legislation, my proposal is consistent with Justice Alito's suggestion in *Jones*, which encourages legislative solutions. According to Justice Alito, "[i]n circumstances involving dramatic technological change, the best solution . . . may be legislative [because] [a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." By incorporating the very "public attitudes" Justice Alito highlights, an opinion which was endorsed by three additional Justices, my proposal would likely garner support from a majority of Supreme Court Justices.

Moreover, as a proposed legislative framework, my proposal is consistent with the recent efforts of various states to enact legislation that would place definitive restrictions upon law enforcement's ability to acquire location information. As of March 2013, at least eleven states had introduced bills designed to govern law enforcement's acquisition of location information, with many of those bills including provisions designed to restrict the acquisition of cell phone information. <sup>260</sup> My

<sup>255.</sup> See 18 U.S.C. §§ 3121–3126 (2012). A pen register is a mechanical device that records the numbers dialed on a telephone; it does not overhear oral communications and does not indicate whether calls are actually completed. Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979).

<sup>256. 50</sup> U.S.C. §§ 1842–1843 (2012).

<sup>257.</sup> See Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013).

<sup>258.</sup> Such distinctions derive from the Court's decision in *United States v. United States Dist.* Court for Eastern Dist. of Mich., 407 U.S. 297 (1972), in which the Court explained that the standards and procedures that law enforcement officials must follow when conducting "surveillance of 'ordinary crime' might not be required in the context of surveillance conducted for domestic national-security purposes."

<sup>259.</sup> See Jones, 132 S. Ct. at 964 (Alito, J., concurring). See also Pell & Soghoian, supra note 114, at 150–51 (emphasizing the need for legislative solutions in this area of law).

<sup>260.</sup> Cyrus Farivar, *Texas Proposes One of Nation's "Most Sweeping" Mobile Privacy Laws*, ARS TECHNICA (Mar. 6, 2013, 8:37 PM), http://arstechnica.com/tech-policy/2013/03/texas-proposes-one-of-nations-most-sweeping-mobile-privacy-laws/.

#### UNIVERSITY OF CINCINNATI LAW REVIEW

[VOL. 82]

proposal continues this trend, and goes further by adopting one uniform set of standards that would likely pass Fourth Amendment scrutiny.

#### VI. CONCLUSION

In *Jones*, the Supreme Court ruled that the Government's installation of a GPS tracking device on a suspect's vehicle and subsequent use of that device to monitor the vehicle's movements constitutes a Fourth Amendment "search." The precise holding of *Jones* was limited to the particular form of GPS monitoring in which police attach a GPS tracking device to an individual's vehicle. 262 Jones did not determine the constitutionality of similar forms of tracking accomplished in the absence of a trespass, such as cell phone tracking; nor did *Jones* resolve whether a warrant, probable cause, reasonable suspicion, or some other standard would make any particular instance of GPS tracking "reasonable" under the Fourth Amendment. Moreover, five Justices in Jones suggested that a twenty-eight day monitoring period utilizing the same method of GPS tracking employed in *Jones* might not trigger the Fourth Amendment where the investigation involved a more serious offense than that in *Jones*, and the remainder of the Court appeared willing to address such issues in future cases.

In the months following *Jones*, I administered two surveys designed to explore possible distinctions in GPS tracking based upon the factors highlighted in *Jones*—most notably, the nature of the crime under investigation and the length of GPS monitoring. The results of these surveys suggest that society is indeed willing to permit warrantless GPS tracking for a longer period of time when investigating the most serious offenses. Reflecting society's beliefs as to what is "reasonable" in this method of investigation, I have set forth a proposal that would make the constitutionality of GPS tracking dependent upon the nature of the crime under investigation and the length of surveillance, specifically, by designating three distinct categories of individuals and proposing different standards for each. With the law of cell phone tracking unresolved and ever-changing, this proposal provides a consistent framework for law enforcement and courts to utilize as these issues arise, one which enjoys both empirical and normative support.

<sup>261.</sup> United States v. Jones, 132 S. Ct. 945, 946 (2012).

<sup>262.</sup> Id. at 948.