STOPPING POLICE IN THEIR TRACKS: PROTECTING CELLULAR LOCATION INFORMATION PRIVACY IN THE TWENTY-FIRST CENTURY

STEPHEN WAGNER[†]

ABSTRACT

Only a small fraction of law enforcement agencies in the United States obtain a warrant before tracking the cell phones of suspects and persons of interest. This is due, in part, to the fact that courts have struggled to keep pace with a changing technological landscape. Indeed, courts around the country have issued a disparate array of holdings on the issue of warrantless cell phone tracking. This lack of judicial uniformity has led to confusion for both law enforcement agencies and the public alike. In order to protect reasonable expectations of privacy in the twenty-first century, Congress should pass legislation requiring law-enforcement agencies to obtain a warrant based upon probable cause before they can track a cell phone except in a limited set of time-sensitive situations and emergencies.

This Issue Brief describes the technology police use to track cell phones, discusses the need for federal legislation, concludes that current Fourth Amendment jurisprudence is inadequate to address cell phone tracking, analyzes two bills dealing with "geolocation information" privacy that legislators have introduced in Congress, and ultimately concludes that one of those bills is superior to the other.

INTRODUCTION

Among deprivations of rights, none is so effective in cowing a population, crushing the spirit of the individual and putting terror in every heart. Uncontrolled search and seizure is one of the first and most effective weapons in the arsenal of every arbitrary government.

—JUSTICE ROBERT H. JACKSON[1]

Almost ninety percent of American adults own a cell phone.[2] Such pervasive cell-phone use has revolutionized the way Americans conduct

---

[†] J.D., 2014, Duke University School of Law. B.A. in History, 2009, Boston College.

[1] Brinegar v. United States, 338 U.S. 160, 180 (1949) (Jackson, J., dissenting).

their lives.[3] In response to this trend, law-enforcement agencies have changed the ways they fight crime.[4] In 2011, law-enforcement agencies sent nine popular cellular-service providers over 1.3 million requests for customer cellular data.[5] Because their use is so prevalent,[6] cell phones serve as convenient tools for tracking suspects and persons of interest.[7] Due to the absence of comprehensive federal legislation, law-enforcement agencies apply a wide variety of different legal standards to determine the propriety of tracking cell phones.[8] Unfortunately, most agencies do not obtain a warrant before they begin monitoring a suspect's cell phone.[9] In fact, the American Civil Liberties Union (ACLU) reports that of over 200 law-enforcement agencies surveyed nationwide, only a "tiny handful" actually acquire a warrant before tracking.[10] In order to protect reasonable expectations of privacy in the twenty-first century, Congress should pass legislation requiring law-enforcement agencies to obtain a warrant based upon probable cause before they can track a cell phone except in a limited set of time-sensitive situations and emergencies.

Warrantless cell-phone tracking presents a great challenge to Fourth Amendment jurisprudence. Courts have churned out a disparate array of holdings on the issue.[11] The lack of judicial uniformity has created confusion for law-enforcement agencies and consumers. Consequently, both groups need comprehensive federal legislation to tackle the privacy challenges presented by warrantless cell-phone tracking. As Justice Alito wrote in *United States v. Jones*, "[i]n circumstances involving dramatic

---

[2] Aaron Smith, *Cell Internet Use 2012*, PEW INTERNET & AM. LIFE PROJECT (Jan. 26, 2012), http://www.pewinternet.org/Reports/2012/Cell-Internet-Use-2012.aspx.

[3] *See Geolocation Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 8–9 (2012) (statement of Prof. Matt Blaze, Assoc. Professor, Univ. of Pennsylvania) [hereinafter Statement of Prof. Blaze].

[4] *See* Somini Sengupta, *Courts Divided Over Searches of Cell Phones*, N.Y. TIMES, Nov. 26, 2012, at A1, *available at* http://www.nytimes.com/2012/11/26/technology/legality-of-warrantless-cellphone-searches-goes-to-courts-and-legislatures.html?pagewanted=all.

[5] Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES, July 9, 2012, at A1, *available at* http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.

[6] Smith, *supra* note 2.

[7] *See* Sengupta, *supra* note 4*; see also* Lichtblau, *supra* note 5.

[8] *Geolocation Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 48 (2012) (statement of Catherine Crump, Staff Attorney, American Civil Liberties Union) [hereinafter Statement of Crump].

[9] *Id.*

[10] *Id.*

[11] Sengupta, *supra* note 4.

technological change, the best solution to privacy concerns may be legislative."[12] Courts are ill-equipped to keep pace with rapid changes in cell-phone technology and the shifting expectations of privacy that accompany them. Conversely, "[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."[13]

First, this Issue Brief discusses the cellular location technology that police use to monitor citizens who use cell phones. Specifically, this commentary will examine cell site, GPS, and WiFi technology. Second, this Issue Brief will show that legislation is needed in this area because cell-phone tracking is a widespread practice that may eventually replace federally regulated wiretapping to some degree. Third, this Issue Brief will dissect *United States v. Jones*, the Supreme Court's landmark GPS case, and explain why the decision is not helpful to lower courts confronted with cell-phone privacy issues. Fourth, this Issue Brief will explain how current Fourth Amendment jurisprudence is problematic when it comes to protecting peoples' expectations of privacy in cellular location data. In particular, this Issue Brief will address the inadequacies of the "third-party doctrine"—the idea that people forfeit their expectations of privacy when they share information with or allow their information to be seen by others.[14] Finally, this Issue Brief will evaluate two bills dealing with "geolocation information" privacy that legislators have introduced in the U.S. House of Representatives and the U.S. Senate. The article concludes that one bill is far more effective in protecting cellular privacy interests than the other.

I. THE TECHNOLOGY

Police can track cell phones using a variety of methods. One method is by obtaining cell-site information.[15] Cell-site information refers to the location data that a cellular-service provider or even a third party can gather when a cell-phone user makes or receives a call.[16] Another method police use is gathering data from the GPS (global positioning satellite)

---

[12] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).
[13] *Id.*
[14] Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. L. & PUB. POL'Y (SPECIAL ISSUE) 2 (2012).
[15] United States v. Jones, 908 F. Supp. 2d 203, 206–07 (D.D.C. 2012).
[16] *Id.* at 206; Brief of the American Civil Liberties Union and ACLU of the Nation's Capital as Amici Curiae Supporting Respondent at 15, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10–1259) [hereinafter ACLU Brief].

technology embedded in "smartphones."[17] Modern smartphones equipped with GPS technology can be located nearly anywhere.[18] Furthermore, many cell phones contain tracking chips that allow service providers to locate subscribers—even when the phones are not in use.[19]

Traditional cell-site tracking is possible because service providers maintain a network of towers that send and receive signals from cell phones.[20] Those companies collect and maintain records so they can identify which towers provided a cell phone with service at the beginning and end of every phone call.[21] The recorded information also identifies the date and time of a call, the number of the cell phone used, and indicates whether the call was incoming or outgoing.[22] Using this data, the government can determine a user's general location at the time of a call.[23] The actual location information is not precise because the government can only tell which cell-phone tower was closest to the user.[24] Furthermore, since the distance between cell-phone towers varies, so does the degree of accuracy in locating a user.[25] Some companies have divided their towers' service areas into 120-degree sectors with each individual tower serving as a focal point. [26] This method allows companies to locate individuals with greater precision, but not with enough spatial specificity to determine whether someone is in a particular building.[27] However, the government is still able to use information from multiple towers to triangulate the origin of a cell-phone call.[28]

Law-enforcement agencies can obtain cell-site tracking information from service providers in two ways.[29] First, agencies can ask a provider for "historical" cell-site data, which is information about a user's past locations

---

[17] *GPS Act*, RON WYDEN SEN. FOR OR., http://www.wyden.senate.gov/priorities/gps-act (last visited Oct. 25, 2014).
[18] Brief of the Rutherford Institute and the National Motorists Ass'n as Amici Curiae Supporting Respondent at 6, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10–1259) [hereinafter Rutherford Institute Brief].
[19] *Id.* at 13.
[20] *Jones*, 908 F. Supp. 2d at 206.
[21] *Id.*
[22] *Id.* at 206–07 (citing United States v. Madison, No. 11-60285-CR-ROSENBAUM, 2012 U.S. Dist. LEXIS 105527, at *4 (S.D. Fla. July 30, 2012)).
[23] *Id.*
[24] *Id.*
[25] *Id.*
[26] *Id.* at 207.
[27] *Id.*
[28] *Id.* n.4. *See In re* Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 451 n.3 (S.D.N.Y. 2006) [hereinafter Kaplan Opinion).
[29] *Jones*, 908 F. Supp. 2d at 207.

collected over a particular time period.[30] The amount of historical data available to police is potentially enormous, since providers keep extensive records of customers' past locations.[31] The U.S. Department of Justice reports that Verizon keeps records of its customers' past locations for one year and AT&T keeps records dating back to July 2008.[32] However, neither Verizon nor AT&T discloses these facts in their privacy policies. Second, agencies can ask for "prospective" data, information that a company provides in real time.[33] Regardless of whether the data is obtained post hoc or in real time, the actual information is identical.[34]

Law-enforcement agencies can also obtain cell-site data directly by using portable devices called StingRays.[35] StingRays mimic cell-phone towers and trick cell phones into sending them information like text messages and cell-site locations.[36] They can gather information from any cell phone in the area.[37] Because StingRays have the potential to collect information from many nearby cell phones, the Electronic Frontier Foundation has called the practice an "unconstitutional, all you can eat data buffet."[38] The U.S. Department of Justice, however, argues that law-enforcement agencies may use StingRay without a warrant when the "device is not capturing the contents of a particular dialogue call . . . ."[39]

Police can also track many modern smartphones through GPS technology.[40] The U.S. Department of Defense maintains the GPS system using twenty-four satellites that orbit the Earth.[41] The government allows civilian manufacturers, including cell phone producers, to use the system.[42]

---

[30] *Id.*
[31] *See* ACLU Brief, *supra* note 16, at 15.
[32] American Civil Liberties Union, *ACLU Affiliate Nationwide Cell Phone Tracking Public Records Requests Findings and Analysis* 5, http://www.aclu.org/files/assets/cell_phone_tracking_documents_-_final.pdf (last visited Oct. 25, 2014).
[33] *Jones*, 908 F. Supp. 2d at 207.
[34] *Id.*
[35] *See* ACLU Brief, *supra* note 16, at 15.
[36] Clarence Walker, *New Hi-Tech Police Surveillance: The "StingRay" Cell Phone Spying Device*, CENTRE FOR RESEARCH ON GLOBALIZATION (Apr. 13, 2013), http://www.globalresearch.ca/new-hi-tech-police-surveillance-the-stingray-cell-phone-spying-device/5331165.
[37] *Id.*
[38] Parker Higgins & Trevor Timm, *What the FBI Doesn't Want You To Know About Its "Secret" Surveillance Techniques*, ELEC. FRONTIER FOUND. (Jan. 17, 2013), https://www.eff.org/deeplinks/2013/01/what-fbi-doesnt-want-you-know-about-its-surveillance-techniques.
[39] Walker, *supra* note 36.
[40] Statement of Prof. Blaze, *supra* note 3, at 11–12.
[41] Rutherford Institute Brief, *supra* note 18, at 6.
[42] *Id.*

Every device that uses GPS technology is embedded with an individualized computer chip that can pinpoint a user's location anywhere on Earth.[43] GPS satellites are able to determine a smartphone's location to within approximately ten meters.[44] Disrupting the ability of GPS satellites to locate devices carrying this technology is against federal law.[45] However, many smartphones allow users to disable the GPS tracking feature.[46]

Some phones even have tracking chips that store a variety of information that can potentially offer law enforcement a comprehensive sketch of a cell-phone user's movements throughout the day.[47] For instance, certain versions of Apple's iPhone collect "geographic data" every time users turn on the Location Services option in their phones' settings or when they use a GPS application.[48] The device will save information about nearby cell-phone towers and WiFi hotspots, assign the data a random identification number, and transmit it to Apple every twelve hours (or whenever Internet access next become available).[49] Using any one of these methods, law-enforcement agencies can determine a user's location easily and cheaply.

II. THE NEED FOR LEGISLATION

Cell-phone use in the United States is ubiquitous.[50] As of April 2012, a total of 88 percent of American adults owned a cell phone.[51] By December 2012, there were approximately 326,400,000 wireless subscriber connections in the country.[52] This means that there are at least ten million more wireless connections than people in the U.S. today.[53] Additionally, in 35.8 percent of American households, cell phones have replaced traditional

---

[43] *Id.*

[44] Statement of Prof. Blaze, *supra* note 3, at 11.

[45] Rutherford Institute Brief, *supra* note 18, at 6–7 (explaining that jamming GPS technology violates 27 U.S.C. § 333 and 47 U.S.C. § 301).

[46] *See* Statement of Prof. Blaze, *supra* note 3, at 12.

[47] Rutherford Institute Brief, *supra* note 18, at 13.

[48] *Id.*; Brian X. Chen, *Why and How Apple is Collecting Your iPhone Location Data*, WIRED (Apr. 21, 2011), http://www.wired.com/gadgetlab/2011/04/apple-iphone-tracking.

[49] Rutherford Institute Brief, *supra* note 18, at 13; Chen, *supra* note 48.

[50] *See* Joanna Brenner, *Pew Internet: Mobile*, PEW INTERNET & AM. LIFE PROJECT (Jan. 31, 2013), http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx.

[51] Smith, *supra* note 2.

[52] CTIA—The Wireless Ass'n, *Quick Wireless Facts*, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (last visited Oct. 25, 2014).

[53] *Id.*; *U.S. & World Population Clocks*, U.S. CENSUS BUREAU, http://www.census.gov/popclock/. Note that the number of wireless connections accounts for tablets and other devices in addition to cell phones.

home phones completely.[54] Cell phones have become a principal feature of contemporary American life.

With the rise of multifunctional smartphones, such as iPhones and BlackBerry devices, cell phones have become even more important. They operate not only as telephones but also as personal digital organizers, cameras, email readers, music players, etc.[55] As one technology expert put it, "[w]e now carry our phones with us wherever we go, and we expect them to have service wherever we happen to be."[56]

As Americans increasingly rely on their cell phones, police continually devote more attention to tracking mobile devices in order to monitor suspects and persons of interest.[57] Data suggests that police are, to some extent, replacing traditional wiretaps with cell-phone tracking.[58] In 2011, the number of warrants issued for wiretaps decreased 14 percent while nine cell-phone service providers responded to 1.3 million police demands for user information.[59] In fact, in order to handle the massive volume of requests, most service providers pay teams of lawyers, data technicians, and other professionals to review requests and provide data to police twenty-four hours a day.[60]

Obtaining tracking information is less expensive and less time-consuming for law enforcement than securing a warrant to wiretap a suspect's phone.[61] A shift away from wiretaps is troublesome because police can increasingly evade the privacy protections of the Electronic Communications Privacy Act (ECPA), a comprehensive statute that places limitations on police wiretapping as well as electronic and aural eavesdropping.[62] Significantly, the interceptions prohibited by ECPA are those that capture a communication's "content," in other words, "information concerning [its] substance, purport, or meaning."[63] Since cellular location data does not include content, the statute does not regulate

---

[54] *See Quick Wireless Facts*, *supra* note 52.
[55] Statement of Prof. Blaze, *supra* note 3, at 9.
[56] *Id.*
[57] *See* Lichtblau, *supra* note 5.
[58] *Id.*
[59] *Id. See also Wiretap Reports*, ADMIN. OFF. OF THE U.S. CTS., http://www.uscourts.gov/Statistics/WiretapReports.aspx (last visited Oct. 25, 2014) for lists of electronically available wiretap statistics for each year from 1997 until 2011.
[60] Lichtblau, *supra* note 5.
[61] *Id.*
[62] Electronic Communications Privacy Act, 18 U.S.C. §§ 2510–22 (2012).
[63] 18 U.S.C. § 2510(8) (2002); Charles Doyle, *Privacy: An Overview of the Electronic Communications Privacy Act* 10, CONG. RES. SERVICE (2012), *available at* http://www.fas.org/sgp/crs/misc/R41733.pdf.

its interception, use, or disclosure.[64] Instead, the widespread police practice of obtaining cellular location information from providers is left in the hands of the courts.[65] Judges, limited to deciding particular cases with particular facts, are simply unable to fashion broad, detailed regulatory schemes like ECPA.[66] The practice should be regulated alonh the same lines as wiretapping in order to protect modern privacy expectations. Any judicial substitute would fall short of that goal.

III. *UNITED STATES V. JONES* OFFERS LITTLE GUIDANCE

The Supreme Court opinion in *United States v. Jones* does not offer direct guidance to lower courts on the question of government cellular geolocation data surveillance.[67] In *Jones*, Justice Scalia, writing for the majority, held that the government's warrantless physical occupation of someone's property qualifies as a per se "search" under the Fourth Amendment.[68] In that case, the government attached a GPS tracking device underneath the defendant's car and monitored his movements on public roadways for twenty-eight days—all without a search warrant.[69] Justice Scalia concluded that this kind of common-law trespass would constitute a violation of the Fourth Amendment as it was understood at the time of the Amendment's ratification and was therefore not acceptable without a warrant.[70]

The holding in *Jones* does not repudiate the "reasonable expectation of privacy" test developed in *Katz v. United States*, but rather complements it.[71] In fact, Justice Sotomayor and Justice Alito both wrote concurring opinions in *Jones* that embraced the application of the "reasonable expectation of privacy" test from *Katz*.[72] In *Katz*, the Court held that the Fourth Amendment protects "people, not places" and the government's placement of a listening device on the outside of a public telephone booth qualified as a Fourth Amendment "search."[73] The "reasonable expectation

---

[64] *See* 18 U.S.C. § 2510(8); 18 U.S.C. § 2511.
[65] *See* 18 U.S.C. § 2510(8).
[66] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 875 (2004).
[67] *See generally* United States v. Jones, 132 S. Ct. 945 (2012). Similarly, in *Riley v. California*, 134 S. Ct. 2473 (2014), the Supreme Court issued a 9-0 decision mandating strong Fourth Amendment protection for substantive data on cell phones such as photographs and videos. While important, that decision does not provide direct guidance on the issue of cell phone tracking either.
[68] *Id.* at 949.
[69] *Id.* at 948–49.
[70] *Id.* at 949.
[71] *Id.* at 953.
[72] *Id.* at 954–55 (Sotomayor, J., concurring); *id.* at 958 (Alito, J., concurring).
[73] Katz v. United States, 389 U.S. 347, 351 (1967).

of privacy" test applied in subsequent cases derives from Justice Harlan's famous concurrence, in which he maintained that the Fourth Amendment has 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.'"[74] Since Justice Scalia's majority opinion did not supplant this test, the government's obtainment of cellular location data from a service provider would fall under the *Katz* test.[75] Indeed, as Justice Scalia explicitly stated, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[76] And as Justice Sotomayor remarked in her concurrence, "[i]n cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority's . . . trespassory test may provide little guidance."[77]

While Justice Sotomayor endorsed both the majority rule and the *Katz* test,[78] Justice Alito rejected Justice Scalia's property-based rule.[79] Instead, Justice Alito would have held for the defendant using a strict *Katz* analysis.[80] Without providing much explanation, he stated simply that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy," and "[w]e 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."[81] Justice Scalia rightfully criticized this conclusion for raising two important unanswered questions.[82] First, if extended GPS tracking would impinge on reasonable expectations of privacy only for "most offenses," what kind of offenses would legitimize such an investigation?[83] And, second, why is four weeks "surely" too long?[84] The answers to these thorny questions should be determined by a legislative body that, as Justice Alito wrote, is "well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[85]

---

[74] *Id.* at 361 (Harlan, J., concurring).
[75] *See Jones*, 132 S. Ct. at 953.
[76] *Id.* (emphasis in original).
[77] *Id.* at 955 (Sotomayor, J., concurring).
[78] *Id.* at 954–55
[79] *Id.* at 957–58 (Alito, J., concurring).
[80] *Id.* at 958.
[81] *Id.* at 964.
[82] *Id.* at 954 (majority opinion).
[83] *Id.*
[84] *Id.*
[85] *Id.* at 964 (Alito, J., concurring).

IV. THE INADEQUACY OF THE CURRENT DOCTRINE

Since *Jones* does not address the problem, lower courts must turn to general Fourth Amendment jurisprudence in order to determine the boundaries of society's reasonable privacy expectations for cellular location data. Unfortunately, courts face a major doctrinal obstacle in aligning Fourth Amendment protections with modern societal norms in the "third-party doctrine"—the idea that when a person shares information with or allows her information to be seen by others, she forfeits her expectations of privacy in that information.[86] While explicating this same basic principle, the Supreme Court has articulated three different manifestations of this doctrine throughout the years.[87]

The first manifestation, referred to as the "knowing exposure" doctrine, was originally articulated in *Katz* when the Court wrote that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[88] The Court applied this doctrine in *United States v. Knotts*, when it held that a "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[89] This idea was expanded in the three so-called "flyover cases," where the Court held that police could observe activities on private property from an aircraft and not run afoul of the Fourth Amendment so long as they stayed in the air.[90]

The second manifestation of the doctrine is referred to as the "general use" idea.[91] In one of the flyover cases, the Court held that a Fourth Amendment "search" does not occur when the government uses technology to survey private property as long as the gadget is "generally available to the public."[92] Therefore, in *Dow Chemical v. EPA*, the government did not conduct a "search" when it used a $22,000 mapmaking camera mounted to an airplane to spy on private property because cameras are readily available to the public.[93]

---

[86] *Making the Most of* United States v. Jones, *supra* note 14, at 2.
[87] *Id.* at 7 n.30.
[88] Katz v. United States, 389 U.S. 347, 351 (1967).
[89] United States v. Knotts, 460 U.S. 276, 281 (1983).
[90] Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, THE FUTURE OF THE CONSTITUTION 4 (Brookings Inst., Dec. 8, 2010), *available at* http://www.brookings.edu/~/media/research/files/papers/2010/12/08%204th%20amendment%20slobogin/1208_4th_amendment_slobogin.pdf (last visited Oct. 25, 2014).
[91] *Id.* at 5.
[92] Dow Chem. Co. v. EPA, 476 U.S. 227, 238 (1986).
[93] *Id.*; Slobogin, *supra* note 90, at 5.

The third and final manifestation of the doctrine is referred to as the "assumption of the risk" principle.[94] The two principal cases articulating the assumption of the risk doctrine are *Miller v. United States* and *Smith v. Maryland*.[95] In *Miller*, the government had obtained copies of the defendant's checks and various records from two of his banks using allegedly defective subpoenas but nonetheless successfully submitted them into evidence during a criminal trial.[96] The Court held that there was no Fourth Amendment violation because a person "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government . . . even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed."[97] The Court went so far as to say that even if the banks acted "solely as Government agents" in copying Miller's information and "complying without protest," their deeds did not violate anyone's Fourth Amendment rights.[98] Furthermore, the banks' failure even to notify Miller about their cooperation with law enforcement was not problematic.[99] In a footnote, the Court deemed this omission "neglect without legal consequences . . . however unattractive it may be."[100]

Dissenting in *Miller*, Justice Brennan quoted at length from *Burrows v. Superior Court*, a California Supreme Court opinion about a case with similar facts.[101] In *Burrows*, a unanimous California Supreme Court concluded that individuals have a reasonable expectation of privacy in bank documents created within the ordinary course of business.[102] The court rejected the view that a depositor surrenders his Fourth Amendment interests in his bank records just because a "detached and disinterested" bank might voluntarily disclose their contents.[103] The reason is because giving financial information to a bank "is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account."[104] The consequences of revoking someone's Fourth Amendment interests in his banking habits are particularly pernicious because, "[i]n the course of such dealings, a

---

[94] Slobogin, *supra* note 90, at 6.
[95] *Id.*
[96] Miller v. United States, 425 U.S. 435, 436–37 (1976).
[97] *Id.* at 443.
[98] *Id.*
[99] *Id.* at 443 n.5.
[100] *Id.*
[101] *Id.* at 447–55 (Brennan, J., dissenting); Burrows v. Superior Court, 529 P.2d 590 (1974).
[102] *Miller*, 425 U.S. at 448–49 (Brennan, J., dissenting) (citing *Burrows*, 529 P.2d at 593).
[103] *Id*. at 451.
[104] *Id.*

depositor reveals many aspects of his personal affairs, opinions, habits, and associations. Indeed, the totality of bank records provides a virtual current biography."[105] With keen foresight, the court went on to remark that the "[d]evelopment of photocopying machines, electronic computers and other sophisticated instruments have accelerated the ability of government to intrude into areas which a person normally chooses to exclude from prying eyes and inquisitive minds."[106] Therefore, courts interpreting constitutional protections of privacy must "keep pace with the perils created by these new devices."[107]

However, the California Supreme Court's warning did not prevent the assumption-of-the-risk doctrine from solidifying. Three years after *Miller*, the Supreme Court decided *Smith* using the same rule.[108] In *Smith*, the police had installed a device called a pen register at a telephone company (with the company's consent) to record any phone numbers the defendant dialed from his house.[109] Smith was convicted of robbery after evidence at trial showed he had called a number which connected him to the crime.[110] Smith argued for the suppression of the evidence on Fourth Amendment grounds,[111] but the Court ultimately held that when a person "voluntarily" dials a phone number, he "assume[s] the risk that the company would reveal to police the numbers he dialed."[112]

Assumption of the risk was what Justice Sotomayor was referring to in *Jones* when she wrote, "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information disclosed to third parties."[113] She elaborated:

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the "tradeoff" of privacy for convenience "worthwhile," or come to accept this "diminution of privacy" as "inevitable," . . . and perhaps not. I for one doubt that people would

---

[105] *Id.*
[106] *Id.* at 451.
[107] *Id.*
[108] Smith v. Maryland, 442 U.S. 745, 744 (1979).
[109] *Id.* at 737.
[110] *Id.* at 737–38.
[111] *Id.* at 737.
[112] *Id.* at 744.
[113] United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

> accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy. I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[114]

The assumption-of-the-risk leg of the third-party doctrine is particularly relevant to a discussion about tracking. Even if a person is "voluntarily" transmitting electronic information to a cellular-service provider, it does not necessarily follow that she is willing to have all of her cellular location data arbitrarily (or even non-arbitrarily) handed over to the police. Viewed in the aggregate and considering how frequently people carry their phones with them outside their homes, cellular location data can paint a vivid and revealing portrait of someone's life. In order to keep those details out of government hands, cellular location data should be kept private.

One scholar refers to this concept as the "mosaic theory"—"the idea that certain types of governmental investigation enable accumulation of so many individual bits about a person's life that the resulting personality picture is worthy of constitutional protection."[115] Not only did Justice Sotomayor express support for the idea,[116] so did Justice Alito when he wrote that "society's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual's car for a very long period."[117] Discussing a case about the warrantless installation of a GPS device similar to that in *Jones*, the New York Court of Appeals put it this way:

> Disclosed in the data retrieved from the transmitting unit, nearly instantaneously with the press of a button on the highly portable receiving unit, will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on. What the technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations—political, religious, amicable and

---

[114] *Id.*
[115] Slobogin, *supra* note 14, at 3–4.
[116] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).
[117] *See id.* at 964 (Alito, J., concurring).

> amorous, to name only a few—and of the pattern of our professional and avocational pursuits.[118]

Whether the GPS data comes from a discreetly installed GPS device or directly from someone's phone makes no difference. The threat of governmental intrusion into the private lives of citizens is the same. Notably, the New York Court of Appeals decided its GPS case under the New York State Constitution instead of federal law because so many federal appellate courts had not yet weighed in on the issue.[119] Unfortunately, federal judicial theory has not yet caught up with today's technological landscape and society's evolving expectations of privacy.[120] And while not insurmountable, the third-party doctrine could very likely stymie the efforts of federal courts to revamp this area of law and lead to logically constrained opinions as judges attempt to reconcile precedent with today's brave new world. Therefore, Congress, not the courts, should take the lead on this issue by introducing legislation that would constrain the third-party doctrine and establish robust privacy protections for cellular location data.

V. LEGISLATION

Legislation is needed to protect the privacy of Americans leading twenty-first century lives. Congressional legislators introduced two bills in 2012 that, if passed, would have regulated the disclosure of cellular location information.[121] The first did not address the problems associated with government tracking and therefore would not have protected citizens' Fourth Amendment rights.[122] The second, which legislators reintroduced in 2013,[123] does address cellular location data privacy problems and is a terrific improvement over the status quo,[124] although it could be strengthened with additional provisions to ensure greater law-enforcement accountability.

---

[118] People v. Weaver, 12 N.Y.3d 433, 441–42 (2009).
[119] *Id.* at 445.
[120] *See id.* But see United States v. Maynard, 278 Fed. App'x 214 (2008), for a lower federal court holding using logic similar to that used in *Weaver*.
[121] Location Privacy Protection Act of 2012, S. 1223, 112th Cong. (2012); Geolocation Privacy and Surveillance Act, H.R. 2168, 112th Cong. (2012).
[122] *See* S. 1223.
[123] Geolocation Privacy and Surveillance Act, H.R. 1312, 113th Cong. (2013), *H.R. 1312 (113th): Geolocation Privacy and Surveillance Act*, GOVTRACK, http://www.govtrack.us/congress/bills/113/hr1312#overview (last visited Oct. 25, 2014) [hereinafter GOVTRACK, H.R. 1312 (113th)]; Geolocation Privacy and Surveillance Act, S. 639, 113th Cong. (2013), *S. 639 (113th): Geolocation Privacy and Surveillance Act*, GOVTRACK, http://www.govtrack.us/congress/bills/113/s639 (last visited Oct. 25, 2014) [hereinafter GOVTRACK, S. 639 (113th)].
[124] *See* H.R. 2168. *See also* H.R. 1312.

The first bill was the "Location Privacy Protection Act of 2012," sponsored by Senator Al Franken (D-MN).[125] Unless an exception applied, the Location Privacy Protection Act would not have allowed certain entities, including service providers,[126] to "knowingly collect, receive, record, obtain, or disclose to a nongovernmental individual or entity the geolocation information from an electronic communications device without the express authorization of the individual that is using the electronic communications device."[127] The term "electronic communications device" would have almost certainly included cell phones,[128] and "geolocation information" would have included cell-site, GPS, and WiFi data.[129] However, the legislation would not have prevented warrantless government searches of that information.[130] The central provision of the Location Privacy Protection Act would have only regulated disclosure to *nongovernmental* individuals and entities.[131] Furthermore, the legislation included an explicit exception for providers disclosing customer geolocation information in response to a request from any "law enforcement or intelligence agency of the United States, a State, or a political subdivision of a State" with no warrant requirement.[132] The legislation, which would have created an private right of action for violations,[133] appeared to be primarily designed as a consumer-protection law and not as a solution to any Fourth Amendment problems.[134]

The other act under consideration by Congress, the "Geolocation Privacy and Surveillance Act" (GPS Act), is far superior because it directly addresses government searches.[135] The original GPS Act died in committee in 2012,[136] but on March 21, 2013, Representative Jason Chaffetz (R-UT) reintroduced it in the House, and Senator Ron Wyden (D-OR) reintroduced a companion bill in the Senate.[137] The principal provision of the Act echoes

---

[125] S. 1223, *S. 1223 (112th): Location Privacy Protection Act of* 2012, GOVTRACK, http://www.govtrack.us/congress/bills/112/s1223 (last visited Oct. 25, 2014).
[126] S. 1223 § 2713(a)(1).
[127] *Id.* § 2713(b)(1).
[128] *See id.* § 2713(a)(2).
[129] *Id.* § 2713(a)(4).
[130] *See id.* § 2713(b)(1), (b)(2)(F).
[131] *Id.* § 2713(b)(1).
[132] *Id.* § 2713(b)(2)(F).
[133] *Id.* § 2713(d)(3).
[134] *See generally id.*
[135] Geolocation Privacy and Surveillance Act, H.R. 1312 § 2602(h), 113th Cong. (2013).
[136] *H.R. 2168 (112th): Geolocation Privacy and Surveillance Act*, GOVTRACK, http://www.govtrack.us/congress/bills/112/hr2168 (last visited Oct. 25, 2014).
[137] GOVTRACK, H.R. 1312 (113th), *supra* note 123; GOVTRACK, S. 639 (113th), *supra* note 123.

the language of 18 U.S.C. § 2510 in ECPA, and, except as otherwise specified, prohibits the actual or attempted intentional interception, disclosure, or use of a person's geolocation information.[138] "Geolocation information" for purposes of the GPS Act means "any information that is not the content of a communication, concerning the location of a wireless communication device or tracking . . . device that, in whole or in part, is generated by or derived from the operation of that device" and can be used to determine the location of the device's user.[139] This broad statement would cover both historical and prospective cellular location data.[140] The GPS Act, therefore, would provide significant privacy protection for cell-phone users.

Rep. Chaffetz testified at a subcommittee hearing that he introduced the GPS Act because "the government and law enforcement should not be able to track somebody indefinitely without their knowledge or consent or without obtaining a probable cause warrant from a judge."[141] The legislation, if passed, would require government entities to obtain a warrant upon probable cause before they could ask a provider for a customer's geolocation information.[142] Unlike ECPA, however, the GPS Act does not detail the exact procedural requirements that law enforcement or investigative officers must follow in order to obtain a warrant.[143] Instead, the warrant provision in the GPS Act refers to the general Federal Rule of Criminal Procedure regarding search and seizure.[144] While certainly an improvement over current state of the law, a more particularized warrant provision embedded within the GPS Act would offer more robust privacy protections. For example, the warrant provision could adopt the rule in ECPA requiring officers applying for a warrant to state whether or not less intrusive surveillance procedures have been tried or if such a procedure would be impractical or too dangerous.[145] Another protection that could be borrowed from ECPA is the provision stipulating that officers must make a "full and complete statement of the facts" regarding previous warrant

---

[138] *Compare* 18 U.S.C. § 2510 (2002) *with* H.R. 1312 § 2602(a)(1), 113th Cong. (2013).
[139] H.R. 1312 § 2601(3).
[140] *See id.*; *see also Geolocation Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 23 (2012) (statement of Rep. Robert C. Scott).
[141] *Geolocation Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 22 (2012) (statement of Rep. Jason Chaffetz).
[142] H.R. 1312 § 2602(h)(2).
[143] *Compare* 18 U.S.C. § 2518 (1998) *with* H.R. 1312 § 2602(h).
[144] *See* H.R. 1312 § 2602(h)(2).
[145] 18 U.S.C. § 2518(1)(c).

applications concerning the "same persons, facilities or places."[146] Furthermore, a reporting requirement should be added so that the Administrative Office of the United States Courts can publish statistics on tracking. By including these provisions in the Act, legislators could ensure that law-enforcement officials are held accountable for their surveillance activities.

While the bill could use improvement, overall it is well crafted and balanced. Tracking the language of ECPA almost exactly, the GPS Act would prohibit the use of illicitly procured geolocation information as evidence.[147] And like the Location Privacy Protection Act, the GPS Act would prohibit providers from disclosing consumer geolocation information generally (due to profit motivations or otherwise).[148] However, the GPS Act would wisely insulate businesses that collect geolocation information in the normal course of business from liability.[149] It also includes other common-sense exceptions for instances of consent,[150] when the information is already public,[151] the interception of information during emergency situations as when someone's "life or safety . . . is threatened,"[152] and when the owner of a device authorizes a person acting under color of law to locate someone who has unlawfully taken the device.[153] Finally, just as in ECPA, the legislation would allow for both criminal punishment and civil remedies in case of a violation while also providing for certain "good faith" defenses to such actions.[154]

Notably, the predecessor of the current bill enjoyed the support of both the ACLU and from industry.[155] Catherine Crump, an ACLU staff attorney, testified at a congressional subcommittee hearing that the GPS Act "would allow legitimate law enforcement investigations to proceed, while ensuring that innocent Americans do not have their privacy intruded

---

[146] *Id.* § 2518(1)(e).
[147] H.R. 1312 § 2605.
[148] *Compare* S. 1223 § 2713(b)(1), 112th Cong. (2012) *with* H.R. 1312 § 2602(a)(1).
[149] H.R. 1312 § 2602(b).
[150] *Id.* § 2602(d).
[151] *Id.* § 2602(e).
[152] *Id.* § 2602(f).
[153] *Id.* § 2602(g).
[154] *Compare* 18 U.S.C. § 2515 (1968) *and* 18 U.S.C. § 2511(4) (2008) *and* 18 U.S.C. § 2520 (2002) *and* 18 U.S.C. § 2522 (1994) *with* H.R. 1312 § 2602 *and* H.R. 1312 § 2605, 113th Cong. (2013).
[155] Statement of Crump, *supra* note 8, at 47; *see Geolocation Privacy and Surveillance (GPS) Act: Hearing on H.R. 2168 Before the Subcomm. on Crime, Terrorism, & Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 45–46 (2012) (statement of Edward J. Black, President & CEO, Comp. & Comm'ns Indus. Assoc.) [hereinafter Statement of Black].

upon."[156] Without a law requiring judicial oversight of police tracking, she opined, "[i]nnocent Americans can never be confident that they are free from round-the-clock surveillance by law enforcement of their activities."[157] Just as important, telecommunications corporations and Internet companies also support a warrant requirement.[158] Edward J. Black, president and CEO of the Computer & Communications Industry Association, spoke at the same hearing to emphasize that businesses in the technology sector want clarifying legislation in order to alleviate consumer concerns about the vulnerability of their geolocation information.[159] On behalf of his organization's member companies, which employ over half a million workers in the United States,[160] Black endorsed the legislation.[161] The GPS Act's popularity with both civil libertarians and industry insiders shows that the legislation enjoys broad support and therefore should be enacted promptly.

CONCLUSION

Obtaining a warrant is not an overly cumbersome task and is made relatively simple with modern technology.[162] In thirty-four states and the District of Columbia, police can apply for a warrant remotely by telephone or electronic means.[163] This includes via e-mail, facsimile, or even text.[164] In Utah, for example, one law enforcement officer calculated that he can obtain an electronic warrant in about twenty minutes.[165] With warrants so easy to procure today, there is little reason why Congress should not pass a bill mandating warrants for cell-phone tracking in non-emergency situations. The simple act of engaging in a modern activities, like using cell phones, should not force Americans to sacrifice their constitutionally protected right to privacy. Adopting a comprehensive geolocation information privacy statute like the GPS Act, even without the suggested improvements mentioned above, would go a long way towards protecting

---

[156] Statement of Crump, *supra* note 8, at 47.
[157] *Id.* at 50.
[158] *Id.* at 48.
[159] Statement of Black, *supra* note 155, at 42–43.
[160] *Id.* at 38.
[161] *Id.* at 45–46.
[162] Brief of the Nat'l Ass'n of Criminal Defense Lawyers et al. as Amici Curiae Supporting Respondent at 18, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10–1259).
[163] *Id.*
[164] *Id.* at 18–19.
[165] *Id.* at 19.

what Justice Louis Brandeis called "the most comprehensive of rights and the right most valued by civilized men"—"the right to be let alone."[166]

[166] Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).