May, 2013

# Has Skinner Killed the Katz? Are Society's Expectations of Privacy Reasonable in Today's Techological World?

Jason Forcier

# HAS SKINNER KILLED THE KATZ?
# ARE SOCIETY'S EXPECTATIONS OF PRIVACY REASONABLE IN TODAY'S TECHNOLOGICAL WORLD?

By Jason Forcier*

## I. INTRODUCTION

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[1]

Is it possible to know if the right to privacy exists anymore in America, when carrying a cell phone? Does the creation of a mobile citizenry, through the exponential increase of using cellular technology,[2] create a society that may no longer expect that there is *any* form of privacy when using mobile technology? Should privacy be all or none, simply based on the whether a person uses cellular technology to keep in touch with those around him or her? Does the ability to manipulate technology to disclose information, otherwise unobtainable, create an unreasonable expectation of privacy? As technology continues to expand should society continue to relinquish its remaining interest in privacy, for the sake of technological advancements? These are questions many are desperately searching for answers to.

The battleground over the right to privacy in America's technological society is taking place on the frontlines of the United States' courts system. Since the advent of the telephone, the

---

* Jason Forcier is a 2014 Juris Doctorate candidate at Phoenix School of Law and Managing Editor of Accord, PHOENIX LAW REVIEW's online journal. The author would like to thank Associate Professor Daniel Dye and Associate Professor Judge (ret.) Michael Jones for their assistance and advice while writing this article.

[1] U.S. CONST amend. IV.

[2] *Wireless Quick Facts*, CITA ADVOCACY, http://www.ctia.org/advocacy/research/index.cfm/aid/10323 (last visited April 19, 2013) (nationwide, cellular subscriptions grew from 48.7M in 1997 to 321.7M in 2012. Cell phone-only households grew from 10.5% in 2007 to 35.8% in 2012.). *See also* Stephen J. Blumberg & Julian V. Luke, *Wireless Substitution: State-level Estimates From the National Early National Health Interview Survey, 2010–2011*, NATIONAL CENTER FOR HEALTH STATISTICS, October 12, 2012, http://www.cdc.gov/nchs/data/nhsr/nhsr061.pdf (last visited April 19, 2013); *See also* Glenn Greenwald, *Are all telephone calls recorded and accessible to the US Government? A former FBI counterterrorism agent claims on CNN that this is the case*, THE GUARDIAN, (May 4, 2013), http://www.guardian.co.uk/commentisfree/2013/may/04/telephone-calls-recorded-fbi-boston.

courts have struggled to maintain a balance between the attempts of law enforcement to thwart the schemes of criminals, and the express language and intent of the Framers under the Fourth Amendment of the U.S. Constitution.[3] In the past, courts have routinely held that there is no "reasonable expectation of privacy in the data given off by . . . cellphone[s]."[4] However, even in recent decisions, like *Skinner*, there are ever increasing splits of whether or not a right to privacy may now exist when it comes to society's expectations.[5] Additionally, other recent developments over the last year may lend support to privacy advocates that the time has come for the courts to recognize a right to privacy with regard to the transmission of cell phone data through manipulation by law enforcement.[6]

This article reconciles recent developments of notable split-court opinions and recent attempts by Congress and state legislatures to limit the actions of law enforcement by requiring probable cause when seeking location data of a person's cell phone. Part II discusses the history of *United States v. Skinner*. Part III surveys attempts by Congress and state legislatures to limit law enforcement use of subpoenas to track cell phones. Part IV examines how law enforcement uses subpoenas and the technology that makes possible the tracking and pinpointing of a cell

---

[3] U.S. CONST amend. IV; Olmstead v. United States, 277 U.S. 438 (1928) (use of wiretapped telephone conversations, obtained by federal law enforcement, without a search warrant, did not violate the defendant's Fourth and Fifth Amendments), *overruled by* Katz v. United States, 389 U.S. 347 (1967) (Overruling *Olmstead*, the Court extended Fourth Amendment protection to all areas where a person has a reasonable expectation of privacy); *See also* United States v. Karo, 468 U.S. 705,716 (1984) ("Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight."); *See also* Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a "search" and is presumptively unreasonable without a warrant.").

[4] United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (*citing* United States v. Knotts, 460 U.S. 276 (1983); *See also* Smith v. Maryland, 442 U.S. 735 (1979); *See also* United States v. Forest, 335 F.3d 942 (6th Cir. 2004).

[5] *See* United States v. Skinner, 690 F.3d 772, 784 (6th Cir. 2012) (Donald, J. concurring).

[6] Ryan Gallagher, *Feds Accused of Hiding Information From Judges About Covert Cellphone Tracking Tool*, March 28, 2013, http://www.slate.com/blogs/future_tense/2013/03/28/stingray_surveillance_technology_used_without_proper_approval_report.html; *See also In re* the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 890 F. Supp. 2d 747 (S.D. Tex. 2012); *See* discussion, *infra* Part III.

phone. Part V discusses and analyzes recent public opinion surveys and polls. Part VI analyzes why the Supreme Court should settle the issue of whether law enforcement should obtain a search warrant prior to gathering geolocation[7] data from cellular devices and the manipulation of cellular devices with tracking technology that is not generally available to the public.

## II. UNITED STATES V. MELVIN SKINNER SUMMARY

### *A. Facts of the case*

In 2007 federal prosecutors charged Melvin Skinner ("Skinner") with two counts drug trafficking, and one count of conspiracy to commit money laundering for his role as a courier in a large, multi-state drug-trafficking ring, led by James Michael West ("West").[8] Following a ten-day trial, a jury of his peers convicted Skinner and sentenced him to 235 months of imprisonment.[9]

The events relating to *Skinner* begin in January 2006 when police stopped Christopher Shearer ("Shearer"), a co-conspirator in West's drug-trafficking operation, near Flagstaff, Arizona with $362,000 in cash.[10] Shearer was on his way to deliver drug-related profits to West's marijuana supplier, Philip Apodaca ("Apodaca"), located in Tucson, Arizona.[11]

To manage his part of the drug trafficking operation and maintain covert communications with his couriers, Apodaca purchased readily available pay-as-you-go cell phones and preprogrammed various contacts, under fictitious names, and gave these cell phones to his

[7] H.R. 2168, §2601(3); S.B. 1212 §2601(4) ("The term 'geolocation information' means, with respect to a person, 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 that could be used to determine or infer information regarding the location of the person").
[8] *Skinner*, 690 F.3d at 775.
[9] *Id*. Skinner was convicted on three counts. *See* 21 U.S.C. §§ 846, 841(a)(1), 841(b)(1)(A) (West); *see* 18 U.S.C. § 1956(h) (2012) (West); *see* 21 U.S.C. §§ 846, 841(a)(1), 841 (b)(1)(B), and 18 U.S.C. §2 (West).
[10] *Skinner*, 690 F.3d at 775.
[11] *Id*.

couriers.[12] From time-to-time, Apodaca would discard and replace the cell phones with new ones to maintain secrecy and security of the drug operation.[13]

In May and June 2006, during the investigation, Drug Enforcement Agency ("DEA") agents obtained wiretap court orders for two phones owned by West.[14] The DEA agents learned through monitoring calls between West and Shearer of a truck driver, codenamed "Big Foot" (later identified as Skinner), as a courier in West's trafficking operation.[15] Not long afterwards, the DEA agents further learned that West was using separate secret cellphones to communicate with Apodaca and Skinner.[16]

Based on this information collected from the wiretaps, authorities learned Big Foot and Apodaca scheduled a meeting for later in July 2006, in Tucson, so Big Foot could pick up 900 pounds of marijuana and transport it to West, located in Tennessee.[17] Subsequently, DEA Agents obtained subpoenas for cellular service providers to provide the geolocation data of the phone thought to belong to Big Foot.[18]

By continuously "pinging" Big Foot's phone, DEA agents tracked his movements while enroute to meet with Apodaca on July 14, 2006.[19] At no point did agents conduct any form of visual surveillance of Big Foot or his vehicle.[20] On July 16, 2006, near Abilene, Texas, agents tracked Big Foot to a truck stop.[21] Discovering a motorhome with Georgia license plates matching a description from previous wiretapped conversations, agents confronted the driver,

---

[12] *Id*.
[13] *Id*.
[14] *Id*.
[15] *Id*.
[16] *Id*.
[17] *Skinner*, 690 F.3d at 776.
[18] *Id*.
[19] *Id*.
[20] *Id*.
[21] *Id*.

later identified as Skinner.[22] After Skinner denied consent to the DEA agent's request to search the motorhome, the DEA agent requested a K–9 officer and dog to the scene to conduct a perimeter dog sniff around the motorhome.[23] During the dog sniff, the dog alerted the officers to the presence of narcotics.[24] Entering the motorhome, officers discovered sixty-one bales of marijuana, more than 1,100 pounds, two cell phones and two handguns. Consequently, Skinner, and his son who was also present, was arrested.[25]

At the arraignment, Federal prosecutors charged Skinner with conspiracy to distribute and possess with intent to distribute in excess of 1,000 kilograms of marijuana,[26] conspiracy to commit money laundering,[27] and aiding and abetting the attempt to distribute in excess of 100 kilograms of marijuana.[28]

In a motion to suppress, Skinner sought to suppress the search of the motorhome.[29] He alleged the use of geolocation data emitted from his cell phone, by DEA agents, constituted a warrantless search that violated the Fourth Amendment.[30] Following an evidentiary hearing, the trial judge determined that Skinner lacked standing to assert Fourth Amendment protection because he did not own the cell phone used in the drug trafficking scheme.[31] Furthermore, the trial judge held Skinner lacked a legitimate expectation of privacy while using the cell phone on public roads, and therefore lacked a legitimate expectation of privacy in the cell phone itself or in the motorhome.[32] Last, the trial judge held that, in this case, even if the search were

---

[22] *Id*.
[23] *Skinner*, 690 F.3d at 776.
[24] *Id*.
[25] *Id*.
[26] *Id*. *See* 21 U.S.C. §§ 846, 841(a)(1), and 841(b)(1)(A) (West).
[27] *Skinner*, 690 F.3d at 776. *See* 18 U.S.C. § 1956(h) (2012) (West).
[28] *Skinner*, 690 F.3d at 776. *See* 21 U.S.C. §§ 846, 841(a)(1), 841 (b)(1)(B), and 18 U.S.C. §2 (West).
[29] *Skinner*, 690 F.3d at 776.
[30] *Id*.
[31] *Id*.
[32] *Id*.

unconstitutional, the good faith exception would apply.[33] On February 3, 2009, Judge Thomas W. Philips convicted Melvin Skinner, following guilty verdicts by a jury, on all three counts.[34]

Following his conviction, Skinner appealed to the Sixth Circuit.[35] On August 14, 2012, the Sixth Circuit issued its decision in *Skinner*, and reaffirmed the long-standing line of decisions upholding that there is no reasonable expectation of privacy when using cellular technology.[36] However, the three-judge panel deciding *Skinner* was split in their reasoning; two judges found no expectation of privacy and one judge found a reasonable expectation of privacy.[37]

*B. Sixth Circuit Holding*

On appeal of his conviction to the United States Court of Appeals for the Sixth Circuit, the question presented was whether Skinner had a reasonable expectation of privacy in the inherent location data broadcasted from his cell phone.[38] The three-judge panel for Sixth Circuit held (3-0) "Skinner did not have a reasonable expectation of privacy in the GPS data and location of his cell phone.[39]

However, what is notable about this case is the concurring opinion by Judge Bernice Donald.[40] Judge Donald concurred in the judgment only, and she did not concur with the majority's reasoning.[41] Specifically, Donald objected to Part II.A of the decision, and concluded, under *Katz*,[42] that there is a reasonable expectation of privacy that society is prepared to

---

[33] *Skinner*, 690 F.3d at 777.
[34] *See* Verdict form, United States v. Skinner, No. 3:07-CR-89 (E.D. Tenn. Feb. 3, 2009), WL 1682818.
[35] *Id*.
[36] *Id*.
[37] *Id*.
[38] *See* Brief of Petitioner-Appellant at x, United States v. Skinner, No. 09-6497 (6th Cir. Sept. 7, 2010), 2010 WL 7355232 ("[t]he question of suppression of location evidence obtained from a cellular telephone in the Defendant's possession presents novel questions of law to this Court.").
[39] *Skinner*, 690 F.3d at 777.
[40] *Id*. at 784.
[41] *Id*.
[42] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

recognize as legitimate.[43] She delineated "between contraband and other property,"[44] noting that the legitimate expectation of privacy is in the legally owned and legally possessed cell phone, not in the marijuana Skinner was trafficking.[45] Accordingly Donald holds, similarly to *Bailey*, "surveillance of non-contraband personal property… constitutes a search or seizure within the meaning of the fourth amendment,"[46] to include cell phones.

The standard for applying whether there is a right to privacy is articulated in *Katz* by Justice Harlan, in his famous concurring opinion that became the relevant test for determining the reasonableness of a defendant's privacy.[47] As such, in her concurring opinion in *Skinner*, Judge Donald focuses on part two of the *Katz* test: "that the [defendant's] expectation [of privacy] be one that society is prepared to recognize as 'reasonable.'"[48] At issue for Judge Donald was the majority's implication that Skinner's criminal conduct is the basis for declaring the expectation of privacy as illegitimate, and thus not one society is ready to acknowledge as reasonable.[49] She addresses this aspect of the majority's rationale by reminding the court their responsibility is to not question the whether there is "a legitimate expectation of privacy in the GPS data emitted from a cell phone used to effectuate drug trafficking," but rather "whether society is prepared to recognize a legitimate expectation of privacy in the GPS data emitted from any cell phone."[50] Disagreeing with the majorities reasoning, and finding a legitimate

[43] *Skinner*, 690 F.3d at 784.
[44] *Id*. at 785 (Donald, J. concurring).
[45] *See* United States v. Bailey, 628 F.2d 938, 944 (6th Cir. 1980) ("But there is a clear line of demarcation between, on the one hand, contraband and other items, such as stolen goods, whose possession is illegal, and on the other, goods, whatever their suspected use, whose possession is legal. The narcotics peddler in whose heroin a beeper is planted has no privacy interest in the substance; but the same is not so of legally-possessed substances into which a beeper is placed, even if these are destined later to be used in the commission of a crime.").
[46] *Id*. ("Beeper surveillance of non-contraband personal property in private areas trenches upon legitimate expectations of privacy and constitutes a search or seizure within the meaning of the amendment.").
[47] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[48] *Id*. at 361.
[49] *Skinner*, 690 F.3d at 786.
[50] *Id*.

expectation of privacy that is reasonable to society, Judge Donald affirmed the conviction by applying the Good Faith Exception.[51]

## III. LEGISLATIVE INVOLVEMENT TO LIMIT CELL PHONE TRACKING POWERS OF POLICE

Articulating the second reasonableness prong of the *Katz* standard, several legislative bodies have manifested their concerns about cell phone tracking by introducing various bills to limit the powers of law enforcement to conduct warrantless surveillance of cell phones.[52] Until recently, attempts to control law enforcement's use of cell phone tracking technology through manipulation of the inherent design of cellular technology had gone largely unregulated, and unnoticed by society, since 1986.[53] However, this tread appears to be coming to an end. The California state legislature repeatedly has passed legislation specifically to limit law enforcement's powers and require probable cause to obtain cell phone location data.[54] Furthermore, United States Congressmen have made recent attempts to draw a line in the sand, introducing the Geolocation Privacy and Surveillance Act ("GPS Act"), requiring a search warrant and probable cause to obtain any cell phone tracking data, rather than a subpoena, which requires the lower standard of reasonable suspicion.[55]

### *A. State Legislative and Law Enforcement Agency Attempts at Protecting Privacy*

Whether it is the California legislature or the increasing number of law enforcement agencies across the country, the concerns regarding geolocation data have brought the debate

---

[51] *Id*. at 786-87 (*citing* United States v. Leon, 468 U.S. 906 (1984)).
[52] *See* discussion *infra* Part III.A-B.
[53] *See generally*, Electronic Communications Act of 1986 (ECPA).
[54] Michelle Maltais, *California bill would block cellphone tracking without warrant*, LOS ANGELES TIMES (April 11, 2012), http://articles.latimes.com/2012/apr/11/business/la-fi-tn-cellphone-tracking-warrantless-search-20120411.
[55] *See*, *Geolocation Privacy and Surveillance (GPS Act)*, RON WYDEN: SENATOR FOR OREGON, http://www.wyden.senate.gov/priorities/gps-act (last visited April 23, 2013); *supra* Maltais, note 54; Somini Sengupta, *Courts Divided Over Searches of Cellphones*, THE NEW YORK TIMES (Nov. 25, 2012), http://www.nytimes.com/2012/11/26/technology/legality-of-warrantless-cellphone-searches-goes-to-courts-and-legislatures.html?pagewanted=all&_r=1&.

over privacy to the local levels.[56] Geolocation is the process or technique of tracking a person or device through the Internet or mobile device, such as a cell phone.[57] Given the various levels of privacy protection by law enforcement across the United States, with regard to a person's geolocation data, these differences may be the indications showing society's growing acceptance to recognize a privacy interest in one's physical location as legitimate and reasonable. Additionally with state legislatures, like California's legislature, sending repeatedly geolocation-limiting legislation to Governor may also demonstrate a similar recognition of society's interest in protecting geolocation information.[58] Taken together, these acts could easily infer a manifestation of society's reasonable expectation of privacy in one's cell phone emissions and geolocation data.

Following the California legislative's most recent attempt to regulate the powers of law enforcement to track an individual's cell phone, other state legislatures have tackled the issue. In March 2013, Texas legislators introduced a bill,[59] similar to California's, requiring law enforcement to obtain a search warrant prior to tracking a suspect's cell phone "if there is probable cause to believe the records disclosing location information will provide evidence in a

[56] Allie Bohm, *New Results From Our Nationwide Cell Phone Tracking Records Request*, AMERICAN CIVIL LIBERTIES UNION (Sept. 10, 2012), http://www.aclu.org/blog/technology-and-liberty-national-security/new-results-our-nationwide-cell-phone-tracking-records (Law enforcement agencies in California, Nevada, North Carolina, Wisconsin, Hawaii, Kansas, Kentucky, and New Jersey have adopted policies of requiring probable cause and search warrants to obtain geolocation data.).

[57] *Geolocation*, OXFORD DICTIONARIES, http://oxforddictionaries.com/us/definition/american_english/geolocation (last visited April 23, 2012).

[58] Hanni Fakhoury, *Governor Brown Vetoes California Electronic Privacy Protection. Again.*, ELECTRONIC FRONTIER FOUNDATION (October 1, 2012), https://www.eff.org/deeplinks/2012/10/governor-browns-vetoes-california-electronic-privacy-protection-again; Declan McCullagh, *Wireless providers side with cops over users on location privacy: The trade association representing AT&T, Verizon, and Sprint opposes a California proposal for search warrants to track mobile devices, claiming it will cause "confusion."*, CNET (April 23, 2012), http://news.cnet.com/8301-31921_3-57418662-281/wireless-providers-side-with-cops-over-users-on-location-privacy/.

[59] Derek Mead, *A Texas Bill Would Bar Warrantless Collection of Cell Phone Location Data*, VICE, http://motherboard.vice.com/blog/a-texas-cell-phone-bill-would-bar-warrantless-location-data (last visited April 23, 2013).

criminal investigation."[60] Likewise, Maine legislators also introduced a bill requiring probable cause except in exceptional circumstances.[61]

In contrast, at least two states have debated enacting an opposite position concerning the tracking of individuals through their cell phones.[62] West Virginia recently passed legislation to compel cellular providers to assist law enforcement to track a person's cell phone in emergency situations in which death or serious bodily harm are at stake.[63] However, the West Virginia statute does not extend tracking to routine police investigations.[64] The Maryland legislature is considering a move backward as well. Currently Maryland applies the standard of probable cause, and is considering lowering its standard for cell phone tracking, allowing law enforcement to obtain tracking data without a search warrant, such as the standard for reasonable suspicion.[65]

From California, to Texas, to Maine, and points in between, political arms of state governments appear to be addressing the right of privacy and anonymity in one's location. As a result of the efforts of representatives of the states, the people in a growing number of states appear ready to recognize the reasonableness of location privacy.

*B. Geolocational Privacy and Surveillance ("GPS") Act & Other Congressional Legislation*

Introduced by Senator Ron Wyden and Representative Jason Chaffetz, the GPS Act is the first of several, high-profile attempts by Congress to strengthen privacy laws.[66] The intent of the

---

[60] H.B. 1608, 83rd Leg., 1st Sess., at 7 (Tex. 2013); S.B. 786, 83rd Leg., 1st Sess., at 6 (Tex. 2013).
[61] Josh Peterson, *Maine would prohibit law enforcement from tracking cell phones without warrant*, THE DAILY CALLER (April 8, 2013), http://dailycaller.com/2013/04/08/maine-bill-would-prohibit-law-enforcement-from-tracking-cell-phones-without-warrant/; *See also Dial 415 for cellphone privacy*, BANGOR DAILY NEWS (April 7, 2013), http://bangordailynews.com/2013/04/07/opinion/dial-415-for-cellphone-privacy/.
[62] *Infra Legislature passes cellphone-tracking bill*, note 63; *infra Maryland bill would allow cell phone tracking without warrant,* note 65.
[63] *Legislature passes cellphone-tracking bill*, ASSOCIATED PRESS, April 12, 2013, http://www.wvgazette.com/News/politics/201304120176.
[64] *Id*.
[65] *Maryland bill would allow cell phone tracking without warrant*, ASSOCIATED PRESS, Feb. 6, 2013, http://www.foxnews.com/politics/2013/02/06/cell-phone-tracking-bill-raises-privacy-concerns/.
[66] Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (1st Sess. 2011) [hereinafter GPS Act], *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr2168ih/pdf/BILLS-112hr2168ih.pdf, *see also*

legislation is to limit the scope and proscribe the manner by which law enforcement goes about obtaining location data of cell phones, smart phones, computers, navigation devices, or any other mobile device that is subject to manipulation by third parties to disclose geolocation data. Generally, the GPS Act makes any act or attempted act to disclose or use geolocation data unlawful.[67] As one of may exceptions to this proposed rule, law enforcement may seek a search warrant.[68] Specifically, §2602(h)(2) authorizes the exception pursuant to the Federal Rules of Criminal Procedure, or state warrant procedures.[69]

What the GPS Act potentially demonstrates (at the federal level), is that society is increasingly recognizing, nationally, that the privacy laws currently in force are not ones that have kept up with the technology, especially the technology explosion that continues in mobile telecommunication and computing. While opponents to the GPS Act will argue that the support introducing the bill is that of only two Congressmen, the ranks of cosponsors grew to twenty-eight other Congressmen and Congresswomen since the Act's introduction.[70] As a result, the GPS Act has growing support.

Even though the current status of the bill appears to have died in committee the GPS Act recently saw life breathed back into it briefly by Congresswoman Representative Zoe Lofgren (D-Ca.) of California, as the "ECPA 2.0 Act of 2012."[71] In 2011 and 2012, senators and representatives of Congress, from both political parties, introduced a number of similar bills to

---

Geolocational Privacy and Surveillance Act, S.B. 1212, 112th Cong. (1st Sess. 2011) [hereinafter GPS Act], *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112s1212is/pdf/BILLS-112s1212is.pdf.
[67] GPS Act §2168, §2602(a).
[68] GPS Act §2602(b)-(i), §2604(a).
[69] GPS Act §2602(h)(2).
[70] *See* GPS Act, H.R. 2168, 112th Cong. (1st Sess. 2011), S.B. 1212, 112th Cong. (1st Sess. 2011).
[71] ECPA 2.0 Act of 2012, H.R. 6529, 112th Cong. (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr6529ih/pdf/BILLS-112hr6529ih.pdf.

limit the scope and authority of law enforcement to subpoena geolocation data.[72] In March 2013, Representative Lofgren again introduced another bill, virtually identical to the GPS Act.[73] Near-simultaneously, Senator Patrick Leahy (D-Vt.) also introduced the Electronic Communications Privacy Act Amendments Act of 2013.[74] As these two bills work themselves through their respective committees, there does not appear to be anything to suggest these new legislative attempts to regulate warrantless searches of geolocation data will subside.

*C. Society's Preparedness to Recognition of Privacy*

The repeated attempts of the California legislature, and Congress, are showing a willingness by American society to demonstrate that the right to privacy to one's location is maturing into a legitimate right that society is willing to recognize as reasonable. In the context of Judge Donald's concurrence in *Skinner*, cell phones are not contraband, but legal devices anyone may own.[75] Consequently, the expectation of privacy is not *per se* unreasonable, as it is in something classified as contraband, such as marijuana, as Donald suggests.[76]

The GPS Act is further evidence of Congress taking action to recognize the importance of privacy in technology. Although attempts at the federal level have not been successful either, the mere fact that it is on the radar of senators and representatives is strong evidence of society's manifestation that virtually all data contained in or emitted from a cell phone is private.

---

[72] *See* Electronic Communications Privacy Act Amendments Act of 2011, S.B. 1011, 112th Cong. (2011); *See* Location Privacy Protection Act of 2012, S.B. 1223, 112th Cong. (2012); *See* Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011); *See* Do Not Track Me Online Act, H.R. 654, 112th Cong. (2012); *See* Electronic Communications Privacy Act Modernization Act of 2012, H.R. 6339, 112th Cong. (2012); *See* Personal Data Protection and Breach Accountability Act of 2011, S.B. 1535, 112th Cong. (2011).

[73] Online Communications and Geolocation Protection Act, H.R. 983, 113th Cong. (2013), *available at* http://lofgren.house.gov/images/stories/pdf/online%20communications%20and%20geolocation%20protection%20act%20-%20lofgren%20-%20030413.pdf.

[74] Press Release, Sen. Patrick Leahy, Leahy, Lee Introduce Legislation To Update Electronic Communications Privacy Act (Mar. 19, 2013), *available at* http://www.leahy.senate.gov/press/leahy-lee-introduce-legislation-to-update-electronic-communications-privacy-act.

[75] United States v. Skinner, 690 F.3d 772, 785 (6th Cir. 2012) (Donald, J., concurring) ("…there is a clear distinction between contraband and other property.").

[76] Timothy MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. MEM. L. REV. 299 (2010), 302-304.

Recently, the United States Attorney General's office has begun to recognize this increasing interest in cell phone privacy.[77] In a Freedom Of Information Act ("FOIA") request from the American Civil Liberties Union ("ACLU"), e-mail discussions have surfaced requiring law enforcement to become more forthcoming with how law enforcement intends to use a subpoena request and how law enforcement intends to obtain the information.[78] From the emails contained in the FOIA, the ACLU filed an amicus brief in *United States v. Rigmaiden* outlining the need to readdress how law enforcement explains its need and use of subpoenas for tracking individuals.[79] Together, taken as a whole, these actions by law enforcement, Congress, and state legislatures show a broad manifestation of the expectation of privacy in one's location and the geolocation data that is emitted from cellular devices.

*D. Legislative Versus Court Solution*

In his concurring opinion, Justice Alito wrote in *United States v. Jones*, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.[80] 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."[81]

---

[77] Linda Lye, *DOJ Emails Show Feds Were Less Than "Explicit" With Judges On Cell Phone Tracking Tool*, AMERICAN CIVIL LIBERTIES UNION (Mar. 27, 2013) http://www.aclu.org/blog/national-security-technology-and-liberty/doj-emails-show-feds-were-less-explicit-judges-cell.

[78] Brief for Defendant Amici Curiae In Support of Daniel Rigmaiden's Motion To Suppress, U.S. v. Rigmaiden, 2012 WL 7767586 (D.Ariz.); Linda Lye, *Fighting for Transparency*, AMERICAN CIVIL LIBERTIES UNION OF NORTHERN CALIFORNIA (July 31, 2012), https://www.aclunc.org/issues/government_surveillance/fighting_for_transparency.shtml; Jennifer Valentino-Devries, *'Stingray' Phone Tracker Fuels Constitutional Clash*, WALL STREET JOURNAL (Sept. 22, 2011), http://online.wsj.com/article/SB10001424053111904194604576583112723197574.html.

[79] Brief for Defendant, U.S. v. Rigmaiden, No. 2:08-cr-00814-DGC, 2012 WL 7767586; *See also* E-mail from Kyle Waldinger (USACAN), U.S. v. Rigmaiden, No. 2:08-cr-00814-DGC (D. Ariz. May 23, 2011), Doc. 985-1; *See "Pen Registers" and "Trap and Trace Devices:" Less Powerful Than a Wiretap But With Much Weaker Privacy Safeguards*, SURVEILLANCE SELF-DEFENSE, https://ssd.eff.org/wire/govt/pen-registers (last visited April 27, 2013) (explaining how pen registers and trap-and-trace devices operate).

[80] See, *e.g.,* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L.REV., 801, 805–06 (2004) ("The "reasonable expectation of privacy" test governs Fourth Amendment law, and it is up to the courts to determine when an expectation of privacy is "reasonable." As a result, the courts must update and redefine the Fourth Amendment as technology evolves, creating and recreating reasonable rules that effectively regulate law enforcement and protect privacy in new technologies. The historical

Although the majority holding in *Jones* rested on the physical intrusion by law enforcement, Justice Alito's opinion leaves much to the imagination when considering the non-physical intrusions and monitoring of individuals as they travel on and off public streets. Joining with Alito were three other justices: Justices Ginsberg, Breyer, and Kagan.[82] Interestingly, Justice Scalia, while disagreeing with respect to technology and nontrespassory surveillance techniques, agreed with Alito "…that, at the very least, "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[83]

According to Justice Alito, he would prefer legislative action to address the issue of when nontrespassory surveillance becomes a search.[84] The trend following the *Jones* decision in January 2012 appears to indicate a move to address his framing of the issue.[85] However, it is too early to tell if the momentum gain will result in new laws protecting geolocation data of an individual's cell phone or other cellular devices. Given more time, the political branches of the federal government may have an answer to his question.

## IV. LAW ENFORCEMENT USE OF SUBPOENAS AND TRACKING TECHNOLOGY

### *A. Service Provider Subpoenas*

In 2012, data complied by Massachusetts Congressman Edward Markey showed a disturbing trend by law enforcement by which police have increased dramatically the number of

---

premise suggests that the courts should play an active role in the regulation of new technologies because they have done so successfully in the past.").

[81] United States v. Jones, 132 S.Ct. 945, 964 (2012) (Alito, J. concurring in the judgment) (The Court held physical 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).

[82] *Id*. at 957.

[83] *Id*. at 955.

[84] *Id.* at 964 (Alito, J. concurring in the judgment).

[85] *See* discussion, *supra* Part III.C.

"requests" for cell phone data.[86] The report showed in 2011 that law enforcement issued a staggering 1.3 million requests for information to cell phone service providers, representing a twelve to sixteen percent increase by some carrier estimates over previous years.[87] The shear number of requests show the logistical concerns to ensure (1) that law enforcement is following proper procedures, and (2) that the cellular service providers can process the requests while ensuring the requests are legitimate. When analyzing this information, several concerns come to mind that courts should weigh in their attempts to evaluate the privacy concerns.

First, is the ability of service providers to comply with the information requests in a responsible manner. The shear number suggests that this is a monumental task for service providers, requiring the staffing of entire departments to accommodate law enforcement subpoenas and informal requests. As a result, service providers like T-Mobile and Verizon have instituted pricing policies for complying with the information requests.[88]

Second, the aspect of providers charging for the information given to law enforcement presents opportunity for profitmaking at the expense of a subscriber's privacy, without meaningful choice for the subscriber to opt-out or object to the policy, given the underlying reason for the need to charge: the shear number of law enforcement requests. For the sake of efficiency, this would conclude that any request, subpoena or not, receives the same treatment, regardless of whether the request is a valid lawful use of law enforcement's power.

---

[86] Brenda Sasso, *Police made 'startling' 1.3 million requests in 2011 for cellphone data*, THE HILL (July 9, 2012), http://thehill.com/blogs/hillicon-valley/technology/236683-startling-rise-in-police-requests-for-cellphone-data.
[87] *Id*.
[88] Andy Greenberg, *These Are the Prices AT&T, Verizon and Sprint Charge For Cellphone Wiretaps*, FORBES (April 3, 2012), http://www.forbes.com/sites/andygreenberg/2012/04/03/these-are-the-prices-att-verizon-and-sprint-charge-for-cellphone-wiretaps/.

In 2009, Sprint surpassed eight million requests, in just over a year's time, for geolocation information by law enforcement.[89] To handle the large volume of requests from law enforcement, in 2009 Sprint began employing roughly 110 employees, including approximately 48 employees and contractors in the "electronic surveillance" group and approximately 65-70 employees and contractors on the "subpoena compliance side."[90] This staff is necessary in addition to a website portal Sprint created exclusively for law enforcement so Sprint could keep up with the demands by law enforcement agencies.[91] What is potentially disturbing is, if law enforcement has unfettered access via a web portal to geolocation data, who is left to ensure law enforcement is not abusing its power, when there is arguable no judicial oversight to how, when, or what information law enforcement is obtaining through the Sprint portal?

Third, the scope of each individual request could tend to create for efficiency reasons the disclosure of information not sought by law enforcement, potentially creating a policy of overbreadth.[92] Though the issue of using geolocation data is not based on a statute, per se, the overarching aspect of the practice has the effect of creating a policy that could encompass law abiding, legal possession of a cell phone and confusing it with the use of cell phones during a

---

[89] Soghoian, Christopher, *8 Million Reasons for Real Surveillance Oversight*, SLIGHT PARANOIA BLOG (Dec. 1, 2009), http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html ("[M]y major concern is the volume of requests. We have a lot of things that are automated but that's just scratching the surface. One of the things, like with our GPS tool. We turned it on the web interface for law enforcement about one year ago last month, and we just passed 8 million requests. So there is no way on earth my team could have handled 8 million requests from law enforcement, just for GPS alone. So the tool has just really caught on fire with law enforcement. They also love that it is extremely inexpensive to operate and easy, so, just the sheer volume of requests they anticipate us automating other features, and I just don't know how we'll handle the millions and millions of requests that are going to come in. -- Paul Taylor, Electronic Surveillance Manager, Sprint Nextel.").

[90] *Id*. ("In the electronic surveillance group at Sprint, I have 3 supervisors. 30 ES techs, and 15 contractors. On the subpoena compliance side, which is anything historical, stored content, stored records, is about 35 employees, maybe 4-5 supervisors, and 30 contractors. There's like 110 all together." -- Paul Taylor, Electronic Surveillance Manager, Sprint Nextel, describing the number of employees working full time to comply with requests for customer records.").

[91] United States v. Pineda-Moreno, 617 F.3d 1120 (9th Cir. 2010) ("The volume of requests grew so large that the 110-member electronic surveillance team couldn't keep up, so Sprint automated the process by developing a web interface that gives agents direct access to users' location data.").

[92] *See generally*, *Overbreadth Doctrine*, 122 HARV. L. REV. 385, 391 (2008).

criminal act. If law enforcement has not determined the target of its investigation by person or by vehicle, how does one know the tracked activity is illegal? The answer is law enforcement cannot with other surveillance acts. As a result, the safeguards expressed and implied by the Fourth Amendment must be protected when it comes to the manipulation of a person's cell phone to transmit geolocation data. Thus, law enforcement must seek out the necessary probable cause to secure a search warrant, unless a valid exception[93] exists because of the potential for abuse by law enforcement and third-party service providers is extremely high.

*B. Stingray Cell phone Tracking Technology*

'Stingray' technology is a type of commercial device used to mimic a cell tower and spoof cell phones into connecting with the device.[94] The Stingray broadcasts an omni-directional signal, 'pinging,' nearby cell phones and causing the phones to connect to the device and measures the signal to determine distance and direction.[95] With two or three of these stingray devices strategically deployed by police, officers can triangulate quickly the position of a particular cell phone, and by proxy its owner, in much the same way GPS works.[96] This pinging and tracking can occur without the knowledge or consent of the owner or user, and at anytime

[93] *See* Warden v. Hayden (exigent circumstances). *See* Chimel v. California, 395 U.S. 752; United States v. Robinson, 414 U.S. 218 (1973); New York v. Belton, 453 U.S. 454 (1981); Arizona v. Gant, 556 U.S. 332 (2009); Whren v. United States, 517 U.S. 806 (1996) (search incident to arrest). *See* Chambers v. Maroney, 399 U.S. 42 (1970); California v. Carney, 471 U.S. 386 (1985); South Dakota v. Opperman, 428 U.S. 364 (1976); United States v. Chadwick, 433 U.S. 1 (1977); California v. Acevedo, 500 U.S. 565 (1991) (automobiles and containers). *See* Horton v. California, 496 U.S. 128 (1990); Arizona v. Hicks, 480 U.S. 321 (1987), (plain view and plain touch doctrines). *See* Schneckloth v. Bustamonte, 412 U.S. 218 (1973); Georgia v. Randolph, 547 U.S. 103 (2006); Illinois v. Rodriguez, 497 U.S. 177 (1990) (consent). *See* Terry v. Ohio, 392 U.S. 1 (1968) ("stop and frisk"). *See generally* Joshua Dressler and George Thomas, CRIMINAL PROCEDURE: PRINCIPLES, POLICIES AND PERSPECTIVES, 2th ed., chapter 4 2003 (West).

[94] Hanni Fakhoury and Trevor Timm, *Stingrays: The Biggest Technological Threat to Cell Phone Privacy You Don't Know About*, ELECTRONIC FRONTIER FOUNDATION (Oct. 22, 2012), https://www.eff.org/deeplinks/2012/10/stingrays-biggest-unknown-technological-threat-cell-phone-privacy; *See* Jennifer Valentino-DeVries, *How 'Stingray' Devices Work*, WALL STREET JOURNAL BLOG (Sept. 21, 2011); http://blogs.wsj.com/digits/2011/09/21/how-stingray-devices-work/; *See* Valentino-DeVries, *supra* note 78.

[95] Farkhoury and Timm, *supra* note 94; Valentino-DeVries, *supra* note 94; Valentino-DeVries, *supra* note 78.

[96] Jeremy Jankowski, *GPS in the IFR System: A Guide from the Ground Up*, AVIATION PUBLISHING GROUP (July 7, 2002), http://www.avweb.com/news/system/183179-1.html (last visited April 27, 2013); *see also How Does GPS Works?*, SMITHSONIAN NATIONAL AIR AND SPACE MUSEUM, http://airandspace.si.edu/gps/work.html (last visited April 27, 2013).

the cell phone is on.[97] Through the manipulation of the inherent properties of cellular technology, law enforcement can spoof any cellular device to transmit its location without the knowledge or consent of the owner, nor must the phone be in use at the time of the geolocation disclosure. Consequently, society has a valid concern in protecting its right of privacy by regulating how law enforcement uses Stingray technology.

What makes stingray technology troublesome is who may obtain one of these devices. Presently, only law enforcement agency may purchase these devices.[98] As a result, this potentially invokes similarities of technology found in *Kyllo*.[99] The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.[100] Consequently, '*effects*' like cell phones and can reasonably be inferred to be secure from unreasonable searches, such as surveillance that does not fit within the traditional scope of the meaning of the word as it once did in 1967 when *Katz* was decided. Back then the Court held in *Katz* "the fourth amendment protects people, not places. What a person knowingly exposes to the public… is not subject to the Fourth Amendment"[101] Thus, if the design of stingray technology is to mimic a cell phone tower, and purposefully tricks a person's cell phone or cellular device to transmit data without his or her knowledge or consent invokes the very same premise found by the Court in *Katz*.

In the Supreme Court case *United States v. Knotts*, the Court held the tracking of chemicals used in the production of methamphetamine via a beeper placed inside one of the five-gallon containers was constitutional.[102] Furthermore, the Court held that visual surveillance from

[97] Farkhoury and Timm, *supra* note 94; Valentino-DeVries, *supra* note 94; Valentino-DeVries, *supra* note 78.
[98] Farkhoury and Timm, *supra* note 94; Valentino-DeVries, *supra* note 94; Valentino-DeVries, *supra* note 78.
[99] Kyllo v. United States, 533 U.S. 27 (2001).
[100] U.S. CONST amend. IV.
[101] Katz v. United States, 389 U.S. 347, 351 (1967).
[102] United States v. Knotts, 460 U.S. 276 (1983).

a public place may be augmented through the use the police officers' sensory faculties in the tracking of the defendant.[103] The issue to note in *Knotts* is that law enforcement established prior visual surveillance of the chemicals prior to tracking them electronically.[104] The use of technology became a tool of surveillance, akin to a flashlight or binoculars, thus it was constitutional.[105] In his concurring opinion, Justice Stevens wrote "[a]lthough the augmentation in this case was unobjectionable, it by no means follows that the use of electronic detection techniques does not implicate especially sensitive concerns."[106] Fast-forward to 2007 and the case *United States v. Garcia*, when the Seventh Circuit held the installing of a GPS tracking device on a defendant's car, while parked in a public area, did not amount to a violation of the Fourth Amendment.[107] The court's rationale was that there is no practical difference in following a vehicle with a police car or with the aid of cameras, or a GPS transmitter.[108] However, important here, is that police visually acquired the subject vehicle before remotely surviellling it and its occupants.[109] Furthermore, the device providing the geolocation data was the property of law enforcement.[110] When it concerns tracking an individual's location via cell phone pinging, the geolocation data is coming from the individual's property, not any attached government-owned device. As a result, the possessor of the cell phone has a property and a privacy interest in the geolocation data omitted from the device.

*C. Compliance under the Communications Assistance for Law Enforcement Act of 1994*

[103] *Id*.
[104] *Id*.
[105] *Id*.
[106] *Id*. at 287.
[107] United States v. Garcia, 474 F.3d 994 (7th Cir. 2007).
[108] *Id*.
[109] *Id*.
[110] *Id*.

In negotiations with the FBI, the Telecommunications Industry Association (TIA) adopted the "J-Standard,"[111] in accordance with the Communications Assistance for Law Enforcement Act of 1994 ("CALEA").[112] Under CALEA, cellular providers receive safe harbor by virtue of compliance with the statute,[113] and the resulting automated forwarding of cell phone records to law enforcement in near real time, "pursuant to a court order or other lawful authorization."[114] However, service providers must also ensure that these records are protected in a manner that ensures "the privacy and security of communications and call-identifying information not authorized to be intercepted."[115] As a result of the implementation of the J-Standard, subscribers have no other abilities to switch carriers, or otherwise object to the required law enforcement tracking provisions of the law, short of discontinuing their cell phone service. While there is a provision to require safeguards of personal information collected, the extent of the privacy is not completely certain because of the unknown meaning of "call-identifying information."[116] Does this information extend to where a person places or may place a call, or where a person receives or may receive a call? From the extensive use of subpoenas by law enforcement, and the courts' granting of the subpoenas, the answer to the question appears to

[111] Brief for Electronic Privacy Information Center as Amici Curiae Urging Affirmance, *In re*: Applications of The United States of America For Historical Cell-Site Data (No. 11-20884), 2012 WL 1029812, at 21 (5th Cir. 2012).
[112] *Id*. at 20.
[113] *Id*. at 21.
[114] *Id*. at 22.
[115] *Id*.
[116] *CALEA FAQ*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/pages/calea-faq (last visited April 27, 2013) ("In the circuit-switched world of traditional telephony, the meaning of "call-identifying information" ("CII") was clear: telephone numbers are CII, and the conversations are content. But in the packet-mode world of the Internet, communications are encapsulated as described above, and each protocol layer is associated with different "signaling information." Whether a component is "signaling information" or "content" depends on which layer is reading it. As the NPRM recognizes, it may not be easy to isolate call-identifying information without examining packet content. Thus CII on the Internet is not a clearly defined concept as it is in the traditional telephony environment.").

be no.[117] However, as discussed earlier, recent acts of the court suggest a change away from the trend of the past. Thereby, the establishment of privacy for geolocation data, either by legislative means or by establishment of new court precedent will provide desperately needed guidance for law enforcement and society.

## V. SURVEYS OF PUBLIC OPINION OF THE EXPECTATION OF PRIVACY

The amount of privacy has become a consistently bothersome area for people throughout America.[118] In 2006, an ABC News/Washington Post poll indicated thirty percent of Americans believed the federal government has intruded unjustly into their personal privacy.[119] Furthermore, society's trust of government to protect privacy continues to wane, especially for law enforcement agencies like the Department of Justice, Office of the Attorney General, Department of Homeland Security, Customs and Border Protection, and Citizenship and Immigration Services.[120] These poll trends continue also into the commercial landscape, especially when concerning privacy and cell phones.[121] According to these polls, more than half of all cell phone users who use mobile apps have reported that the level of privacy maintained by

---

[117] Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, THE NEW YORK TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.

[118] *Public Opinion on Privacy*, EPIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/survey/ ("Public opinion polls consistently find strong support among Americans for privacy rights in law to protect their personal information from government and commercial entities.").

[119] Gary Langer, *Poll: Broader Concern on Privacy Rights, But Terrorism Threat Still Trumps*, ABC News (Jan. 10, 2006), http://abcnews.go.com/Politics/story?id=1490715#.UXHIoyvF3rY; *See also Broader Concern on Privacy Rights, But Terrorism Threat Still Trumps*, ABC NEWS/WASHINGTON POST (Jan. 8, 2006), http://abcnews.go.com/images/Politics/1003a3WiretapsandPrivacy.pdf. The statistics indicates an increase of almost 100% in just a few years, rising from seventeen percent in 2003 to thirty percent in 2006.

[120] *2010 Privacy Trust Study of the United States Government*, PONEMON INSTITUTE (June 30, 2010), at 3, http://www.privacylives.com/wp-content/uploads/2010/07/ponemon-2010-privacy-trust-study-of-us-govt-06302010.pdf.

[121] Bob Sullivan, *Poll: Cellphone users dump apps to save privacy, lose phones anyway*, NBC NEWS BLOG (Sept. 5, 2012), http://redtape.nbcnews.com/_news/2012/09/05/13664261-poll-cellphone-users-dump-apps-to-save-privacy-lose-their-phones-anyway?lite ("Slightly more than half (54 percent) of cell phone consumers who use mobile apps have decided not to install an app after realizing how much personal information they'd have to share; and nearly one-third (30 percent) of that group has uninstalled an app for privacy reasons"); *See also Survey: cellphone users concerned about privacy in apps*, ASSOCIATED PRESS, Sept. 5, 2012, http://usatoday30.usatoday.com/tech/products/story/2012-09-05/mobile-app-privacy/57599260/1.

the app developer affected their use of the apps. While specific poll and survey results are not available regarding the specifics of geolocation surveillance by law enforcement, what is available shows American society appear increasingly less willing to forego its privacy interests in sharing cell phone data. So, based on these surveys, a person can likely infer nonconsensual surveillance by law enforcement of an individual's geolocation data from his or her cell phone as unreasonable without a search warrant.

## VI. LIKELIHOOD OF SCOTUS[122] GRANTING CERTIORARI

The *United States v. Jones* the Court gives ample reasons for privacy advocates to pause and to look beyond the narrow holding of the Court with regard to cell phone tracking.[123] Although the Court voted 9-0 in favor of Jones, the dissection of the vote is crucial to understanding the Court's thoughts to nontrespassory surveillance and the search warrant requirement of the Fourth Amendment.[124] After dissection, the *Jones* holding demonstrates a 4-1-4 decision for privacy advocates.[125]

### *A. Alito's Opinion in Jones Applied to the Issue in Skinner*

Rather than analyzing the issue in *Jones* from a trespassory view, Justice Alito would answer the question by asking, "whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[126] However, answering this question requires modernizing America's privacy laws. The one aspect of the majority opinion by Justice Scalia that Justice Alito can agree with is "that we must 'assur[e]

[122] "SCOTUS" is an abbreviation for Supreme Court of the United States.
[123] United States v. Jones, 132 S.Ct. 945 (2012).
[124] *Id*. at 954 (Justice Soytomayor's concurring opinion).
[125] *Id*. The majority opinion by Justice Scalia, in which Chief Justice Roberts and Justices Kennedy, Thomas, and Sotomayor joined, addressed solely the narrow holding of the physical trespass by law enforcement; while Justice Alito's opinion, in which Justices Ginsberg, Breyer, and Kagan joined, contemplated the nontresspassory aspect. Justice Soytomayor's concurring opinion suggests both Scalia's and Alito's opinions are valid, however she joined with Scalia to maintain a narrow holding. This section will further discuss in greater detail Sotomayor's opinion and why *Skinner* appears to be the case the Court is waiting for to settle this split holding in *Jones*.
[126] *Id*. at 958 (Alito, concurring in the judgment).

preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[127] Justice Alito opines current search and seizure application remained based on the preservation of privacy based on the language of eighteenth century.[128] His analysis leads to the following revelation:

> Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users—and as of June 2011, it has been reported, there were more than 322 million wireless devices in use in the United States. For older phones, the accuracy of the location information depends on the density of the tower network, but new "smart phones," which are equipped with a GPS device, permit more precise tracking. For example, when a user activates the GPS on such a phone, a provider is able to monitor the phone's location and speed of movement and can then report back real-time traffic conditions after combining ("crowdsourcing") the speed of all such phones on any particular road. Similarly, phone-location-tracking services are offered as "social" tools, allowing consumers to find (or to avoid) others who enroll in these services. The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.[129]

Because of the lack of legislative action regulating geolocation tracking for law enforcement purposes, the best the Court can do, Justice Alito suggests, is application of existing Fourth Amendment doctrine and determine whether a reasonable person would have anticipated the degree of intrusion.[130] Under his approach short-term monitoring would not offend society's reasonable expectation of privacy; however, longer term electronic monitoring would offend.[131] As such, Justice Alito's opinion can give encouragement to privacy advocates, should the Court issue a ruling for *Skinner*.

---

[127] *Id*.
[128] *Id*. ("But it is almost impossible to think of late–18th-century situations that are analogous to what took place in this case. (Is it possible to imagine a case in which a constable secreted himself somewhere in a coach and remained there for a period of time to monitor the movements of the coach's owner?" *See* n.3 ("The Court suggests that something like this might have occurred in 1791, but this would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience.").
[129] *Id*. at 963 (Alito, concurring in the judgment) (citations omitted). *See Wireless Quick Facts*, *supra* note 2; *See*, *e.g.*, *The bright side of sitting in traffic: Crowdsourcing road congestion data*, GOOGLE BLOG (August 25, 2009), http://googleblog.blogspot.com/2009/08/bright-side-of-sitting-in-traffic.html.
[130] *See Jones*, 132 S.Ct at 964.
[131] *Id*. ("For such offenses, 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.").

*B. Application of Justice Sotomayor's Opinion in Jones in Skinner.*

In Justice Sotomayor concurring opinion, she made several references to Justice Alito's opinion suggesting that she is willing to consider the nontrespassory implication of warrantless searches. First she opines her reasons for siding with the majority was to ensure the long-standing common trespassory law is not displaced or diminished and that the *Katz* reasonable-expectation-test merely augments trespassory common law.[132] However, Justice Sotomayor takes notice of Justice Alito's concern that "physical intrusion is now unnecessary in many forms of surveillance."[133] Likewise, "[i]n 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. But "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.""[134]

Before going further, it is important to review what GPS is and how it works. GPS, or Global Positioning System is a network of geosynchronized satellites in orbit around the Earth.[135] Using a GPS receiver, these satellites can triangulate a person's or an object's position.[136] By triangulating with three or more satellites a person can quickly and easily determine his or her position within only a few meters or feet, and elevation.[137] Understandably, aviation uses GPS extensively, allowing precise navigation enroute to a destination and to land in low visibility weather conditions.[138] Today, cellular manufacturers incorporate GPS technology into their cell phones offered by cellular service providers like AT&T, T-Mobile, Verizon, and Sprint. These phones further allow users to install other services and applications to increase the

[132] *See Id*. at 954-57 (Sotomayor, concurring).
[133] *Id*. at 955, *post* at 961-63.
[134] *See Jones*, at 955, *ante* at 953.
[135] Jankowski, *supra* note 96; *How Does GPS Works?*, *supra* note 96.
[136] *How Does GPS Works?*, *supra* note 96.
[137] *Id*.
[138] *Navigation In The Air*, SMITHSONIAN NATIONAL AIR AND SPACE MUSEUM, http://airandspace.si.edu/gps/airnav.html (last visited April 27, 2013); Jankowski, *supra* note 96.

functionality of the cell phone, such as turn-by-turn navigation, finding nearby gas prices, or find nearby restaurants.[139] The importance of understanding how GPS works is precisely because of Justice Sotomayor's comment, in which "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.""[140] As a result, in the situation at issue in *Skinner*, law enforcement's cellular tracking techniques are akin to that of GPS tracking. Applying Justice Sotomayor's reasoning, these actions by law enforcement in *Skinner* should be subject to the *Katz* standard.[141]

The reasonableness prong of *Katz* will require the Court to readdress privacy as it applies to today's digital age and mobility. Justice Sotomayor gave a telling insight to her belief regarding this exact issue:

> I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful

---

[139] *See generally*, *e.g.*, *Google Maps for Andriod*, GOOGLE MOBILE, http://www.google.com/mobile/maps/ (last visited April 29, 2013); *Get a GasBuddy App for your Phone!*, GASBUDDY, http://gasbuddy.com/GasBuddyMobileApps.aspx (last visited April 29, 2013); *Yelp Mobile*, YELP, http://www.yelp.com/yelpmobile (last visited April 29, 2013).

[140] United States v. Jones, 132 S.Ct. 945, 955, *ante* at 953 (2012).

[141] *Id*. at 955-56 ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. 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."). *See*, *e.g.,* People v. Weaver*,* 12 N.Y.3d 433, 441–42 (2009) ("Disclosed in [GPS] data ... 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"). The Government can store such records and efficiently mine them for information years into the future. *Pineda–Moreno,* 617 F.3d, at 1124 (opinion of Kozinski, C.J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: "limited police resources and community hostility." Illinois v. Lidster*,* 540 U.S. 419, 426 (2004). Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." United States v. Cuevas–Perez*,* 640 F.3d 272, 285 (7th Cir., 2011) (Flaum, J., concurring)."

> conventional surveillance techniques. I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent "a too permeating police surveillance.[142]

Examining Justice Sotomayor's reasoning, little is left to the imagination regarding her concerns over potential abuse by law enforcement without appropriate oversight from the legislative or judicial branches.[143] In this digital age, the lack of meaningful consent for information that is voluntarily disclosed to third parties should be sufficient grounds for reexamining the reasonable of expectation of privacy. As a result, "[the current] 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."[144] Justice Sotomayor further stated:

> I for one doubt that people would 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.[145]

Although Justice Sotomayor joined with the majority in *Jones*, her opinion is highly suggestive of her support to reexamine the process by which law enforcement currently seeks to

---

[142] *Jones*, at 956 (citations omitted), *See* Kyllo v. United States, 533 U.S. 27, 35, n.2 (2001); *ante*, *Jones* at 954 ("leaving open the possibility that duplicating traditional surveillance "through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy.""); *See* United States v. Di Re, 332 U.S. 581, 595 (1948). *See Jones*, 132 S.Ct. at n.* ("United States v. Knotts, 460 U.S. 276[] (1983), does not foreclose the conclusion that GPS monitoring, in the absence of a physical intrusion, is a Fourth Amendment search. As the majority's opinion notes, *Knotts* reserved the question whether " 'different constitutional principles may be applicable' " to invasive law enforcement practices such as GPS tracking. *See ante,* at 952, n.6 (quoting 460 U.S., at 284.").

[143] *Jones*, 132 S.Ct. at 956.

[144] *Id.* at 957.

[145] *Id*. *See* Smith v. Maryland, 442 U.S. 735, 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); *see also* Katz v. United States, 389 U.S. 347, 351-52 (1967) ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

gain geolocation data of cell phones to discover a person's location. Because of the methods employed by law enforcement and the common use of Stingray devices, the issue in *Skinner* appears to fit extremely well within the framework of Justice Sotomayor's opinion from *Jones* and can provide further guidance with regard to cellular technology and the methods of collecting geolocation data.[146]

### *C. Reasoning for the Court to Grant Certiorari for Skinner*

Assessing the reasoning of the *Jones* opinions and comparing how the judges voted to the issue in *Skinner*, it appears in all likelihood this is the very case that can put the unanswered questions in *Jones* to rest. Coupled with Justice Alito and Justices Ginsberg, Breyer, and Kagan who joined with him in *Jones*, there appears to be a strong consensus in philosophy among the four justices that Justice Sotomayor can agree with regarding nontrespassory searches and seizures. Consequently, the privacy concerns and the issue of warrantless cell phone tracking in *Skinner* seem particularly well suited for consideration by the Supreme Court, resulting in a majority of justices who could side with Skinner, recognizing a legitimate privacy interest in one's anonymity and emission from one's cellular device. [147]

## VII. CONCLUSION

In *Skinner*, law enforcement did not know the subject of their investigation, nor the vehicle used by Skinner.[148] Law enforcement never established visual surveillance to track the

[146] *Jones*, at 957 (Sotomayor, concurring) ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision. I therefore join the majority's opinion").
[147] United States v. Skinner, 690 F.3d 772 (6th Cir. 2012), *petition for cert. filed* (U.S. Dec. 26, 2012) (No. 12-7971); *see* Letter from William K. Suter, Clerk of the Court, to Clerk of the United States Court of Appeals for the Sixth Circuit, Clerk of the court, (Jan. 4, 2012), *available at* http://www.supremecourt.gov/Circuits/Docketing/Circ6_09-6497_12-7971.pdf, ("The petition for a writ of certiorari in the above entitled case was filed on December 26, 2012 and placed on the docket January 4, 2013 as No. 12-7971.").
[148] United States v. Skinner, 690 F.3d 772 (6th Cir. 2012).

movement of Skinner.[149] The only lead law enforcement had been the telephone number of the cell phone that an informant had given to Skinner.[150] Law enforcement did not observe the transferring of the telephone to Skinner.[151] The sole method of surveillance used was the obtaining of a subpoena to compel the cooperation of the telephone's service provider to provide location data on the cell phone.[152] These facts run contrary to the holdings in *Knotts*, *Garcia*, and *Kyllo*. As such, *Skinner* is distinguishable from these Fourth Amendment cases. Furthermore, advancements in technology, generally, have created an opportunity for the Court to update its line of holdings protecting an individuals privacy interests.

Black's Law Dictionary defines 'surveillance' as "[c]lose observation or listening of a person or place in the hope of gathering evidence."[153] Granted there are similar type of observation that qualifies as surveillance, through the use of technology, such as unmanned aerial vehicles (UAV) and satellite observations.[154] However, these are tools of technology merely aid an officer's vision, and thus do not provide a defendant with a legitimate expectation of privacy.[155] But how should the courts resolve this issue when there is no aiding of an officer's visual acuity? How can a court reconcile the lack of expected privacy by travelling on a public road, when the method of surveillance cannot conclusively show that the subject is on a road?

According to Joshua Engel, several state courts have acknowledge the limitations on the antiquated doctrines of *Knotts*, *Garcia*, and *Kyllo*, suggesting the Court's involvement in updating appropriate levels of electronic surveillance is relevant.[156] While Engel's discussion

---

[149] *Id*.
[150] *Id*.
[151] *Id*.
[152] *Id*.
[153] BLACK'S LAW DICTIONARY 1486 (8th ed. 2004).
[154] *See* California v. Ciraolo, 476 U.S. 207 (1986).
[155] *Id*.
[156] Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U.MEM.L.REV. 233, 248 (2010).

addresses the privacy interest in the data contained in a cell phone, similar to a personal computer, the use of stingray technology to manipulate a cell phone to transmit geolocation data using internal components is akin to searching the contents of the cell phone. Creating a doctrine that encompasses how law enforcement obtains geolocation data and whether the manipulation of cellular technology to disclose one's position when one may not wish to disclose should be reason enough for the Supreme Court to review *Skinner*. Furthermore, Congress must update the United States Code continue to protect the rights of American citizens as technology expands the abilities of ordinary persons to remain accessible while remaining private or anonymous.

Ultimately, Justice Scalia may very well have predicted the future, opining in *Jones* "[i]t may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question."[157] As a result, *Skinner* appears to be the case on the horizon for the Court to address this question, regardless if Congress acts in the matter, if only to resolve the split between the states and an increasing number of federal and state courts. In 1967, *Katz* overruled *Olmstead*; ending nearly forty years of Fourth Amendment precedent because of the advancements in telecommunications technology became an integral part of American society.[158] Similarly, *Skinner* represents a point in American society where advancements in cellular telecommunications technology have become an integral part of every day life. Perhaps it is time again for the next advancement in privacy, similar to how Katz created a new precedent for Fourth Amendment protection. Should the Court decide to continue hearing the case and hold in favor of Skinner, the result will be a clear victor for privacy advocates, thereby updating society's expectations of privacy within today's technological world. Ultimately, if the issue in

[157] United States v. Jones, 132 S.Ct. 945, 954 (2012).
[158] Katz v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438 (1928).

*Skinner* is decided in favor of privacy rights, it is likely Skinner's conviction will be affirmed because of the Good Faith Exception, as noted by Judge Donald in her concurring opinion.[159]

[159] *See* United States v. Skinner, 390 F.3d 772, 786 (6th Cir. 2012) (Donald, J. concurring) (*citing* United States v. Leon, 468 U.S. 906 (1984)).