Comments

FRANK LIN*

Siri, Can You Keep a Secret? A Balanced Approach to Fourth Amendment Principles and Location Data

* J.D. Candidate, University of Oregon School of Law, 2014; Executive Editor, Oregon Law Review, 2013-14. The positions expressed in this comment represent the author's opinions and do not reflect/represent the views of other persons or institutions. I wish to thank Professor Margie Paris for her insightful comments as faculty advisor of this Comment as well as Laura Fishman, Dustin Littrell, and Emma Pelkey for their editorial work. Further thanks go to Denna Rawie and AUSAs William "Bud" Fitzgerald, Christopher Cardani, Nathan Lichvarcik, Frank Papagni, Amy Potter, Tim Simmons, and Jeff Sweet for their mentorship and guidance. Finally, for offering her friendship, humor, and encouragement during this process, I owe deep gratitude to Katherine Eitenmiller.

> *The real danger is the gradual erosion of individual liberties through the automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.*
>
> U.S. Privacy Protection Study Commission, 1977

INTRODUCTION

The Fourth Amendment to the United States Constitution provides the right for "people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[1] Underlying this phrase are guiding principles that have deep roots reaching as far as the Roman Empire. For instance, Roman statesman Cicero stated, "[w]hat is more inviolable . . . than the house of a citizen[?] . . . This place of refuge is so sacred to all men, that to be dragged from thence is unlawful."[2]

But how do historic principles apply to modern society? The Fourth Amendment traditionally protected papers located in homes or in luggage.[3] Today, however, information is no longer constrained to

---

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

[2] NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 15 (1937).

[3] *See* Olmstead v. United States, 277 U.S. 438, 463 (1928) (recognizing the "well-known historical purpose of the Fourth Amendment" as preventing warrantless searches of a person's house, papers, and effects) *overruled by* Katz v. United States, 389 U.S. 347 (1967); *see also* Morgan Cloud, *A Liberal House Divided: How the Warren Court*

fading parchment. Information and methods of communication have transcended into a digital era, where ideas and beliefs reside in computer systems in distant locations that are maintained by third parties. Thus, it is not always clear how the Fourth Amendment applies to the information age.

Many argue that the Fourth Amendment was designed to adapt to the constantly changing conditions of life. Justice Louis D. Brandeis adopted this position in 1928 when addressing government wiretapping, saying:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home . . . . Can it be that the Constitution affords no protection against such invasions of individual security?[4]

Justice Brandeis's prediction has become a reality. Since 1928, technology has seen many changes, but most significantly for this Comment is the advent of smartphones. "Smartphones" are defined as portable devices that are capable of more than communication via voice and SMS (texting).[5] They have the capability to remotely browse the Internet, access e-mail, download third-party applications, provide turn-by-turn directions by connecting to global positioning satellites, and more.[6] Additionally, smartphones transmit "location data," information that enables service providers to determine the location of the phone, and thus, the user, with shocking precision.[7]

Law enforcement has utilized location data to efficiently investigate and prosecute crimes.[8] For instance, it once took the U.S.

Dismantled the Fourth Amendment, 3 OHIO ST. J. CRIM. L. 33, 33 (2005) (recognizing the dissolution between property law and privacy law).

4 *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

5 Daniel Zamani, *There's an Amendment for That: A Comprehensive Application of Fourth Amendment Jurisprudence to Smart Phones*, 38 HASTINGS CONST. L.Q. 169, 169–70 (2010).

6 *Id.*; Jordan Robertson, *Your Phone, Yourself: When is Tracking Too Much?*, U.S.A. TODAY (Apr. 23, 2011, 10:39 PM), http://www.usatoday.com/tech/news/2011-04-23-smartphone-tracking.htm.

7 *See In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 751 (S.D. Tex. 2005); Noam Cohen, *It's Tracking Your Every Move and You May Not Even Know*, N.Y. TIMES, Mar. 26, 2011, at A1, *available at* http://www.nytimes.com/2011/03/26/business/media/26privacy.html.

8 *See, e.g.*, Declan McCullagh, *ACLU: FBI Used 'Dragnet'-Style Warrantless Cell Tracking*, CNET NEWS (June 22, 2010, 9:37 AM), http://news.cnet.com/8301-31921_3

Marshals Service an average of forty-two days to track a fugitive.[9] It now takes the U.S. Marshals Service a mere two days to accomplish this same task.[10] Having immediate access to location data allows law enforcement to deploy available resources effectively while reducing undue risk to officers and the public.[11]

Some worry that law enforcement's use of location data can pose an objective harm, as they fear that the government will subject the public to non-stop surveillance. Judge Flaum from the Seventh Circuit noted that "[t]he constitutional ill of prolonged or mass use of GPS technology would not necessarily be based on the information acquired by the device but on the fact of the government's gaze."[12]

The legality of law enforcement's use of location data remains ambiguous in the absence of clear direction from either the judiciary or the legislature.[13] Further, the majority of the existing scholarship on the subject remains unworkably vague and hostile toward the government's use of location data to aid in the investigation and prosecution of crime.[14] This Comment proposes a standard for government access to location data that is not only practical, but also one that balances the legitimate interests of law enforcement and the privacy concerns of citizens.

-20008444-281.html ("[P]olice are tapping into the locations of mobile phones thousands of times a year . . . .").

9 *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism & Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) [hereinafter *Landau Hearing*] (statement of Dr. Susan Landau), *available at* http://judiciary.house.gov/hearings/pdf/landau02172011.pdf.

10 *Id.*

11 *See The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 5 (2011) [hereinafter *Baker Statement*] (statement of James A. Baker, Assoc. Deputy Att'y Gen., U.S. Dep't of Justice), *available at* http://www.judiciary.senate.gov/pdf/11-4-6%20Baker%20Testimony.pdf.

12 *See* United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring).

13 *See* Lyria Bennett Moses, *Recurring Dilemmas: The Law's Race to Keep Up with Technological Change*, 2007 U. ILL. J.L. TECH. & POL'Y 239, 241 (2007) (noting that the law has fallen behind technology).

14 *See generally ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 77–78 (2010) (statement of U.S. Magistrate Judge Stephen Wm. Smith, Southern District of Texas), *available at* http://judiciary.house.gov/hearings/printers/111th/111-109_57082.pdf; Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS L.J. 1309, 1312–13 (2012); Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281, 282 (2011).

Part I reviews the current state of technology and explains the various methods to obtain location data from smartphones. Part II provides an overview of Fourth Amendment doctrine as it pertains to location data. Part III discusses whether the government can utilize location data to aid in the investigation and prosecution of crimes while acting in accordance with existing Fourth Amendment rules.

Part IV considers the policy concerns of privacy advocates as well as the governmental interest in public safety. Part V proposes a new standard that features a practical application of the Fourth Amendment while balancing the concern for individual liberty with the competing governmental interest to secure public safety.

I
OVERVIEW OF TECHNOLOGY

Smartphone technology is only one development in the larger picture of technological advancements. In order to lay the groundwork to understand how technology has infused itself with American life, this section provides a broader review of modern technology. In the process, it will become clear how smartphones can potentially reveal intimate details of a citizen's life.

Paul Ohm, an associate professor who specializes in information privacy, describes four categories of technology that are responsible for shifting society into one that is more connected and less privacy-oriented.[15] First is the "one device," which is the convergence of a person's computing needs "into a single, portable, high-powered machine, equipped with an always-on, high-speed connection to the Internet, and outfitted with dozens of sensors, including multiple digital cameras . . . a microphone, a GPS chip, and a digital compass."[16] Ohm's "one device" best describes the smartphone.

There is mounting evidence that smartphones are becoming increasingly prevalent. In 2011, a Pew Internet study found that eighty-three percent of adults in the United States have a cell phone of some kind.[17] Among cell phone owners, forty-two percent own a

---

15 Ohm, *supra* note 14, at 1314.

16 *Id*.

17 Aaron Smith, *Smartphone Adoption and Usage*, PEW INTERNET & AMERICAN LIFE PROJECT 2 (July 11, 2011), http://pewinternet.org/~/media//Files/Reports/2011/PIP_Smartphones.pdf.

smartphone.[18] Thus, thirty-five percent of the American adult population uses smartphones.[19]

In addition to traditional phone calls and text messages, smartphones transmit data from third-party applications, including social media and e-mail programs. The use of data is becoming more common. Between 2007 and 2010, AT&T saw an 8000% increase in data traffic.[20] Part of the transmitted data is location data. In fact, *The Wall Street Journal* noted in 2011 that 47 of the 101 most popular smartphone applications sent location information to third parties.[21] Given the increasing prevalence of smartphone ownership, the quantity and quality of data transmitted through these devices, and the fact that these devices are constantly at their owner's side, third-party access to smartphone data has the potential to reveal intimate details about the user's life.[22]

The second technological advancement is "the cloud," which facilitates "the migration of essential computing and storage facilities from local devices owned by users to distant servers owned by providers."[23] Data sent to these distant servers is remotely accessible from any computer, phone, or portable laptop with an Internet connection.[24]

The third technological shift is the rapid development of social media, or what Ohm calls, "the social."[25] The social provides consumers with the ability to interact with a larger and more diverse network.[26] The social also gives consumers a reason to adopt

---

[18] *Id*.

[19] *Id*.

[20] Dan Meyer, *AT&T Filing Provides Interesting Industry Data*, RCR WIRELESS NEWS (Apr. 25, 2011), http://www.rcrwireless.com/article/20110425/carriers/110429949/at-t-filing-provides-interesting-industry-data.

[21] Jennifer Valentino-DeVries & Julia Angwin, *Latest Treasure is Location Data*, WALL ST. J. (May 9, 2011, 7:37 PM), http://online.wsj.com/article/SB10001424052748703730804576313522337383898.html.

[22] Zamani, *supra* note 5, at 170 (citing John Boudreau, *Your Phone, Your Life: Applications For Your iPhone, Blackberry or Other Mobile Device Are Changing How You Navigate Your World*, SAN JOSE MERCURY NEWS, Mar. 15, 2009, at 1A, *available at* 2009 WLNR 5010619 ("Because their smart-phone is with them everywhere they go, people develop far closer attachments to the devices than to their home PCs or laptops. . . Nothing is as close to us all the time—not even your spouse or partner.")).

[23] Ohm, *supra* note 14, at 1315.

[24] *Id.*

[25] *Id*. at 1316.

[26] *See* KEITH N. HAMPTON ET AL., SOCIAL ISOLATION AND NEW TECHNOLOGY: HOW THE INTERNET AND MOBILE PHONES IMPACT AMERICANS' SOCIAL NETWORKS, PEW

technical advances like the one device and the cloud by building "upon the innate desire of humans to want to connect to others."[27] The danger here is that, on social networks, "people reveal more of their thoughts and behavior, including things they might have before chosen to hide, and to more people than they ever have before."[28] It is even possible to draw conclusions from information that a user does not explicitly reveal. For example, students at MIT determined the sexual orientation of individuals on Facebook with shocking accuracy based on patterns of how they "friended" others.[29]

The final advancement is "big data." This refers to the use of data by companies to "squeeze more value from their existing data by making inferences."[30] For instance, Amazon.com prompts users to consider buying additional items based on what the user has recently purchased or searched for.[31] In this fashion, people are really no longer anonymous, as it is possible to determine one's identity by studying patterns in data.[32]

These four technologies have the collective potential to reveal a comprehensive and intimate picture of one's life. Because the one device is almost always on and often carried by the user, it provides continuous access to the cloud and the social. People relay various information about their lives on the social and perhaps store even more intimate knowledge on the cloud.[33] Big data examines the other

---

INTERNET & AMERICAN LIFE PROJECT 3–4 (Nov. 4, 2009), *available at* http://www .pewinternet.org/~/media//Files/Reports/2009/PIP_tech_and_social_isolation.pdf.

27 Ohm, *supra* note 14, at 1316.

28 *Id*.

29 *See* Carter Jernigan & Behram F.T. Mistree, *Gaydar: Facebook Friendships Expose Sexual Orientation*, 14 FIRST MONDAY 10 (Oct. 5, 2009), *available at* http://journals.uic .edu/ojs/index.php/fm/article/view/2611/2302. *But see* Nadia Wynter, *'Gaydar' Project at MIT Attempts to Predict Sexuality Based on Facebook Profiles*, N.Y. DAILY NEWS (Sept. 22, 2009, 1:17 PM), http://www.nydailynews .com/life-style/gaydar-project-mit-attempts-predict-sexuality-based-facebook-profiles-article-1.404453 (questioning the validity of the MIT study).

30 Ohm, *supra* note 14, at 1316.

31 Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 249 (2013).

32 *Id*.

33 *See* M. James Daley, *Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure & Data Privacy*, 12 SEDONA CONF. J. 121, 123 (2011) (discussing social networking applications and their access to location data).

three technologies to produce data and paint a complete portrait of an individual's life.[34]

Taken together, these technologies arguably indicate the shift in cultural values of privacy and interconnectedness.[35] This does not necessarily mean that privacy has no value in light of new technology.[36] Indeed, as Professor Daniel Solove posits, if the focus is solely on the general public's current expectation of privacy, "our conception of privacy would continually shrink given the increasing surveillance in the modern world."[37] While technology has facilitated the communication of intimate details to a much broader network of both personal contacts as well as service providers, this does not mean that there is no value in remaining free from undue government intrusion.[38]

Central to this Comment is an analysis of how the government should access location data in light of new and increasingly prevalent technology. "Location data" refers to information that reveals the geographical position of a technological device and its user. It implicates all four technological advances. The one device generates location data, which in turn is often conveyed through functions of the social and the cloud. This information is potentially analyzed by big data to decipher patterns in human behavior.[39]

---

[34] *See also* United States v. Jones, 132 S. Ct. 945, 955–56 (Sotomayor, J., concurring) ("The Government can store [location data] and efficiently mine them for information years into the future.").

[35] *See The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 4 (2011) [hereinafter *Kerry Hearings*] (testimony of Cameron F. Kerry, Gen. Counsel, U.S. Dept. of Commerce) (discussing social importance and economic value of recent digital communications, including location data in the formation of relation and political advocacy), *available at* http://www.judiciary.senate.gov/pdf/11-4-6%20Kerry%20Testimony.pdf.

[36] *But see* Rushin, *supra* note 14, at 327 (arguing that our socially reasonable expectation to privacy is at its weakest in light of social media).

[37] Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1142 (2002).

[38] *See* Saby Ghoshray, *Privacy Distortion Rationale for Reinterpreting the Third-Party Doctrine of the Fourth Amendment*, 13 FLA. COASTAL L. REV. 33, 82 (2011) (explaining that even with increase in social media, individuals still maintain the "right to be left alone").

[39] *See* Tene & Polonetsky, *supra* note 31, at 247 (listing ways that big data and location data can reveal patterns in food shortages, crime waves, and learning outcomes in developing country schools).

Many individuals carry electronic devices that reveal location data, primarily cell phones.[40] In fact, the Federal Communications Commission has mandated that cell phone manufacturers make a minimum of ninety-five percent of their phones traceable.[41] Recent data suggests that the government has utilized this function. For instance, in 2008, Sprint gathered the real-time location of its cell phone subscribers over eight million times at the request of law enforcement.[42] To expedite the process, Sprint launched a self-service website where law enforcement could monitor the movements of any cell phone subscriber.[43]

There are two ways that smartphones emit location data. First, many phones calculate extremely accurate location data using a GPS satellite receiver that is built directly into the cellular device.[44] Typically, the user must activate this function and consent to this information being collected.[45] Smartphones with GPS capability will often have software that coaxes users into revealing their location to third-party services.[46] Many users choose to share their real-time or historical location information online for social networking purposes.[47] Other users convey location data for nonsocial purposes. For example, Google Maps taps into smartphones that are currently using its turn-by-turn GPS directions feature and subsequently collects the phones' current location and speed.[48] Google then uses

---

40 *See* Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614, 632 (2011).

41 43 C.F.R. § 20.18(g); *see also* Laura E. Gomez-Martin, *Smartphone Usage and the Need for Consumer Privacy Laws*, 12 U. PITT. J. TECH. L. & POL'Y 1, 9 (2012).

42 Alex Kozinski, *Symposium Keynote: The Dead Past*, 64 STAN. L. REV. ONLINE 117, 119 (2012).

43 *Id*.

44 *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, & Civil Liberties of the H. Comm. on the Judiciary*, 112th Cong. 5 (2010) [hereinafter *Blaze Testimony*] (testimony of Professor Matt Blaze), *available at* http://www.privacywonk.net/download/blaze-judiciary-20100624.pdf.

45 *Id*.

46 *See* Robertson, *supra* note 6; *see also* Scott Thurm & Yukari Iwatani Kane, *Your Apps Are Watching You*, WALL ST. J. (Dec. 17, 2010, 10:01 PM), http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html.

47 *See* Janice Y. Tsai et al., *Location-Sharing Technologies: Privacy Risks and Controls*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 119, 120–23 (2010) (reviewing various social media applications that share location data).

48 *See* Tim Simonite, *Android's Rise Helps Google Grow Its Traffic Surveillance System*, MIT TECH. REV. (Aug. 7, 2012), http://www.technologyreview.com/news/428732/androids-rise-helps-google-grow-its-traffic-surveillance-system/.

this information to update real-time traffic information.[49] This transaction benefits the user by providing some type of service, which in this case, is detailed information on the quickest route to a given destination.

The second method occurs through "network-based" location data. Similar to the first method, network-based location data provides information regarding a phone's location but is less precise than GPS.[50] Cell phones typically send out signals, called "pings," to nearby cell towers in order to find the nearest tower with the greatest signal strength.[51] This happens passively, meaning that it occurs without any action by the user.[52]

Cell towers are maintained by service providers and are generally spread across geographic areas, providing voice and data services to phones. Service providers are constantly recording the approximate geographic area where a cell phone is located by determining which cell tower the phone is using.[53] This data is used to gauge which cell towers experience the heaviest call volume and thus help service providers determine where to install new towers.

While network-based data tends to be less precise than GPS, there are several methods to increase the accuracy of the location data. For instance, through a method called "triangulation," service providers can locate a phone by measuring the relative angles and length of time that a ping from a mobile device takes to reach multiple cell towers.[54] This data is generally only available prospectively, usually because the user has dialed 911 or because a law enforcement agency has asked a carrier to collect the data.[55]

The prevalence of cell phones and their ability to provide access to intimate details of an individual's life pose murky waters for law

---

[49] *Id*.

[50] Courtney E. Walsh, *Surveillance Technology and the Loss of Something a Lot Like Privacy: An Examination of the "Mosaic Theory" and the Limits of the Fourth Amendment*, 24 ST. THOMAS L. REV. 169, 239 (2012).

[51] William Curtiss, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistence Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139, 144 (2011).

[52] Walsh, *supra* note 50, at 239.

[53] *Blaze Testimony*, *supra* note 44, at 7.

[54] Kevin McLaughlin, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426–27 (2007).

[55] Stephanie K. Pell & Christopher Soghoian, *Can You See Me Now?: Toward Reasonable Standards for Law Enforcement Access to Location Data That Congress Could Enact*, 27 BERKELEY TECH. L.J. 117, 131 (2012).

enforcement and privacy activists. The next section will provide an overview of existing principles and case law that may shed light on how courts may decide crucial privacy questions in the future.

II
OVERVIEW OF LAW

A. Underlying Principles of the Fourth Amendment

The history of the Fourth Amendment reveals that the Framers of the Constitution were not necessarily concerned with privacy.[56] In fact, "privacy" did not enter the vocabulary of the search and seizure analysis until the late 1800s, about one hundred years after the Fourth Amendment was adopted.[57] Over time, privacy became a court-recognized aspect of Fourth Amendment law, although not an aspect that is textually mandated by the Fourth Amendment.[58] In this context, privacy acts more as a proxy for what the Framers were truly concerned about: the relationship between a government and its people.

While drafting the Fourth Amendment, fresh in the Framers' minds was the relationship between the people and the crown, an affair that was marked by insecurity and imbalanced power.[59] It is well documented that the Fourth Amendment was intended to enhance individual liberty through the restraint of government power.[60] Take, for instance, the general warrant, which authorized an official of the crown to apprehend anyone they suspected of a crime or to search any place they suspected might contain evidence of a crime. The Framers considered the use of general warrants intolerable.[61] They took

---

[56] *See* James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 668 (1985) (arguing that the Framers were not concerned about "mere secrecy" as much as they were constrained search and seizure).

[57] *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195–96 (1890).

[58] Walsh, *supra* note 50, at 175.

[59] *See* Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 296–97 (1993).

[60] Morgan Cloud, *The Fourth Amendment During the* Lochner *Era: Privacy, Property, and Liberty in Constitutional Theory*, 48 STAN. L. REV. 555, 618–19 (1996); *see also* Cloud, *supra* note 59, at 295 ("The [F]ourth [A]mendment exists for the very purpose of enhancing individual liberty by constraining government power.").

[61] *See* STEPHEN J. SCHULHOFER, MORE ESSENTIAL THAN EVER: THE FOURTH AMENDMENT IN THE TWENTY-FIRST CENTURY 29 (2012).

particular offense to having the crown's menial servants violate the privacy of the home.[62] It was against this backdrop that the Framers drafted the Fourth Amendment. Professor Stephen Schulhofer noted three points that were emphasized in the eighteenth-century period: judicial authorization, specificity, and the control of executive discretion.[63]

For a warrant to be valid, it must be authorized by a judicial officer.[64] The Framers further believed that narrowly and specifically drawn warrants were a "vital means of protection."[65] Finally, the Framers were concerned with curtailing the discretion of the official executing the search warrant.[66] Chief Judge Hale explained that one of the prime evils of the general warrant is the fact that it "makes the party [executing it] to be in effect the judge."[67] Judge Blackstone shared similar sentiments, explaining that "a *general* warrant . . . is illegal and void for its uncertainty . . . ; for it . . . ought not be left to the officer, to judge of the grounds of suspicion."[68]

Thus, the warrant process became a mechanism for assuring the King's subjects that royal powers were being exercised under judicial oversight and within the bounds of the law. But this was just part of a larger movement by the Framers to promote a relationship with the government that safeguarded the peoples' right to be secure.[69] The aim of the Fourth Amendment is, as Professor Schulhofer describes, the "preservation of a vibrant society that respects the freedom and autonomy of each individual."[70]

The Framers could not have possibly predicted the sweeping technological changes to come, such as the advent of the Internet or global positioning systems. Nor could they have envisioned the modern-day organized system of law enforcement, a far cry from the

---

62 *Id*.

63 *Id*. at 23.

64 *Id*. at 31.

65 *Id*. at 33 (citing Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 619–68 (1999)).

66 *Id.* at 34.

67 *Id*. at 35 (citing 2 SIR MATTHEW HALE, HISTORY OF THE PLEAS OF THE CROWN 150 (P.R. Glazebrook gen. ed., London Professional Books Ltd. 1971) (1736)).

68 *Id*. at 36 n.25 (citing 4 WILLIAM BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 288 (facsimile ed., Univ. of Chicago Press 1979) (1769)).

69 *Id.* at 39.

70 *Id*. at 142.

eighteenth-century constable.[71] Surely, the Framers intended the Constitution to be an assertion of fundamental values rather than an outdated treatise of criminal procedure.

As times change, courts are faced with the challenge of applying eighteenth-century principles to twenty-first-century problems. In order to preserve the foundational standards envisioned by the Framers, courts must understand the distinction between eighteenth-century rules and eighteenth-century principles. In Justice Brandeis's words:

> [T]ime works changes . . . and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping . . . . The makers of our Constitution . . . knew that only a part of the pain, pleasure and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotion and their sensations. They conferred, as against the government, the right to be let alone.[72]

In order to effectuate Justice Brandeis's vision, policy makers must respect the intentions of the Framers to create a relationship between a government and its people that safeguards personal development and civic engagement.

B. Electronic Communications Privacy Act

Congress has remained silent on law enforcement's ability to obtain location data. In fact, the one major piece of legislation impacting digital communications, the Electronic Communications Privacy Act (ECPA), was enacted in 1986 and is hopelessly outdated.[73] Even though the ECPA is the primary statute governing law enforcement access to wire, oral, and electronic communications, it does not provide guidance on how law enforcement should use location data and does not even contain the word "location." Four

---

[71] The recent phenomenon of militarizing local law enforcement, such as the procurement of armored personnel carriers, helicopters, Humvees, and even military-grade weapons, would be unknown to the Framers. *See* Radley Balko, *Rise of the Warrior Cop: How Did America's Police Become A Military Force on the Streets?*, 99 JULY. A.B.A. J. 44, 46 (2013).

[72] Olmstead v. United States, 277 U.S. 438, 473, 476, 478 (1928) (Brandeis, J., dissenting).

[73] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

bills that address the problem of undue intrusion of location data were recently introduced, but these bills all failed to pass.[74]

The Department of Justice has interpreted the ECPA to allow the collection of location data from cell phones through several methods, including through court orders.[75] However, the statute does not specify a standard by which the government must meet to obtain a court order.[76]

The lack of clear direction from the legislature has resulted in inconsistent standards at the district court level. Some courts apply a heightened standard, requiring law enforcement officials to provide probable cause to obtain prospective, real-time location data to track suspects in criminal investigations.[77] Some courts exercise a lower standard, requiring only a showing of specific and articulable facts.[78]

C. Case Law

Few commentators are particularly fond of Fourth Amendment case law.[79] Over time, the Court has eroded Fourth Amendment protections as it pertains to electronic communications. This section begins by explaining how the Court arrived at the reasonable expectation of privacy test. It then discusses two of the most widely criticized doctrines in Fourth Amendment case law: the plain view

---

74 Geolocation Privacy and Surveillance Act of 2011, S. 1212, 112th Cong. § 2 (2011); Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. § 5 (2011); Location Privacy Protection Act of 2011, S. 1223, 112th Cong. (2011); Commercial Privacy Bill of Rights Act of 2011, S. 799, 112th Cong. (2011).

75 *The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. § 5, at 8 (2011) [hereinafter *Baker Testimony*] (testimony of James A. Baker, Assoc. Deputy Att'y Gen., U.S. Dep't of Justice), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg70856/pdf/CHRG-112shrg70856.pdf.

76 *Id*.

77 *See, e.g.*, *In re* Application of the U.S. for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 134, 135 (D.D.C. 2006); *In re* Application of the U.S. for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [sealed] and [sealed], 416 F. Supp. 2d 390, 391 (D. Md. 2006).

78 *See, e.g.*, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 315–19 (3d. Cir. 2010); *In re* Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device & Cell Site Location Authority on a Certain Cellular Telephone, 415 F. Supp. 2d 663, 666 (S.D. W. Va. 2006).

79 *See, e.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480 (2011) (commenting on search and seizure law as a "theoretical embarrassment").

doctrine and the third party doctrine. It concludes by discussing the significance of two recent cases that impacted the landscape of government access to location data.

1. Reasonable Expectation of Privacy Test

Olmstead v. United States kicked off the modern Fourth Amendment line of cases.[80] In *Olmstead*, the defendants were convicted of violating Prohibition by conspiring to import, possess, and sell alcohol.[81] Federal agents wiretapped the defendant's phone lines from outside the house.[82] Because there was no physical trespass, that is, no "actual physical invasion" of the defendant's property, the Supreme Court held that there was no Fourth Amendment violation.[83] According to Chief Justice William Howard Taft, the Fourth Amendment only extended protection to "material things."[84]

Justice Brandeis responded with his famous dissent, acknowledging that as time, society, and technology changes, so too must Fourth Amendment doctrine. He believed in a broader application of the Fourth Amendment, where "every unjustifiable intrusion by the government upon the privacy of the individual, *whatever the means employed*, must be deemed a violation of the Fourth Amendment."[85]

Decades later, the court adopted Justice Brandeis's approach and overturned *Olmstead* in the landmark case *Katz v. United States*.[86] In *Katz*, federal agents planted an electronic listening device against the outside of a phone booth, in which the defendant subsequently placed an incriminating phone call.[87] At no point did the agents physically enter the booth.[88] However, the Court recognized that Fourth Amendment protection did not "turn upon the presence or absence of a physical intrusion," and the fact that the agents did not penetrate the

---

80 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

81 *Id*. at 455.

82 *Id*. at 456–57.

83 *Id*. at 466.

84 *Id*. at 464.

85 *Id*. at 478–79 (Brandeis, J., dissenting) (emphasis added).

86 389 U.S. 347, 353 (1967).

87 *Id*. at 348.

88 *Id*.

walls of the booth had no constitutional significance.[89] Using what became one of the most cited phrases in Fourth Amendment case law and scholarship, Justice Stewart wrote, "the Fourth Amendment protects people, not places."[90]

Concurring Justice Harlan's "reasonable expectation of privacy" test later became the prevailing test for Fourth Amendment search and seizure.[91] The test has two prongs. First, the defendant must have a subjective expectation of privacy.[92] Second, that expectation must be an objective one that society is prepared to recognize as reasonable.[93]

Katz ushered in a new era of Fourth Amendment doctrine. Prior to *Katz*, the Court's analysis turned on the existence of a trespass upon a constitutionally protected area. Subsequently, the Court abandoned the requirement of a physical trespass and focused instead on the protection of persons—not property. Some have posited that the Court abandoned the trespass requirement due to social developments.[94] That is, changes in everyday life, such as the indispensable function of public telephones in private communications, made the surveillance in *Katz* unconstitutional.[95] Despite this, the Court has weakened Fourth Amendment protections over time, especially through the plain view and third party doctrines.

2. Plain View Doctrine

Under *Katz*, the basic premise of the plain view doctrine is that a person does not have a reasonable expectation of privacy to anything that he knowingly exposes to the public.[96] The Supreme Court has applied this doctrine to location data in two key cases, known as the Beeper Cases.

The first Beeper Case is *United States v. Knotts*.[97] There, with the consent of a chemical company, police placed a beeper in a five-gallon drum of chloroform that was subsequently purchased by the defendant.[98] Using both visual surveillance and the signal emitted

---

89 *Id.* at 353.

90 *Id.* at 351.

91 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 740 (1979).

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

93 *Id.*

94 SCHULHOFER, *supra* note 61, at 119.

95 *Id.*

96 *Katz*, 389 U.S. at 351.

97 460 U.S. 276 (1983).

98 *Id.* at 278.

from the beeper, law enforcement tracked the defendant's movements on public roads to an illicit drug lab.[99] The Supreme Court held that this type of surveillance did not violate the Fourth Amendment because the government's conduct amounted to following a vehicle on public roads and a person has no reasonable expectation of privacy in public movements from one place to another.[100]

Conversely, in *United States v. Karo*, the Supreme Court concluded that the government's use of a beeper to obtain location data was unconstitutional because the beeper revealed information about the interior of the home.[101] Unlike *Knotts*, the information gathered here could not be obtained by tracking the defendant's movements on public roads and was not otherwise available to the public. Thus, the interior of the home fell within the protection afforded by the Fourth Amendment.

In the Beeper Cases, the Court reaffirmed the plain view doctrine in the context of location data and government surveillance. However, the Court's approach does not make clear whether there is a limit to governmental surveillance of citizens, even on public thoroughfares. Rather, the Court specifically left the unanswered question of whether law enforcement can perform twenty-four hour surveillance of any citizen without judicial knowledge or supervision.[102]

3. Third-Party Doctrine

Under the third-party doctrine, the Fourth Amendment does not protect information that an individual reveals to a third party, even if the information was revealed on the assumption that the confidence placed in the third party will not be betrayed.[103] In the words of the Ninth Circuit's Chief Judge Alex Kozinski, "[n]ot everything an individual wishes to keep private is legally protected as such."[104]

Courts have applied the third-party doctrine to information regarding transactions made through financial institutions,[105] numbers dialed on phones,[106] and even a list of every person an accused has

---

99 *Id.* at 278–79.

100 *Id.* at 281.

101 468 U.S. 705, 715 (1984).

102 *Knotts*, 460 U.S. at 283–84.

103 United States v. Miller, 425 U.S. 435, 443 (1976).

104 Kozinski, *supra* note 42, at 119.

105 *Id.*

106 *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743 (1979).

emailed.[107] Consistent in the reasoning is a distinction between the content of the communication and the information that was "voluntarily" conveyed to service providers, the latter being information that is presumably void of any actual expectation of privacy. For instance, while the contents of a telephone conversation are not revealed to the phone company, all "telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[108]

The slow erosions of Fourth Amendment protections by the third-party doctrine make it impossible to protect informational privacy in the modern world. According to the Court, the above forms of information are not truly private because citizens voluntarily choose to expose such information, thereby assuming the risk that it may become exposed to law enforcement.[109] Yet, under such logic, *Katz* should have come out differently. There, Katz chose to place a call from a public location. Thus, Katz assumed the risk that federal agents could listen in on the conversation.

The Court in *Katz* held that the warrantless surveillance violated the Fourth Amendment because of the recognition that public telephones became an indispensible function of everyday life. Thus, even though the surveillance did not involve physical trespass, it still violated Katz's reasonable expectation of privacy because to say otherwise would be to "ignore the vital role that the public telephone has come to play in private communication."[110]

The Court has not determined how the plain view doctrine and the third-party doctrine applies to location data emitted from smartphones. However, in 2012, the Court handed down an opinion in *United States v. Jones* that fundamentally altered the landscape of electronic surveillance and provided a glimpse into how various members of the Court may rule in the future.[111]

---

107 *See, e.g.*, United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008).

108 *Smith*, 422 U.S. at 742.

109 *See, e.g.*, United States v. Miller, 425 U.S. 435, 443 (1976) ("The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government.").

110 Katz v. United States, 389 U.S. 347, 352 (1967).

111 132 S. Ct. 945 (2012).

4. The Jones *Decision*

In *United States v. Jones*, federal agents placed a GPS tracker to the bottom of a vehicle belonging to the defendant's wife.[112] Over a period of twenty-eight days, the government monitored the vehicle's movements using the GPS tracker.[113] A unanimous Court held that the secret placement of the GPS tracker on the vehicle violated the Fourth Amendment, but came to this conclusion on varying grounds.[114]

Writing for the majority, Justice Scalia grounded his opinion on the narrowest grounds possible, focusing on the physical intrusion of a protected area for the purpose of obtaining information.[115] Basing his decision on the physical trespass that occurred, Justice Scalia wrote that "the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[116] By attaching the GPS tracker to the vehicle, the officers encroached on a protected area, thus violating the defendant's Fourth Amendment protections.[117]

Justice Scalia relied upon an originalist reading of the Fourth Amendment, acknowledging the "18th-century guarantee against unreasonable searches, which we believe must provide *at a minimum* the degree of protection it afforded when it was adopted."[118] This reading of the Constitution boils down to the notion that a search violates the Fourth Amendment if it involves a physical trespass onto the defendant's property. Yet, this appears to be the logic that was overruled in *Olmstead*. Justice Scalia reconciles this discrepancy by recognizing that *Katz* did not replace the trespass test but rather augmented it.[119] He does acknowledge that government tracking through electronic means without actual physical trespass may be "an unconstitutional invasion of privacy," but he explicitly refused to address this issue.[120]

---

112 *Id.* at 948.

113 *Id.*

114 *Id.* at 949.

115 *Id.* at 950.

116 *Id.*

117 *Id.* at 952.

118 *Id.* at 953.

119 *Id.* at 950.

120 *Id.* at 954 ("[T]he present case does not require us to answer that question. . . . We may have to grapple with these 'vexing problems' in some future case where a classic

Justice Scalia's emphasis on trespass is troubling given the strong body of Supreme Court decisions that examine trespass in the context of the Fourth Amendment. For example, in *Oliver v. United States*, the Court held that the search of an open field did not violate the Fourth Amendment, even though law enforcement committed a trespass upon the defendant's property.[121] There, the Court reasoned that "even a property interest in premises may not be sufficient to establish a legitimate expectation of privacy with respect to particular items located on the premises or activity conducted thereon."[122] Thus, the rule placed forth in *Jones* seems contrary to existing case law and creates greater ambiguity as to how the Fourth Amendment applies to government surveillance through location data when conduct does not involve trespass.[123]

In her concurring opinion, Justice Sotomayor agreed that *Katz* was meant to augment the trespass test, not replace it.[124] But she recognized that the trespass doctrine ultimately provides little guidance on cases where electronic or other novel modes of surveillance are successfully implemented without physical invasion of property.[125]

Importantly, Justice Sotomayor acknowledged that long-term monitoring of location interferes with a citizen's expectations of privacy.[126] Location data reveals details about one's "familial, political, professional, religious, and sexual associations."[127] Awareness of government surveillance in this regard "chills associational and expressive freedoms. . . . The net result is that GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[128]

---

trespassory search is not involved and resort must be had to *Katz* analysis; but there is no reason for rushing forward to resolve them here.").

121 466 U.S. 170, 183 (1984).

122 *Id*.

123 Hon. Kevin Emas & Tamara Pallas, United States v. Jones*: Does* Katz *Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116, 149 (2012).

124 *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

125 *Id*.

126 *Id*.

127 *Id*.

128 *Id*. at 956 (citing United States v. Cuevas Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

In this context, Justice Sotomayor questions the third-party doctrine.[129] She notes that the all-or-nothing approach of the third-party doctrine 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."[130] She briefly reasserts a "degrees of privacy" approach, first made by Justice Thurgood Marshall in a decades-old dissent from *Smith v. Maryland*.[131] The principle is that people maintain varying degrees of privacy in voluntarily disclosed information to third parties, and in our age, we cannot avoid disclosing information to certain sources such as banks or phone companies.[132] This approach has support in *Katz*, where it was understood that "what [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[133]

Justice Alito's concurrence criticizes the majority's narrow trespass approach: "The Court's reasoning largely disregards what is really important (the *use* of a GPS for the purpose of long-term tracking) and instead attaches great significance to something that most would view as relatively minor (attaching to the bottom of a car a small, light object that does not interfere in any way with the car's operation)."[134] The majority thus leaves unanswered a solution to the "vexing problems" where surveillance can be carried out through electronic means that do not involve physical contact.[135]

Justice Alito would institute *Katz* as the exclusive test for whether a Fourth Amendment search has occurred.[136] He modifies the *Katz* test to address non-physical, electronic surveillance, concluding that police conduct is a search when it "involve[s] a degree of intrusion

---

129 *Id*. at 957 ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

130 *Id*.

131 *Id.*

132 *Id*. (citing Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting) ("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.")).

133 *Id*. (alteration in original) (quoting Katz v. United States, 389 U.S. 347, 351–52 (1967)).

134 *Id*. at 961 (Alito, J., concurring).

135 *Id*. at 962.

136 *Id*. at 959–60.

that a reasonable person would not have anticipated" in that "particular case."[137]

One factor that Justice Alito uses to assess the "degree of intrusion" is the length of the surveillance.[138] He notes that four-week long tracking certainly violates society's reasonable expectation of privacy while short-term tracking does not.[139] This is because an individual does not necessarily have a reasonable expectation of privacy in a single trip made on public thoroughfares. But that individual may find it unreasonable to be followed over the course of a long period of time, even if the surveillance took place on public roads. Unfortunately, Justice Alito fails to explain at what point the line would be crossed, and even recognizes that long-term tracking may be reasonable if the crime is severe enough.[140]

Even with its recognized ambiguities, Justice Alito's four-vote approach may become the majority, as Justice Sotomayor has given weight to his approach in her own concurrence.[141] What is noteworthy about Justice Alito's concurrence is that it shifts the question from what society allows an individual to demand and asks what a reasonable person would anticipate that the police would do.[142]

Many commentators have criticized the Court for failing to determine the legality of invasive, long-term invasions of privacy created by government surveillance.[143] Many have also hypothesized about the effect of the *Jones* decision on GPS tracking.[144] Further, the

---

137 *Id*. at 964.

138 *Id*.

139 *Id*.

140 *Id*. The majority also criticizes Justice Alito on this point, noting that:

> [I]t remains unexplained why a 4-week investigation is 'surely' too long and why a drug-trafficking conspiracy involving substantial amounts of cash and narcotics is not an "extraordinary offens[e]" which may permit longer observation. What of a 2-day monitoring of a suspected purveyor of stolen electronics? Or of a 6-month monitoring of a suspected terrorist?

Id. at 954 (citation omitted).

141 *Id*. at 955 (Sotomayor, J., concurring).

142 *Id*. at 964 (Alito, J., concurring).

143 *See* Dahlia Lithwick, *Alito vs. Scalia*, SLATE (Jan. 23, 2012, 6:38 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2012/01/u_s_v_jones_supreme_court_justices_alito_and_scalia_brawl_over_technology_and_privacy_.html (noting that Justice Sotomayor "seems best to understand that [intrusive government surveillance] is the real problem the court [sic] should be focused on, even though she refuses to address it today").

144 *See, e.g.*, Lauren Millcarek, *Eighteenth Century Law, Twenty-First Century Problems:* Jones, *GPS Tracking, and the Future of Privacy*, 64 FLA. L. REV. 1101, 1110

decision has left many law enforcement agencies grappling with the aftermath of *Jones*.[145] The next section explores *United States v. Skinner*, a recent Sixth Circuit case that looks at electronic surveillance through cell phones in light of the *Jones* decision.

5. United States v. Skinner*: A Recent Approach to Location Data Surveillance*

In May 2006, the Drug Enforcement Administration (DEA) obtained a court order authorizing agents to "ping" a cell phone carried by Melvin Skinner, a suspect in an ongoing investigation.[146] Agents tracked Skinner's location via his cell phone as he traveled across state lines, eventually locating him at a truck stop where he was found with over 1100 pounds of marijuana.[147]

In denying Skinner's motion to suppress, the Sixth Circuit held that the DEA agents did not require probable cause to ping Skinner's cell phone and obtain his precise location because there was not a reasonable expectation of privacy in data given off by Skinner's cell phone.[148] At the very outset, the court declared that "[w]hen criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when police take advantage of the inherent characteristics of those very devices to catch them."[149]

The court focused particularly on two aspects: the voluntary procurement of the cell phone by Skinner and the use of public thoroughfares.[150] The Fourth Amendment was not violated because there could not be a reasonable expectation of privacy in data sent

---

(2012) ("Under *Jones*, the police can still install trackers into your electronics before you come into possession of them and track you theoretically *ad infinitum*, without consequences.").

145 *See, e.g.*, Tom Goldstein, *Why* Jones *Is Still Less of a Pro-Privacy Decision Than Most Thought (Conclusion Slightly Revised Jan. 31)*, SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/?p=138066; Carrie Johnson, *FBI Still Struggling with Supreme Court's GPS Ruling*, NPR, Mar. 21, 2012, http://www.npr.org/2012/03/21/149011887/fbi-still-struggling-with-supreme-courts-gps-ruling; Lior J. Strahilevitz, *Can the Police Keep up with* Jones*?*, CHI. TRIB. (Jan. 27, 2012), http://articles.chicagotribune.com/2012-01-27/opinion/ct-perspec-0127-privacy-20120127_1_facial-recognition-gps-device-cameras (describing possibly constitutionally suspect police technologies).

146 United States v. Skinner, 690 F.3d 772, 775 (6th Cir. 2012).

147 *Id*. at 774.

148 *Id*. at 775.

149 *Id*. at 774.

150 *Id*. at 781.

from a *voluntarily* procured cell phone.[151] Further, the court determined that there was no inherent constitutional difference between physically trailing a defendant and tracking via voluntarily procured technology.[152] This analysis places emphasis on what the defendant is disclosing to the public rather than what is known by the police.[153] As a public policy matter, this approach allows law enforcement tactics to evolve with technological advancements and promotes more efficient means of discovering a suspect's movements.[154]

The majority, citing Justice Alito's concurrence in *Jones*, noted that prolonged comprehensive tracking might be unreasonable under the Fourth Amendment.[155] However, because the relatively short-term monitoring here (three days) did not come close to the tracking in *Jones* (twenty-eight days), the court declined to elaborate on this standard.[156]

In applying the two-pronged *Katz* analysis, the dissent notes that society is prepared to recognize a legitimate expectation of privacy in location data given off by cell phones.[157] Influenced by the prevalence of cell phones in everyday life, the dissent recognizes that phones are "not contraband and . . . possession of the phone [is] not illegal."[158] Just because a phone is used in a crime doesn't mean there is "no expectation of privacy in the data emitted from the phone."[159]

Skinner poses several challenges to both law enforcement and privacy activists. First, while the Sixth Circuit recognizes that overly comprehensive tracking of location data emitted from cell phones may violate the Fourth Amendment, it leaves unanswered questions regarding what level of surveillance constitutes overly comprehensive tracking. Further, the Sixth Circuit emphasized that the monitoring took place while Skinner was on public thoroughfares and relied upon the rationale of the beeper cases. However, unlike vehicles, cell phones are actually taken within protected spaces, such as the

---

151 *Id*. at 777.
152 *Id*. at 778.
153 *Id*. at 779.
154 *Id*. at 778.
155 *Id*. at 780.
156 *Id*.
157 *Id*. at 786 (Donald, J., dissenting).
158 *Id.* at 785.
159 *Id*.

home.[160] It is unclear how law enforcement will distinguish when an individual is on public roadways as opposed to protected spaces.[161] Additionally, cell phone monitoring provides much more comprehensive information than placing a tracking device on a vehicle.[162]

The Sixth Circuit also relied on the fact that Skinner voluntarily procured his phone, and thus voluntarily conveyed his location. However, several courts have questioned the premise that consumers are voluntarily conveying information by simply using their phones.[163]

Taken to the extreme, if a citizen wants to avoid government surveillance of location through cell phones, the option left by the Sixth Circuit is to withdraw from the use of cell phones completely. This could not have been the price that the Framers expected us to pay for retaining any claim of privacy. The Fourth Amendment was established to define the type of relationship a government should have with its people in order to promote civic life, not to stifle it.

In summary, despite the existence of a large body of law regarding government surveillance of citizens, a review of the case law reveals several ambiguities. First, the Court has created tension between the trespass doctrine and the reasonable expectation of privacy test, even though *Katz* arguably rejected the trespass doctrine in the context of Fourth Amendment searches.[164]

Second, the Court did not address whether law enforcement can conduct twenty-four hour surveillance of any citizen without judicial oversight. *Jones* missed an opportunity to provide clarity in this realm and failed to recognize the various ways that long-term tracking could be instituted without the use of trespass. The following section will

---

160 *See* Brian Davis, *Prying Eyes: How Government Access to Third-Party Tracking Data May be Impacted by* United States v. Jones, 46 NEW ENG. L. REV. 843, 865–66 (2012) (noting how cell phone users' movements are highly unpredictable and can enter into constitutionally protected areas unexpectedly).

161 *See* Kyllo v. United States, 533 U.S. 27, 37 (2001) ("In the home . . . *all* details are intimate details.").

162 *See* Marc McAllister, *The Fourth Amendment and New Technologies: The Misapplication of Analogical Reasoning*, 36 S. ILL. U. L.J. 475, 492 (2012) (tracking movements through cell phones is more invasive than tracking one's movements during single journeys and more difficult to replicate through traditional forms of surveillance).

163 *See, e.g.*, *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317–18 (3d Cir. 2010).

164 *See, e.g.*, United States v. White, 401 U.S. 745, 748–49 (1971) (recognizing that *Katz* overruled *Olmstead*).

attempt to adress this issue in light of existing precedent as well as the concurring opinions of five justices of the Supreme Court.

III
ANALYSIS: THE CONSTITUTIONALITY OF GOVERNMENTAL ACCESS TO LOCATION DATA

Can the government utilize smartphone technology to aid in the investigation and prosecution of crime without violating constitutional guarantees of privacy? The oversimplified answer is yes. As demonstrated in *Skinner*, under the plain view doctrine, there is no reasonable expectation of privacy to location data so long as movements are made on public thoroughfares.[165] Further, under the third-party analysis, there is no reasonable expectation of privacy to location data conveyed to service providers. However, this analysis may change soon, as several members of the Court have expressed concerns over these doctrines.

A. Plain View Analysis

Under the plain view doctrine, an individual does not have a reasonable expectation of privacy to information that is exposed in plain view and visible to the public.[166] The *Skinner* opinion serves as an example of the plain view doctrine applied to location data. Relying on the Supreme Court's rationale in *Knotts*, the Sixth Circuit determined that the Fourth Amendment does not protect location data emitted from a cell phone while driving on public streets because there is no reasonable expectation of privacy to travel on public thoroughfares.[167] The government conduct was compared to what occurred in *Knotts*, where police could have obtained the data by following the defendant's vehicle on public roads.[168]

Both the Sixth Circuit and the Supreme Court have recognized the value in police efficiency. In *Knotts*, the Court refused to "equate[] police efficiency with unconstitutionality."[169] In *Skinner*, the Sixth Circuit posits that "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals

---

165 United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012).

166 *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 215 (1986).

167 *Skinner*, 690 F.3d at 778.

168 *Id.*

169 United States v. Knotts, 460 U.S. 276, 284 (1983).

from circumventing the justice system."[170] In this context, the warrantless use of location data fits comfortably within constitutional doctrine, especially since a person does not have a reasonable expectation of privacy to their movements in public and obtaining this information does not provide police with any information that could not be gathered from mere observation.[171]

Some scholars argue for a reassessment of the presumption that individuals have no reasonable expectation of privacy in their public movements.[172] There is no doubt that an individual has no reasonable expectation of privacy in a single trip made in public. However, it is less clear whether it is reasonable to expect the totality of one's movements to be monitored, even when made in public.[173]

Justice Sotomayor expressed concern over long-term monitoring in *Jones*.[174] Specifically, because location data reveals details about one's "familial, political, professional, religious, and sexual associations," awareness of government surveillance may "chill[] associational and expressive freedoms. . . . The net result is that GPS monitoring . . . may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[175]

B. Third Party Analysis

Under the third-party doctrine, law enforcement can access location data from service providers. As mentioned above, modern cell phones routinely transmit signals to the nearest tower to ensure the strongest possible signal.[176] Service providers then create internal records of this data in order to determine where to erect additional cell

---

170 *Skinner*, 690 F.3d at 778.

171 *See also* Kyllo v. United States, 533 U.S 27, 34 (2001) (discussing the reason why technology that provides extrasensory information violated objective reasonable expectations of privacy).

172 *See* Rushin, *supra* note 14, at 327.

173 Courtney Burten, *Unwarranted! Privacy in a Technological Age: The Fourth Amendment Difficulty in Protecting Against Warrantless GPS Tracking and the Substantive Due Process and First Amendment Boost*, 21 S. CAL. INTERDISC. L.J. 359, 369 (2012) (arguing that it is not reasonable to expect the totality of one's movements to be monitored, even on public thoroughfares).

174 United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring).

175 *Id*. at 956 (citing United States v. Cuevas Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

176 William Curtiss, *Triggering a Closer Review: Direct Acquisition of Cell Site Location Tracking Information and the Argument for Consistence Across Statutory Regimes*, 45 COLUM. J.L. & SOC. PROBS. 139, 144 (2011).

towers.[177] Much like how we lose our reasonable expectation of privacy to transactions with banks, we lose any Fourth Amendment protection of data once it is transmitted to third parties, such as cell phone service providers.[178]

There have been many criticisms of this approach.[179] Some scholars contend that privacy has never been equated with mere secrecy. For instance, Professor Schulhofer believes that privacy is "the *right to control* knowledge about our personal lives, [and] the right to decide how much information gets revealed to whom and for which purposes."[180] Professor Schulholfer further contends that, "[r]elationships give meaning to our lives and define a large part of who we are. To insist that information is private only when it remains completely secret is preposterous."[181] While Professor Schulholfer's interpretation of privacy would severely impede the government's ability to conduct vital law enforcement functions, it is not without merit.

Even Justice Sotomayor's concurring opinion in *Jones* recognizes that, in the digital age, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[182] Some predict that other members of the Supreme Court likely believe that the mere existence of a digital intermediary does not remove all reasonable expectation of privacy.[183] Because modern communications often rely on a third-party service provider, the third-party doctrine becomes unduly restrictive.[184] Without using these third-party services, individuals living in today's technological world will not be able to communicate with his or her community and will not be able to participate fully in society.[185] These implications

---

177 *See* United States v. Graham, 846 F. Supp. 2d 384, 399 (D. Md. 2012).

178 *See* United States v. White, 401 U.S. 745, 752 (1971).

179 *See* Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 265 (2006) (urging abandonment of third-party doctrine); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 41 (urging restricting third-party to its original context in bank records and telephone numbers, but preventing the spread to network services); Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 546 (2006) (recognizing the rationale for third-party doctrine is "exceptionally strained").

180 SCHULHOFER, *supra* note 61, at 130.

181 *Id*.

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

183 *See* Strandburg, *supra* note 40, at 618.

184 *See* Ghoshray, *supra* note 38, at 65.

185 *Id*. at 73–74.

raise the question of whether such a blind adoption of the third-party doctrine should be permissible.[186] After all, the Court has sought to protect privacy, not solitude.

C. Criticisms of the Reasonable Expectation of Privacy Analysis

Katz's reasonable expectation of privacy test has recently come under scrutiny. Some of the criticism is directed at the ambiguity that arose from *Jones*. Recognizing the significance of modern wireless devices and the ability of service providers to track and record the location of users, Justice Alito expressed concern that real time surveillance on a constant basis for a prolonged duration is unreasonable under the *Katz* analysis.[187] But at what point does long-term monitoring become unreasonable under the reasonable expectation of privacy analysis? Law enforcement typically requests data from providers for periods of up to sixty days,[188] more than twice as long as the twenty-eight day surveillance in *Jones*.

Some scholars believe that the reasonable expectation of privacy analysis is inherently flawed. For example, Associate Professor Marc McAllister believes that this analysis denies a meaningful approach to the Fourth Amendment because stare decisis mandates the application of reasoning from an earlier technological era to modern cases.[189]

Further, the reasonable expectation of privacy analysis is unpredictable. As Justice Alito noted in his *Jones* concurrence, judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks at.[190] Indeed, the Court has noted in prior instances that there is "no talisman that determines in all cases those privacy expectations that society is prepared to accept as reasonable."[191] The *Katz* analysis is further flawed because it assumes that a reasonable person has a

---

186 *See* Joshua A. Engel, *Doctrinal Collapse: Smart Phones Cause Courts to Reconsider Fourth Amendment Searches of Electronic Devices*, 41 U. MEM. L. REV. 233, 238 (2010) (discussing how SCOTUS has been reluctant to "determine the exact contours of the reasonable expectation of privacy in the face of new technology").

187 *Jones*, 132 S. Ct. at 960–63 (Alito, J., concurring).

188 *See, e.g.*, *In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 829 (S.D. Tex. 2010).

189 McAllister, *supra* note 162, at 483–84.

190 *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (citing Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)).

191 *See, e.g.*, O'Connor v. Ortega, 480 U.S. 709, 715 (1987).

"well-developed and stable set of privacy expectations."[192] But as technology changes, the expectations of the hypothetical reasonable person change as well.[193]

In sum, under current law, the government can access cell phone technology to aid in the investigation and prosecution of crime without violating the Fourth Amendment. However, the underlying doctrine on which this conclusion rests has been sharply criticized by scholars and judges. Given this, the next question is not whether the government *can* utilize smartphone technology to aid in criminal investigation and prosecution, but whether the government *should* be able to and *to what degree*?

IV
POLICY

A. Society's Interest in Privacy

What if society is moving away from a culture that fundamentally values privacy? In this context, does the Fourth Amendment become antiquated in the same way that the fear of state-mandated quartering of soldiers became antiquated?[194] Smartphones allow people to maintain a constant connection with the social world. Consumers share a wealth of personal information with private entities, often to the benefit of both the user and entity. Indeed, Professor Paul Ohm believes that "[s]ystems of private surveillance are not simply becoming more powerful and widespread, but they are becoming all-knowing and ubiquitous," resulting in a "full evisceration" of the Fourth Amendment.[195] Thus, Professor Ohm asks: In a world without privacy, what good is a reasonable expectation of privacy test?[196]

It is worth mentioning the social and economic value behind recent shifts in technology. The value of developments in social media is inherent in their ability to promote the formations of friendships and the facilitation of political advocacy.[197] Further, recent communication developments provide great economic value.

---

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

193 *Id.*

194 *See* Ohm, *supra* note 14, at 1329.

195 *Id*. at 1311.

196 *But see* Nick Bilton, *Privacy Isn't Dead. Just Ask Google+*, N.Y. TIMES BITS (July 18, 2011, 12:59 PM), http://bits.blogs.nytimes.com/2011/07/18/privacy-isnt-dead-just-ask-google/?pagemode=print.

197 *See Kerry Hearings*, *supra* note 35, at 4.

Developments such as location data collected from cell phones allow companies tremendous flexibility in how they manage and store data, relate to customers, and assemble their workforces.[198] Thus, the importance of maintaining a specific type of relationship between a government and its people has collateral value, both economically and socially.

While we may be moving away from a society that values privacy over the benefits of constant connection, it is important to remember what the Fourth Amendment was designed to address: the relationship that a government should have with its people. In this context, privacy is merely a proxy for this relationship, albeit an outdated one. Two common misconceptions regarding privacy will help clarify this point: first, that the intimate details of people's lives are already exposed; and second, that individuals with nothing to hide should not fear governmental surveillance.

First, many people believe that information about their lives is already "out there."[199] This follows the prevailing rationale behind the third-party doctrine. That is, if we expose significant portions of our lives to private entities, then why should the government, who is charged with our safety, be denied access to that information?[200] Professor William Stuntz takes this position and views the support for privacy as a "disease" that undermines public safety and national security in the face of transnational threats and social disorder.[201]

But the Fourth Amendment does not directly address *information*. As Professor Ohm notes, if we are focused on information, then in the technological age, very little information about ourselves is private. Rather, the true core of the Fourth Amendment "offers a guarantee

---

198 *Id.*; *see also The Electronic Communications Privacy Act: Promoting Security and Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 111th Cong. 4 (2010) (statement of Brad Smith, Gen. Counsel, Microsoft Corporation) (uncertainty about how ECPA applies to various data hinders adoption of new technologies by individuals and impedes innovation), *available at* http://judiciary.senate.gov/pdf/10-09-22SmithTestimony.pdf.

199 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) (recognizing that many people view the tradeoff between increased convenience at the expense of privacy worthwhile, if not inevitable).

200 *But see id.* at 957 (Sotomayor, J., concurring) ("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.").

201 William J. Stuntz, *Secret Service: Against Privacy and Transparency*, NEW REPUBLIC (Apr. 17, 2006), http://www.newrepublic.com/article/against-privacy-and-transparency.

not merely of secrecy but of *personal autonomy*."[202] That is, the Fourth Amendment mandates that the government may not intrude on its citizens' ability to thrive as independent persons, for such intrusions stifle "associational and expressive freedoms."[203]

The second commonly held misconception is that individuals with nothing to hide would not object to governmental surveillance. However, this logic is deeply flawed. The Fourth Amendment was not designed to protect those with something to hide. Rather, the Framers intended to protect those very individuals with nothing to hide.[204] Individuals who commit crimes lose their Fourth Amendment protections upon a showing of probable cause that a crime has occurred.[205] Conversely, the Fourth Amendment shields the innocent from undue governmental intrusion and thereby preserves the relationship between the government and those who have done nothing wrong.

Here, the harm to the general public is the intrusive surveillance from the government. Awareness of government surveillance "chills associational and expressive freedoms" and alters "the relationship between citizen and government in a way that is inimical to democratic society."[206] Some scholars have drawn comparisons between the government's surveillance through location data and the architecture of a Panopticon prison, a circular prison that is designed such that every inmate is potentially observed at all times.[207] In monitoring location data through cell phones, governmental gaze becomes "internalized in the very minds of those subjected to its influence as a mechanism of rehabilitative discipline."[208] Targets of governmental gaze have no way of knowing if and when they are being watched, yet it is commonly understood that you can be tracked via cell phones.[209] It is this simultaneous dichotomy of surveillance

---

202 SCHULHOFER, *supra* note 61, at 6.

203 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (citing United States v. Cuevas Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

204 *See* SCHULHOFER, *supra* note 61, at 171.

205 Arrests based on probable cause significantly reduce an individual's privacy interest. *See generally* Maryland v. King, No. 12-207, 23–27 (2013) (recognizing lowered expectations of privacy after lawful arrest based on probable cause).

206 *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (citing *Cuevas Perez*, 640 F.3d at 285 (Flaum, J., concurring)).

207 *See* Pell & Soghoian, *supra* note 55, at 164.

208 *Id*.

209 *Id*. at 166.

that produces the anxiety that forms the panoptic effect.[210] This is what Justice William O. Douglas had in mind when he said, "[m]onitoring, if prevalent, certainly kills free discourse and spontaneous utterances."[211]

Some scholars pose a different theory on the relationship between the individual and society. Professor Solove believes that the individual's interest in privacy and society's interest in privacy are interrelated rather than antagonistic.[212] Thus, the value of protecting the individual is a social one. "Part of what makes a society a good place in which to live is the extent to which it allows people freedoms from the intrusiveness of others. A society without privacy protection would be oppressive."[213]

Some members of the Court have endorsed the normative belief that one should be free from persistent visual observation, even when in public. Former Chief Justice William Rehnquist has argued that some acts, though public, are not expected to be recorded.[214] For example, driving to a public bar is not necessarily private, but patrons would likely feel uneasy if they knew that a police officer was recording how many times they went to that bar in a given week.[215] Justice Rehnquist suggests that perhaps the focus should not be on the individual interest asserted, but rather, the government interest justifying the action.[216]

B. Legitimate Government Interests

The government has a legitimate interest in obtaining location data in criminal investigations and also in ensuring public safety. When location data is immediately accessible, law enforcement can deploy resources effectively "without placing officers, or the public, at undue risk."[217] Access to location data has reduced the amount of time it takes for the U.S. Marshals to find fugitives from forty-two days to

---

210 *Id*. at 167.

211 United States v. White, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting).

212 DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 49 (2011).

213 *Id*. at 50.

214 William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 10 (1974).

215 *Id*.

216 *Id*. at 11.

217 *Baker Statement*, *supra* note 11, at 5.

two.[218] Further, location data helped law enforcement find the main plotter of the September 11th terrorist attacks and one of the July 21st London bombers after the suspect had fled to Rome.[219] Importantly, location data can provide special assistance in cases of kidnapping and missing persons.[220] Thus, any restrictions on law enforcement to quickly and efficiently determine the general locations of criminal activity may have a very direct cost in terms of the governments ability to safely and efficiently ensure public safety.

Some scholars argue that in the information age, as criminals begin to use sophisticated technology to avoid detection, the government should also be able to use such technology to aid in the apprehension of suspects. In an argument in favor of the third-party doctrine, Professor Orin Kerr believes that the Fourth Amendment should not prevent technology from giving criminals a leg up on avoiding detection.[221] It was once true that criminals had to perform physical acts to carry out their plots, but now, these acts can be performed behind computers in an attempt to conceal their actions.[222] In this context, the third-party doctrine is necessary to level the playing field. This principle was recognized in *Skinner*. "When criminals use modern technological devices to carry out criminal acts and to reduce the possibility of detection, they can hardly complain when the police take advantage of the inherent characteristics of those very devices to catch them."[223] Indeed, location data is most useful in the early stages of a criminal investigation, when the government lacks probable cause to obtain a warrant.[224]

In a world where privacy is not significantly valued, some do not find it unreasonable for law enforcement to utilize location data while in pursuit of terrorists and criminals.[225] In arguing that our concept of

---

218 *Landau Hearing*, *supra* note 9, at 2.

219 *Id*.

220 *See* Lynne Terry, *Washington Police Used Cell Phone Pings to Zero in on Fugitive in Amber Alert*, OREGONLIVE.COM (Mar. 2, 2011, 5:44 PM, updated Mar. 3, 2011, 6:01 AM), http://www.oregonlive.com/pacific-northwest-news/index.ssf/2011/03/washington_police_used_cell_phone_pings_to_zero_in_on_fugitive_in_amber_alert.html.

221 Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580 (2009).

222 *Id*. at 576.

223 United States v. Skinner, 690 F.3d 772, 774 (6th Cir. 2012).

224 *See Baker Statement*, *supra* note 11, at 4.

225 Kozinski, *supra* note 42, at 124.

privacy has gotten out of hand, Justice Rehnquist urged for a return to the core area of privacy: the person, house, papers, or effects.[226]

Justice Rehnquist also posits that law enforcement is necessary for our society to have privacy.[227] Privacy is justified by civil liberties, which rely upon a self-governing society.[228] If we adopt the view that law-enforcement is necessary for a self-governing society, then civil liberties can only exist in a society maintained by public order.[229]

Of course, there are other recognized benefits of governmental access to location data. First, a digitally efficient investigative state reduces criminal activity.[230] If individuals recognize that their movements are being monitored regularly, they will be less likely to engage in criminal activity for fear of being apprehended.[231] Further, effective investigation of crime has a budgetary impact. Not only is it cheaper to monitor individuals through technology as opposed to assigning law enforcement to trail a particular suspect, but the taxpayers will also be spared expenses caused by property crimes.[232] Given that the United States spent over $98 billion on policing and over $46 billion on the judiciary in 2007, the budgetary consequences of restraining governmental access to location data cannot be ignored.[233]

V
TOWARDS A BALANCED APPLICATION OF THE FOURTH AMENDMENT TO LOCATION DATA

In *Jones*, five members of the Court expressed their concerns that the application of the trespass doctrine to the modern era is inconsistent with the Fourth Amendment. In particular, Justice Sotomayor's concurring opinion, as well as Justice Alito's concurring opinion (joined by Justice Ginsburg, Justice Breyer, and Justice

---

226 Rehnquist, *supra* note 214, at 3.

227 *Id*. at 21–22.

228 *Id*. at 22.

229 *Id*.

230 Rushin, *supra* note 14, at 294.

231 *Id*.

232 *Id*. (detailing studies that indicate surveillance technology substantially deters property crime); *see also Crime in the United States, 2011: Property Crime*, FED. BUREAU OF INVESTIGATION (finding that property crimes in 2011 resulted in an estimated loss of $15.6 billion), http://www.fbi.gov/about-us/cjis/ucr/crime-in-the-u.s/2011/crime-in-the-u.s.-2011/property-crime/propertycrimemain_final.pdf (last visited Aug. 5, 2013).

233 Rushin, *supra* note 14, at 297.

Kagan), suggests that when the Court hears the issue of location data, a new approach may be necessary.

This section will begin by reviewing an approach that is gaining prominence among scholars: the Mosaic Theory. The conclusion of this section then proposes a new standard that balances the interests of privacy activists and legitimate government interests.

A. The Mosaic Theory

According to the Mosaic Theory, whether government conduct amounts to a search does not depend upon whether a particular individual act is a search, but rather, whether an entire course of conduct, viewed collectively, amounts to a search.[234] Thus, individual acts that may not be searches on their own accord may rise to the level of a search when committed in particular combinations.

The rationale behind the Mosaic Theory can be linked to the reasonable expectation of privacy test. It is not reasonable to expect that the *totality* of one's movements would be monitored by a member of the public.[235] Thus, under the Mosaic Theory, a person has a reasonable expectation of privacy in the totality of his movements made in public if the aggregation of those movements was made possible through technological means.[236]

The Mosaic Theory has gained prominence from the courts. Before reaching the Supreme Court, the D.C. Circuit applied the Mosaic Theory to *Jones*.[237] In concluding that long-term GPS surveillance of movements exposed to the public view was a search, the D.C. Circuit reasoned that prolonged surveillance revealed information substantively different than short-term surveillance.[238] In particular, a person who knows the totality of another person's movements is able to determine whether someone is a "weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts."[239]

---

234 Bethany L. Dickman, *Untying Knotts: The Application of Mosaic Theory to GPS Surveillance in* United States v. Maynard, 60 AM. U. L. REV. 731, 736 (2011).

235 Walsh, *supra* note 50, at 233.

236 *Id.*

237 *See, e.g.*, United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

238 *Id.*

239 *Id.*

The Mosaic Theory also has some support from members of the Supreme Court. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, came to the conclusion that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[240] Additionally, Justice Sotomayor explicitly endorsed this language from Justice Alito's concurrence.[241]

The primary criticism of the Mosaic Theory is that it remains largely unworkable in the absence of bright-line rules.[242] That is, at what point would a series of acts trigger the Mosaic Theory?[243] There is some guidance from Justice Alito, who does not answer the question directly but does tell us "the line was surely crossed before the [four]-week mark."[244] Unfortunately, Justice Alito's concurrence ultimately perpetuates the confusion surrounding the standard for law enforcement to access location data. As the Solicitor General stated in his brief, "the 'mosaic' theory is unworkable. Law enforcement officers could not predict when their observations of public movements would yield a larger pattern and convert legitimate short-term surveillance into a search."[245]

B. A Practical and Balanced Approach

In proposing a workable application of the Fourth Amendment to the government's access to location data, this Comment seeks to strike a balance between legitimate governmental interests and the right to be free from undue governmental intrusion. The original ECPA was a compromise between these two competing, yet equal interests.[246] Further, the tension between these interests has existed even before the technological age. Justice Rehnquist noted that in the

---

240 United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

241 *Id*. at 955 (Sotomayor, J., concurring) ("I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

242 *See, e.g.*, New York v. Belton, 453 U.S. 454, 458 (1981) (acknowledging the importance of translating the Fourth Amendment into rules that law enforcement can predictably apply).

243 Pell & Soghoian, *supra* note 55, at 147.

244 *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

245 Brief for the United States at 14, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259).

246 *See The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age: Hearing Before the S. Comm. on the Judiciary*, 112th Cong. 3 (2011) (opening statement of Sen. Patrick J. Leahy), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112shrg70856/pdf/CHRG-112shrg70856.pdf.

history of political theory and constitutional law, the concern for individual liberty (freedom) has competed with the need for the government to remain responsive to the public's needs.[247] A free society seeks to achieve a balance between these two principles because unregulated freedom results in anarchy, while absolute order is despotism.[248]

While it exceeds the scope of this Comment, it is worth recognizing the ongoing debate regarding whether it should be up to Congress or the Court to decide what is an appropriate balance.[249] Because there are several members of the Court who believe that the legislature is in the best position to act, this Comment will defer to the legislature.[250]

Given that there are two ways to obtain location data, this Comment will propose a dual standard. First, in order to obtain precise location data (via GPS, triangulation, etc.), the government must obtain a warrant by providing specific and articulable facts demonstrating probable cause that a crime has been committed. Further, the location data sought must be reasonably related to the ongoing investigation. This probable cause standard protects the intimate details that are revealed by our location, minimizing undue surveillance that "chills associational and expressive freedoms."[251] It further tailors the scope of the information gathered to a level that is reasonable to the needs of the investigation.

The government's interest in law enforcement is satisfied because police will have access to a reasonable scope of location data upon a showing of probable cause. In fact, this standard is consistent with

---

247 Rehnquist, *supra* note 214, at 2.

248 *Id*.

249 *Compare* SOLOVE, *supra* note 212, at 165–66 (arguing that the court should devise a standard because (1) Congress has failed to regulate many new technologies; (2) statutes are often as unclear as the Fourth Amendment; and (3) courts can quickly update rules as technology shifts), *with* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 868–75 (2004) (arguing that legislatures should regulate new technologies because (1) courts are confined to deciding disputes from past events and thus cannot be forward thinking; (2) limitations caused by stare decisis limit the ability of judicial rules to change quickly; and (3) legislative rules tend to incorporate information from wide sources of information while courts are restrained to briefs and oral arguments by two parties).

250 *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (recognizing that the legislature is best suited to "gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way").

251 *Id*. at 956 (Sotomayor, J., concurring) (citing United States v. Cuevas Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

U.S. Department of Justice standards, which dictate that investigators must have probable cause to obtain a warrant for GPS information.[252] Thus, this proposal codifies existing Department of Justice policy. Additionally, this standard has found support in some courts, where it has already been concluded that applications seeking GPS data may be granted only after a showing of probable cause.[253]

Second, in order to access network-based location data, the government must obtain a warrant based on reasonable suspicion that a crime has been committed. Network-based location data is much less precise than GPS/triangulation location data and tends to reveal only the cell phone's general vicinity. Thus, it does not reveal the intimate details that accompany knowledge of precise location. Accordingly, the burden for law enforcement should be lower.

Because location data is crucial in the beginning stages of an investigation, a lower threshold will allow law enforcement to more efficiently gather evidence leading to probable cause. This lowered standard for general location data is also consistent with existing Department of Justice policy.[254]

Thus, while the dual standard proposed in this Comment is not necessarily new, the legislature or the Supreme Court has not permanently codified it. This Comment therefore recommends the formal adoption of this standard in order to provide a clear, uniform, and balanced application of the Fourth Amendment to location data.

The Supreme Court should also abandon the distinction between protected spaces and public spaces in the context of location data emitted from smartphones for two reasons. First, only precise location data (such as GPS data) has the potential to reveal details regarding a protected space. Under the balanced approach, law enforcement must present probable cause that a crime has been committed. Thus, because law enforcement will already have presented probable cause to obtain this data, government monitoring of protected spaces would not violate the Fourth Amendment.

---

252 *Baker Testimony*, *supra* note 75, at 8.

253 *See In re* Application of the U.S. Authorizing the Release of Historic Cell-Site Info., 809 F. Supp. 2d 113, 118–19 (E.D.N.Y. 2011) (explaining records sought that captured enough of the user's location information for a long enough time period to depict a sufficiently detailed and intimate picture of his movements required probable cause showing); *see also In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 835 (S.D. Tex. 2010).

254 *See Baker Testimony*, *supra* note 75, at 20.

Second, network-based location information is not sufficiently precise to reveal a phone's location within a particular private space.[255] Based on the reasoning in *Karo*, the government's collection of network-based location data would not violate Fourth Amendment protections, even when the phone happens to be located in a private space, because the location data would not allow the government to know it is in any particular private space.[256]

Perhaps, more radically, Fourth Amendment jurisprudence should stop treating secrecy as a prerequisite for privacy.[257] This position has support from at least one member of the Court, as Justice Sotomayor 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."[258]

Given that various Justices have recognized that the length of surveillance is a critical factor in determining the legality of electronic surveillance,[259] the warrant should be issued for a period that is no greater than the amount of time reasonable to allow law enforcement to carry out the investigation. This period should not exceed thirty days, at which point the government may seek a renewal of the warrant by providing affidavits that the investigation is still ongoing.

CONCLUSION

Despite recent technological advances, the body of law regarding the Fourth Amendment's approach to location data has remained relatively unchanged. As discussed, a review of Fourth Amendment doctrine reveals that there is no uniform, defined standard for law enforcement to obtain location data. Further, principles such as the plain view doctrine and the third-party doctrine complicate the analysis when advanced technologies enter the picture.

Because the scholarly discussion about these issues has remained largely hostile to the legitimate interests of law enforcement, this Comment proposes a new standard that balances the concern for

---

255 Walsh, *supra* note 50, at 239.

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

257 *See* Smith v. Maryland, 442 U.S. 735, 749 (1979) (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.").

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

259 *See, e.g.*, Jones, 132 S. Ct. at 964 (2012) (Alito, J., concurring); *id*. at 955 (Sotomayor, J., concurring).

individual liberty and the equal yet competing governmental interest to remain responsive to public safety. While this approach was designed to reflect Fourth Amendment principles, it was not only inspired by what has been, it also contemplates what may be.