Journal of Technology Law & Policy

Volume XIII – Spring 2013

ISSN 1087-6995 (print)

DOI 10.5195/tlp.2013.120

http://tlp.law.pitt.edu

Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance

Michael T.E. Kalis

Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance

Michael T.E. Kalis*

INTRODUCTION

Cell phones play an ever-expanding role in the lives of cell users and in the functioning of modern society.[1] They are used to browse the Internet, send/receive emails and texts, purchase goods online, provide directions, store and play music; they serve as planners, calendars, dictionaries, encyclopedias, and more. In many respects, their utility has made them a necessity. A person who wishes to partake in the social, cultural, and business affairs of society has no realistic choice but to use a cell phone.[2] Consequently, cell phones accompany their users wherever they go—business offices, entertainment venues, vacations, places of religious worship, and the homes of friends and family.[3]

As cell phone users move about in their daily lives, phone in hand or pocket, their cell phones communicate their locations to the cell service providers. These communications generate cell site location information ("CSLI" or "location data"). Prospective CSLI provides real-time cell phone locations and historical CSLI reveals past cell phone locations. This article considers the privacy implications of historical CSLI.

Historical CSLI has vast privacy implications because the government frequently compels cell service providers to disclose this trove of information to aid in surveillance and investigations. Law enforcement agents mine through historical location data looking for evidence of a crime. But this practice of gathering and surveying historical CSLI extends to citizens beyond those subject to a criminal

* J.D. Candidate, University of Pittsburgh School of Law, May 2014; B.A., Political Science, Kenyon College.

[1] 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, 126 (2012) (more than ninety-five percent of the United States population subscribed to a cell phone by the end of 2010).

[2] *See In re* Application of the U.S. for an Order Authorizing the Release of Historical Cell-Site Information, 736 F. Supp. 2d 578, 582 (E.D.N.Y. 2010).

[3] *In re* Application U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 541 (D. Md. 2011).

Journal of Technology Law & Policy

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

investigation. The government regularly analyzes the historical CSLI of innocent parties—friends, associates, neighbors, and complete strangers who happen to pass by a cell tower at a given time. Permeating surveillance such as this brings to mind images of George Orwell's Big Brother Government, or Jeremy Bentham's Panopticon prison architecture and its coercive social power envisioned by Michel Foucault.[4] In addition to the breadth of this practice, historical CSLI surveillance creates an unparalleled intrusion into the private life of the person whom the government targets.

Unlike other surveillance techniques, historical CSLI does not reveal details from a single moment in time—a single trip, a single phone number dialed on the telephone, or a single stakeout—its scope and utility is much broader. "[N]o single journey reveals the habits and patterns that mark the distinction between a day in the life and a way of life, nor the departure from a routine that, like the dog that did not bark in the Sherlock Holmes story, may reveal even more."[5] In the digital age, cell phones are artists, CSLI their canvas, and the movements of cell users their palette—the finished product being an intimate portrait of each cell user's life.

Despite historical CSLI surveillance's pervasive and invasive qualities, courts regularly permit law enforcement agencies to obtain location data without first establishing probable cause as required by the Fourth Amendment.[6] Courts do this by holding that historical CSLI falls within the purview of the federal Stored Communications Act[7] or that the government's use of the data does not constitute a search under the Fourth Amendment. In holding that historical CSLI surveillance does not implicate the Fourth Amendment, these courts rely on two classic Fourth Amendment exceptions—the third-party exception and the public exposure exception—to rule that a cell user has no reasonable expectation of privacy in historical CSLI.[8]

---

[4] Pell & Soghoian, *supra* note 1, at 164–73 (discussing the works of each author). *See* United States v. Pineda-Moreno, 617 F.3d 1121 (9th Cir. 2010) (Kozinski, J., dissenting) ("1984 may have come a bit later than predicted, but it's here at last."); GEORGE ORWELL, 1984 (1950). *See* MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON (2d ed. 1995); JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., 1995) (1787).

[5] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

[6] *See* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 690–91 (2011); Patrick T. Chamberlain, *Court Ordered Disclosure of Historical Cell Site Location Information: The Argument for a Probable Cause Standard*, 66 WASH. & LEE L. REV. 1745, 1755–58 (2009).

[7] Electronic Comm. Privacy Act of 1986 § 201, 18 U.S.C §§ 2701–2711 (2006). *See also* Chamberlain, *supra* note 6, at 1755–58.

[8] *See infra* Parts III and IV.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

This article furthers the general position that the government's use of historical CSLI for surveillance implicates the Fourth Amendment. In making this argument, this article refutes the applicability of these Fourth Amendment exceptions and highlights the novel theory several courts have adopted to hold that the Fourth Amendment does apply.[9] Finally, in light of the unparalleled intrusion created by historical CSLI surveillance, this article stresses the need to reevaluate the approach underlying the exceptions, which treats secrecy as a prerequisite for privacy.[10]

I. THE TECHNOLOGY OF CELL SITE LOCATION INFORMATION

A. Types of CSLI

CSLI refers to the data generated by communications made between cell phones and cell sites.[11] Cell sites are transmitting devices that form a cell network and they are usually located on cell towers.[12] Cell service providers strategically spread cell sites throughout their geographic coverage area.[13] Service providers record various types of CSLI.[14]

As a person travels with her cell phone, the phone's signal shifts from cell site to cell site to receive the best signal.[15] To maintain the strongest signal, a cell phone continuously and automatically registers itself with the closest cell site every seven seconds.[16] This process generates registration data.[17] When a cell user begins and ends a call, the cell phone generates initiation and termination data—that is, a record of the closest cell site when the call starts and finishes.[18] During a call, the cell phone creates duration data.[19] This data reflects the communications that the

[9] *See infra* Parts IV and V.

[10] *See infra* Conclusion.

[11] Freiwald, *supra* note 6, at 702–03.

[12] Pell & Soghoian, *supra* note 1, at 126.

[13] *Id. See also* Freiwald, *supra* note 6, at 702.

[14] Pell & Soghoian, *supra* note 1, at 128.

[15] Freiwald, *supra* note 6, at 702–03; Pell & Soghoian, *supra* note 1, at 127–28.

[16] Freiwald, *supra* note 6, at 702–03; Chamberlain, *supra* note 6, at 1752.

[17] Freiwald, *supra* note 6, at 705–06; Chamberlain, *supra* note 6, at 1752–53.

[18] Freiwald, *supra* note 6, at 703–04.

[19] *Id.* at 704–05.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

cell phone had with cell sites throughout the call.[20] For example, if a cell user changes locations while on a call, duration data reveals the various cell sites that the phone communicates with as it moves through the network.[21] Cell service providers store historical CSLI for diagnostic, billing, and other purposes; and they generally retain each subscriber's location data for at least one year.[22]

B. CSLI Precision

The precision with which CSLI pinpoints a cell phone—and cell user—depends on the proximity of the cell sites to each other.[23] The closer together the cell sites, the more precise the reading.[24] To compensate for the higher number of active cell users, densely populated areas generally contain a greater number of cell sites spaced closer together than do rural areas.[25] Service providers are constantly adding more cell sites to their networks.[26] The current distribution of cell sites enables CSLI to pinpoint a cell user's location with nearly the same precision as Global Positioning System ("GPS") technology.[27]

Methods such as triangulation and sector-identification also improve the locating precision of CSLI.[28] Analysts can triangulate the position of a cell user by using a mathematical equation that considers data from overlapping cell towers and changes in strength of communication signals.[29] Triangulation locates a cell user with the accuracy of GPS technology.[30] Sector-identification refers to determining

---

[20] *Id.*

[21] *Id.*

[22] Allie Bohm, *How Long Is Your Cell Phone Company Hanging On To Your Data?*, ACLU (Sept. 28, 2011, 10:17 AM), http://www.aclu.org/blog/technology-and-liberty/how-long-your-cell-phone-company-hanging-your-data.

[23] *Id.* at 710–11; 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, 850 (2012) ("The precision of the cell phone user's location directly correlates with the cell-site size.").

[24] Davis, *supra* note 23, at 850.

[25] Freiwald, *supra* note 6, at 710.

[26] *Id.* ("With providers adding towers to their networks all the time, tower proximity in any particular place should be increasing."); Davis, *supra* note 23, at 850 ("The number of cell sites in the United States has tripled over the last decade. . . .").

[27] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 837 (S.D. Tex. 2010); *see In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 534 (D. Md. 2011).

[28] Freiwald, *supra* note 6, at 711–12.

[29] *Id.* at 712–13.

[30] *Id.* at 712.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

the sector of a cell tower with which a cell phone communicated.[31] By identifying the particular sector, the cell user's location can be narrowed by one-third.[32]

Finally, as technology improves so too will the precision with which CSLI pinpoints cell users.[33] As one court stated: "The inexorable combination of market and regulatory stimuli ensures that cell phone tracking will become more precise with each passing year."[34]

II. POLICE USE OF CSLI

CSLI surveillance has increased exponentially in a very short amount of time.[35] Between 2008 and 2012, Sprint received nearly 200,000 requests for location data.[36] A congressional subcommittee report from 2010 estimated that the total number of electronic surveillance orders issued at the federal level exceeded 10,000 per year.[37] The rise in CSLI surveillance is a representative of the government's increasing requests for all types of cell data.[38] Law enforcement requests for cell data—including but not limited to CSLI—have increased between twelve to sixteen percent annually.[39] In response to a 2012 congressional inquiry, cell service providers reported that they handled 1.3 million demands for subscriber

[31] *Id.* at 711.

[32] *Id.*

[33] *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 534 (D. Md. 2011).

[34] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010).

[35] Pell & Soghoian, *supra* note 1, at 121; Eric Lichtblau, *More Demands on Cell Carriers in Surveillance*, N.Y. TIMES (July 8, 2012), http://www.nytimes.com/2012/07/09/us/cell-carriers-see-uptick-in-requests-to-aid-surveillance.html?pagewanted=all&_r=0.

[36] Chris Soghoian, *Tuesday: Federal Appeals Court Hears Important Cell Phone Tracking Case*, ACLU (Oct. 1, 2012, 3:05 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/tuesday-federal-appeals-court-hears-important-cell.

[37] Scott A. Fraser, *Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell-Site Location Jurisprudence*, 52 SANTA CLARA L. REV. 571, 574 (2012).

[38] Interestingly, as cell surveillance has increased, the number of warrants issued for wiretaps has decreased. Lichtblau, *supra* note 35 ("The diverging numbers suggest that law enforcement officials are shifting away from wiretaps in favor of other forms of cell tracking that are generally less legally burdensome, less time consuming and less costly.").

[39] Lichtblau, *supra* note 35.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

information in 2011 alone.[40] AT&T fielded roughly 700 requests per day; and Sprint received 1,500 requests per day.[41]

The rise in CSLI surveillance can largely be attributed to its effectiveness as an investigatory tool.[42] Prospective CSLI proves invaluable during emergencies such as child abductions and suicide calls.[43] In one instance, police used prospective location data to find a stabbing victim who was in a basement hiding from the attacker.[44] Equipped with prospective CSLI, U.S. Marshals now find fugitives in approximately two days, down from forty-two days.[45] Among many other functions, historical CSLI allows the government to place a target at the scene of a crime;[46] undermine a suspect's alibi;[47] or show a pattern of movements that, when viewed in the aggregate, evidence criminal activity.[48] In addition, CSLI allows authorities to allocate resources more effectively and cost-efficiently, and reduce unnecessary risks.[49]

Needless to say, CSLI is a valuable weapon that produces real-life benefits.[50] Law enforcement agents have gone as far as to suggest that its benefits outweigh any legal questions.[51] Reasoning like this calls to mind Justice Brandeis's admonition that "[e]xperience should teach us to be most on our guard to protect liberty when the government's purposes are beneficent."[52]

---

[40] *Id.*

[41] *Id.*

[42] Pell & Soghoian, *supra* note 1, at 120–21; Fraser, *supra* note 37, at 574.

[43] Eric Lichtblau, *Police are Using Phone Tracking as a Routine Tool*, N.Y. TIMES (Mar. 31, 2012), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html ?pagewanted=all.

[44] *Id.*

[45] Pell & Soghoian, *supra* note 1, at 120.

[46] *Id.* at 119–20.

[47] Briana Schwandt, *Is the Government in My Pocket? An Overview of Government Location Tracking of Cell Phones under the Federal System and in Montana*, 72 MONT. L. REV. 261, 263 (2011).

[48] *See infra* Parts IV-B and Part V.

[49] Pell & Soghoian, *supra* note 1, at 120; 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, 171 (2012).

[50] Lichtblau, *supra* note 43.

[51] *Id.*

[52] Olmstead v. United States, 277 U.S. 438, 572 (1928) (Brandeis, J., dissenting).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

Historical CSLI surveillance is an abusive surveillance practice when unchecked. Law enforcement agents regularly conduct "dragnet surveillance" by compelling a service provider to turn over the CSLI of every cell user whose phone communicated with a cell site at a particular time.[53] The government then mines that data, which may include the CSLI of hundreds or thousands of cell users, to try to figure out who was involved with the crime.[54] The government also actively targets and scrutinizes the historical CSLI of friends or associates of persons under criminal investigation.[55] For instance, in one case the government sought the historical CSLI of a woman allegedly associated with the criminal suspect, though she herself was not a suspect in the investigation.[56]

Without a probable cause warrant requirement providing a detached judiciary to oversee the use of this intrusive technology, the only impediment to abuse is governmental abstention.[57] The Supreme Court has historically rejected self-restraint as a reason for permitting government conduct: "[T]his Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end."[58]

III. RELEVANT FOURTH AMENDMENT JURISPRUDENCE

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[59] As indicated by its language, the Fourth Amendment applies when

[53] Freiwald, *supra* note 6, at 723; *see also* Lichtblau, *supra* note 35 (describing cell tower "dump[s]" as being when a police agency requests the CSLI of all cell subscribers who were near a cell tower at a certain time).

[54] Freiwald, *supra* note 6, at 723; Lichtblau, *supra* note 35; *see also* Declan McCullagh, *ACLU: FBI Used 'Dragnet'-Style Warrantless Cell Tracking*, CNET (June 22, 2010, 9:37 AM), http://news.cnet.com/8301-31921_3-20008444-281.html ("[T]he government obtained information that could be used to track the movements and locate the whereabouts at specific times of up to 180 people.").

[55] Freiwald, *supra* note 6, at 723; *see also id.* n.258 (describing common practice where government agents seek the CSLI of persons with whom the target communicates).

[56] *In re* U.S. for an Order Directing a Provider of Elec. Comm. Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 588 n.11 (W.D. Pa. 2008) (noting that government had provided "no specific information connecting these two individuals, or connecting the Criminal Suspect to the cell phone."); *see also* Freiwald, *supra* note 6, at 692.

[57] Freiwald, *supra* note 6, at 720–21.

[58] Katz v. United States, 389 U.S. 347, 356–57 (1967).

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

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

there has been a search or seizure.[60] To determine whether there has been a search, the court asks whether an individual has an expectation of privacy that society is prepared to recognize as reasonable.[61] This test traces back to Justice Harlan's concurrence half a century ago in *Katz v. United States*.[62]

The *Katz* test was believed to have completely replaced the trespass test from *Olmstead*.[63] In *United States v. Jones*, however, the Supreme Court clarified that, in fact, the reasonable expectation of privacy test only augmented the trespass test.[64] Despite the reemergence of the trespass test, the *Jones* court made clear that "[s]ituations involving merely the transmission of electronic signals without trespass [remain] subject to *Katz* analysis."[65] Therefore, this article reviews the constitutionality of historical CSLI surveillance under the *Katz* reasonable expectation of privacy test.

The courts that have ruled that historical CSLI surveillance does not implicate the Fourth Amendment have relied on two classic Fourth Amendment exceptions to hold that cell users possess no reasonable expectation of privacy in their CSLI.[66] These exceptions are the third-party exception and the public exposure exception. Underlying both of these exceptions is the notion that secrecy is a prerequisite for privacy.[67]

A. Third-Party Exception

In *United States v. Miller*,[68] the government compelled two banks to disclose all of the defendant's account records.[69] The Supreme Court considered whether the disclosure of a customer's bank records constituted a Fourth Amendment

---

[60] Chamberlain, *supra* note 6, at 1760.

[61] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[62] *Katz*, 389 U.S. at 361 (1967) (Harlan, J., concurring).

[63] *Id.* at 352–53 ("We conclude that the underpinnings of Olmstead [have been] so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.").

[64] *See* United States v. Jones, 132 S. Ct. 945, 953 (2012).

[65] *Id.*

[66] *See, e.g.*, United States v. Suarez-Blanca, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008); United States v. Benford, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010); United States v. Skinner, 690 F.3d 772 (6th Cir. 2012); United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012); United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

[67] *See Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

[68] United States v. Miller, 425 U.S. 435 (1976).

[69] *Id.* at 437–38.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

search.[70] The Court held that there had been no search, as the defendant had no reasonable expectation of privacy in the information in question.[71] The defendant lacked an expectation of privacy in the information because "[a]ll of the documents obtained, including financial statements and deposit slips, contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[72] In disclosing this information to a third party, the defendant assumed the risk that the government could access those records without a warrant.[73]

In *Smith v. Maryland*,[74] the government had the telephone company install a pen register to record the numbers dialed from the petitioner's telephone.[75] The Supreme Court examined "whether the installation and use of a pen register constitute[d] a search within the meaning of the Fourth Amendment."[76] The Court rejected the petitioner's claim that he had a reasonable expectation of privacy regarding the number he dialed on his phone.[77] Therefore, no search had been conducted.[78] The Court reasoned that the petitioner "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business."[79] The petitioner assumed the risk that those records would be revealed to the police.[80] In its analysis, the Court also noted the limited intrusiveness of the government's activity: "Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[81]

---

[70] *Id.* at 439–40.

[71] *Id.* at 442.

[72] *Id.*

[73] *Id.* at 443.

[74] Smith v. Maryland, 442 U.S. 735 (1979).

[75] *Id.* at 735. *See also* Chamberlain, *supra* note 6, at 1762 ("A pen register is a device that records the numbers dialed from a particular phone.").

[76] *Smith*, 442 U.S. at 736.

[77] *Id.* at 742.

[78] *Id.* at 745–46.

[79] *Id.* at 744.

[80] Smith v. Maryland, 442 U.S. 735, 744 (1979).

[81] *Id.* at 741.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

B. Public Exposure: The Beeper Cases

In *United States v. Knotts*,[82] government agents attached a radio beeper to a container of chemicals stored in the defendant's automobile.[83] The agents then followed the automobile on public streets and highways.[84] The Court held that the beeper monitoring did not constitute a search under the Fourth Amendment, as "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[85] Through his public movements, the defendant "voluntarily conveyed to anyone who wanted to look" his progress and route.[86] In reaching this conclusion, the Court reserved the question of whether a warrant would be required in a case involving twenty-four hour surveillance.[87]

One year later in *United States v. Karo*,[88] the Court considered similar facts as *Knotts* but reached the opposite conclusion; thereby limiting its holding in *Knotts*. Unlike in *Knotts*, the beeper in *Karo* was used to locate the targeted item within a private residence.[89] Thus, the Court addressed whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violated the Fourth Amendment.[90] The Court held that the government's monitoring of the beeper did constitute a search, citing to the reasonable expectation of privacy existing in private residences.[91] The beeper surveillance impinged on this expectation because it revealed, "that the beeper was inside the house, a fact that could not have been visually verified."[92]

---

[82] United States v. Knotts, 460 U.S. 276 (1983).

[83] *Id.* at 278.

[84] *Id.*

[85] *Id.* at 281.

[86] *Id.* at 281–82.

[87] *Id.* at 283–84; *see also* United States v. Maynard, 615 F.3d 544, 556–58 (D.C. Cir. 2010) (citing other courts that have recognized the limited scope of the *Knotts* holding).

[88] United States v. Karo, 468 U.S. 705 (1984).

[89] *Id.* at 708–10 (describing facts of case).

[90] *Id.* at 713.

[91] *Id.* at 714–15.

[92] *Id.* at 715.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

Together, *Knotts* and *Karo* stand for the general proposition that the government may use a tracking device to ascertain an individual's location in public but not in a private.[93]

IV. DISTINGUISHING CSLI—WHY THE FOURTH AMENDMENT EXCEPTIONS DO NOT APPLY

A. Distinguishing Miller *and* Smith

Courts have used the *Miller/Smith* third-party exception to hold that cell users have no reasonable expectation of privacy in their CSLI.[94] Just as the defendant in *Smith* voluntarily conveyed numerical information to the phone company by dialing phone numbers and the defendant in *Miller* by giving documents to the bank, so too does the cell user voluntarily convey her CSLI to the service provider by using a cell phone.[95] Accordingly, the government's acquisition of a cell user's historical CSLI does not constitute a search under the Fourth Amendment.

The argument that a cell user voluntarily conveys CSLI to the service provider mischaracterizes the process by which cell phones generate CSLI, and does not consider the qualitative difference in information revealed by CSLI as compared to other surveillance practices. The defendant in both *Miller* and *Smith* unquestionably conveyed the information at issue.[96] One gave documents to a bank employee and the other dialed numbers on a telephone.[97] A cell phone user, however, "has not knowingly exposed or voluntarily conveyed [CSLI] to the provider, as those phrases are ordinarily understood."[98] Unlike the conveyances in

---

[93] *In re* U.S. for an Order Directing a Provider of Electronic Communications Service to Disclose Records to the Government, 534 F. Supp. 2d 585, 613 (W.D. Pa. 2008).

[94] *See, e.g.*, United States v. Suarez-Blanca, 2008 WL 4200156 (N.D. Ga. Apr. 21, 2008); United States v. Benford, 2010 WL 1266507 (N.D. Ind. Mar. 26, 2010).

[95] *See In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 843–44 (S.D. Tex. 2010) (discussing government's arguments for granting CSLI disclosure); *see also* Brief for the United States, at 15–23, *In re* U.S. for Historical Cell Site Data, No. 11-20884 (5th Cir. Feb. 15, 2012), *available at* https://www.eff.org/sites/default/files/filenode/GovOpeningBrief.pdf.

[96] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 844.

[97] *See supra* Part III-A (briefing *Miller* and *Smith*); *see also* Brief for American Civil Liberties Union Foundation et al., as Amici Curiae Supporting Affirmance, *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827 (S.D. Tex. 2010) (No. 11-20884), *available at* http://www.aclu.org/files/assets/5th_circuit_cell_phone_tracking_amicus_brief_texas.pdf.

[98] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 845; *see also* Freiwald, *supra* note 6, at 736 ("Cell phone users do not voluntarily, actively, and knowingly convey location data to providers."); Chamberlain, *supra* note 6, at 1785 ("Because CSLI is conveyed without user intervention, proponents of probable cause contend that the [third party] doctrine—which depends upon individuals voluntarily conveying information—simply does not apply.").

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

Miller and *Smith*, CSLI is an automatic byproduct of cell phone use and design.[99] To turn on the phone or make or receive a call, cell users do not enter their zip code, area code, or other location identifiers; nor do any of the digits they press reveal their location.[100]

The facts of *United States v. Forest*[101] illustrate one example of the lack of control cell phone users have over the creation of CSLI. In *Forest*, law enforcement agents dialed the defendant's phone but hung up before the phone rang.[102] The call still caused the defendant's phone to generate CSLI, which the agents then used to track his movements.[103] The court correctly concluded that the user had not voluntarily conveyed the CSLI—the agent, not the defendant, called the phone causing it to generate CSLI.[104]

Historical CSLI surveillance is also a substantially more intrusive practice than the practices at issue in *Miller* and *Smith*. The Court in *Smith* explicitly noted the limited intrusion created by the pen register.[105] By contrast, historical CSLI surveillance records the cell user's movements over a prolonged period of time, revealing travels, activities, and associations.[106] As Magistrate Judge Smith in the Southern District of Texas incisively observed: "If the telephone numbers dialed in *Smith v. Maryland* were notes on a musical scale, the location data sought here is a grand opera."[107]

B. Distinguishing Knotts *and* Karo

Courts have reasoned that CSLI locates users only imprecisely, thereby avoiding the privacy interests of the home at issue in *Karo*.[108] Implicit in this position is the belief that CSLI can never reveal an individual's presence or

---

[99] *See supra* Part I (describing different types of CSLI); *see also* Brief for American Civil Liberties Union Foundation et al., *supra* note 97, at 39 ("[Cell users] do not communicate their location to the cell phone company of their own volition.").

[100] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 844.

[101] United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

[102] *Id.* at 947.

[103] *Id.*

[104] *Id.* at 951.

[105] *See supra* Part III-A (discussing *Smith*).

[106] *See In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 839 (S.D. Tex. 2010).

[107] *Id.* at 846.

[108] *See id.* at 837.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

movements in places shielded from public view.[109] In adhering to *Knotts*' general principle, the courts reason that cell phone users have no reasonable expectation of privacy as they move from one public place to another, much as the defendant in *Knotts* had no expectation of privacy while traveling on public streets and highways.[110] These arguments are based on outdated assumptions and ignore the substantial intrusion permitted by historical CSLI.

The position that CSLI surveillance does not implicate the privacy interests stated in *Karo* is based on "yesteryear's assumption that [CSLI locates] users only imprecisely."[111] Cell site technology—microcells, triangulation, and sector identification—can now reveal a cell phone user's location with nearly the same precision as GPS data.[112] Anyone who has used Google Maps knows that GPS data can easily pinpoint a particular street address.[113] Moreover, as service providers continue to increase the number of cell sites in their network, CSLI will locate cell phones with greater precision.[114] In addition to the technological aspects, the ability to infer greatly enhances the precision of CSLI.[115] For example, by comparing CSLI with common sleep hours one would likely be able to determine when a cell user was at home.[116] For the foregoing reasons, it is simply incorrect that CSLI can never reveal "whether a particular article—or a person, for that matter—is in an individual's home at a particular time."[117]

The simplistic argument that historical CSLI surveillance amounts to following a person moving in public ignores the fundamental difference in the intrusion created by this practice.[118] In *Knotts*, the tracking was limited to a single

---

[109] *See id.* at 837 (citing Brief for the United States at 34–35, 2009 WL 3866618 (Feb. 13, 2009); *see also* Freiwald, *supra* note 6, at 729; Chamberlain, *supra* note 6, at 1787–88).

[110] *See supra* Part III-B (discussing *Knotts*).

[111] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 837.

[112] *See supra* Part I (regarding CSLI technology); *see also In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 837; Freiwald, *supra* note 6, at 710–13 (discussing precision of triangulation and sector identification).

[113] Freiwald, *supra* note 6, at 713–14 (regarding the precision of GPS data).

[114] *See supra* Part I.

[115] *See* Freiwald, *supra* note 6, at 724–25.

[116] *Id.* at 724–25; *see also id.* n.268 ("[This] would show the telephone on in the same place for long periods (for example, sleeping hours) that would correspond to the time the target was home.").

[117] United States v. Karo, 468 U.S. 705, 716 (1984).

[118] *See* Freiwald, *supra* note 6, at 730 ("An attempt to minimize the privacy intrusion that location data monitoring presents by analogizing it to bumper-beeper monitoring or even visual surveillance by police ignores fundamental differences.").

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

trip from one place to another.[119] What the government learned during that trip was limited to what could be observed over the course of that trip.[120] Historical CSLI surveillance, by contrast, reveals the totality and pattern of one's movements twenty-four hours a day and over a period of weeks, months, or even years.[121] Prolonged surveillance like this is drastically different than the surveillance practice considered in *Knotts*.[122] Unlike an individual's movements during a single journey, the whole of one's movements over the course of several months is not exposed in the same way.[123] Although each individual movement may be exposed to the public, one's aggregated movements tell a different story.[124]

Together, *United States v. Jones* and the *Jones* retrial[125] illustrate how the sequence of one's movements reveals more than any one of its constituent parts, and historical CSLI's ability to evidence that sequence. In *Jones*, the government tracked Jones' movements for one month using a GPS device installed on the defendant's vehicle.[126] At trial, the government used the GPS data to show, not the location of the stash house or Jones' movements over any one trip or even day, but the pattern of his movements to evidence his involvement in cocaine trafficking.[127] The government prosecutor said in his opening statement: "I want to . . . just show you an example of how the pattern worked. . . . The meetings are short. But you will again notice the pattern you will see in the coming weeks over and over again."[128]

The Supreme Court eventually ruled in *Jones* that the government's attaching of the GPS device to Jones' vehicle violated the Fourth Amendment and therefore excluded the evidence generated by the device.[129] The *Jones* case is now on

---

[119] *See supra* Part III-B (regarding *Knotts*).

[120] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 838–39 (S.D. Tex. 2010).

[121] *Id.* at 839. *See also supra* Part I (discussing CSLI technology).

[122] *See supra* Part III-B (briefing *Knotts*). *See also In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 838–39.

[123] *See infra* Part V.

[124] *Id.*

[125] *See* Sarah Roberts, *Court Says No GPS Tracking? How About Cell Phone Tracking?*, ACLU (Apr. 6, 2012, 12:55 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/court-says-no-gps-tracking-how-about-cell-phone.

[126] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[127] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

[128] *Id.*

[129] *Jones*, 132 S. Ct. at 949.

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

retrial.[130] To supplant the excluded GPS data, the government has obtained five months worth of Jones' CSLI.[131] Tellingly, the government seeks to prove with CSLI the same pattern of movements gathered by the GPS device.[132]

V. OF A REASONABLE EXPECTATION OF PRIVACY IN THE SUM OF ONE'S MOVEMENTS

For the Fourth Amendment to have force in the digital age, the Fourth Amendment must accommodate the changes brought about by technology. Cell phones and the CSLI they generate have made possible a level of governmental intrusion previously inconceivable.[133] The difference is not one of degree but of kind, for "the whole is something different than the sum of its parts."[134]

> Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month . . . a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he 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.[135]

Recognizing that cell users do not voluntarily convey or publicly expose these intimacies of life revealed by historical CSLI, several courts have held that the

[130] Roberts, *supra* note 125.

[131] *Id.*

[132] *Id.*

[133] *In re* United States for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d. at 126.

[134] United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2012) (citing KURT KOFFKA, PRINCIPLES OF GESTALT PSYCHOLOGY 176 (1935)).

[135] *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 839 (quoting United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010)).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

Fourth Amendment exceptions do not apply.[136] In doing so, these courts adopted the "mosaic theory"[137] to hold that society recognizes as reasonable an expectation of privacy in the totality of one's movements.[138] People do not expect their every movement, twenty-four hours a day and over a prolonged period of time, to be monitored.[139] Nor do people reasonably expect that their movements "will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[140] The intrusion historical CSLI surveillance makes into a person's private life stands in stark contrast to the relatively brief intrusions made in *Miller*, *Smith*, and *Knotts*.[141] Moreover, such an intrusion contradicts the Fourth Amendment, which "reflects a choice that our society should be one in which citizens dwell in reasonable security and freedom from surveillance."[142]

The mosaic theory marks an important step toward fortifying the Fourth Amendment in the digital age. By focusing the analysis on the aggregation of one's movements, this standard appropriately accounts for the new threats to individual privacy produced by historical CSLI surveillance. Moreover, this standard allows for meaningful consideration of these emerging threats to individual privacy by freeing Fourth Amendment jurisprudence from the constraints imposed by the third-party and public exposure exceptions, and the all or nothing approach to privacy underlying them.[143]

---

[136] *See, e.g.*, *In re* United States for Historical Cell Site Data, 747 F. Supp. 2d at 839 (quoting *Maynard*, 615 F.3d at 562); *In re* United States for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d at 118–19.

[137] *Maynard*, 615 F.3d at 562; *see also* Orin Kerr, *What's the Status of the Mosaic Theory After* Jones*?*, THE VOLOKH CONSPIRACY (Jan. 23, 2012, 1:59 PM), http://www.volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/.

[138] *See, e.g.*, *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d at 118–19; *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010).

[139] *See In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. 2d at 118 (quoting *Maynard*, 615 F.3d at 560); *In re* Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526 (D. Md. 2011); *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d at 839–40; *Maynard*, 615 F.3d at 563.

[140] United States v. Jones, 132 S. Ct. 945, 956 (Sotomayor, J., concurring).

[141] *See supra* Part III.

[142] California v. Ciraolo, 476 U.S. 207, 217 (1986) (Powell, J., dissenting); *see also Jones*, 132 S. Ct. at 956 (discussing "the Fourth Amendment's goal to curb arbitrary exercises of police power and to prevent a too permeating police surveillance.").

[143] *See supra* Part III (discussing Fourth Amendment exceptions).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

CONCLUSION

The pervasive and invasive nature of historical CSLI surveillance implicates Fourth Amendment privacy interests. As indicated in the foregoing sections, there are sufficient differences with historical CSLI to clear the hurdles imposed by the Fourth Amendment exceptions.[144] Nevertheless, there are courts that still apply the exceptions to conclude that a cell user has no reasonable expectation of privacy in historical CSLI. The root cause of these courts' decisions seems to be an adherence to the general notion imbedded within the Fourth Amendment exceptions—that secrecy is a prerequisite for privacy.[145]

This approach fails to appreciate the unique attributes of modern society where "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[146] Indeed, while CSLI may conceptually fit the paradigm of these exceptions—information is revealed to a third party and movements are exposed to the public—it also permits unparalleled intrusion, revealing drastically more intimate information than preceding surveillance techniques.[147] By applying the exceptions to historical CSLI, the government may engage in surveillance that "alter[s] the relationship between citizen and government in a way that is inimical to a democratic society," thereby contravening the purpose of the Fourth Amendment.[148] As Justice Sotomayor stated in her concurrence in *Jones*, "[a]wareness that the Government may be watching chills associational and expressive freedoms."[149]

Of course technology will always outpace the level of protection afforded by the law. However, this does not justify confining the law's protections to the evils of past decades. Courts today should embrace the spirit of Justice Brandeis dissent in *Olmstead*, where he wrote: "Clauses guaranteeing to the individual protection against specific abuses of power, must have [the capacity to adapt] to a changing

---

[144] *See supra* Part IV.

[145] *Jones*, 132 S. Ct. at 957.

[146] *Id.*

[147] *See supra* Part IV (detailing depth of intrusion created by CSLI surveillance); *see also In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 126 (E.D.N.Y. 2011) ("Applying the third-party-disclosure doctrine to cumulative cell-site-location records would permit governmental intrusion into information which is objectively recognized as highly private.").

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

[149] *Id.*

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu

world."[150] The Fourth Amendment's efficacy in the digital age depends on, more than ever, the contemplation of not only what has been but of what may be.[151] This can only happen if Fourth Amendment jurisprudence advances past the all or nothing approach to privacy rooted in the third-party and public exposure exceptions.

[150] Olmstead v. United States, 277 U.S. 438, 472 (1928) (Brandeis, J., dissenting).

[151] *See* Kylo v. United States, 533 U.S. 27, 35–36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."); *see also In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Information, 809 F. Supp. at 126; *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

Volume XIII – Spring 2013 ● ISSN 1087-6995 (print) 2164-800X (online)
DOI 10.5195/tlp.2013.120 ● http://tlp.law.pitt.edu