University of Denver Criminal Law Review

Volume 4 | Issue 1 Article 3

January 2014

Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment

R. Craig Curtis

Michael C. Gizzi

Michael J. Kittleson

Using Technology the Founders Never Dreamed of: Cell Phones as Tracking Devices and the Fourth Amendment

Keywords

Cell phones, Communications law, Criminal law, Criminals, Fourth Amendment, Law Enforcement, Police, Technology

USING TECHNOLOGY THE FOUNDERS NEVER DREAMED OF: CELL PHONES AS TRACKING DEVICES AND THE FOURTH AMENDMENT

R. Craig Curtis[*], *Michael C. Gizzi*[†], *& Michael J. Kittleson*[‡]

Abstract

This paper considers the Fourth Amendment issues surrounding warrantless surveillance by law enforcement using cell phone data to track the location of suspects and the potential application of the Supreme Court's 2012 decision in *United States v. Jones* to this behavior. The paper provides an overview of the Court's historic privacy jurisprudence from *Olmstead v. United States* to *Katz v. United States* and of the recent decisions in *Jones* and *Florida v. Jardines*. A dataset of federal and state cases in which the use of cell phones to track suspects was at issue was constructed and analyzed. At this point in time, there is no clear legal standard by which the courts can provide oversight over law enforcement in this growing area of police practice. It is suggested that the application of Justice Scalia's trespass standard will only make the problem worse and the probable cause standard adopted in five states could easily be applied to all jurisdictions without limiting police effectiveness while still providing protection for the privacy rights of Americans.

[*] Associate Professor, Department of Political Science, Bradley University, Peoria IL. Ph.D., Washington State University, 1991. M.A., Washington State University, 1987 J.D., University of the Pacific, McGeorge School of Law, 1985. B.A., Millsaps College, 1982.

[†] Associate Professor of Criminal Justice, Illinois State University. Ph.D., The University at Albany, State University of New York. 1996. A.B., Saint Michael's College, Vermont. 1990.

[‡] 2L, University of Washington School of Law. Undergraduate degrees in Political Science and Communications, Bradley University, Peoria, IL.

INTRODUCTION: IT'S 10 PM AND THE POLICE MAY ALREADY KNOW WHERE YOUR CHILDREN ARE

Back in the 1960s, some television stations would run a public service announcement just before the late evening news. A sonorous voice would intone, "It's 10 pm. Do you know where your children are?"[1] The announcement was intended to remind parents that there was a curfew in place, but now, in light of the fact that local and national law enforcement agencies are already commonly tracking the locations of people without a warrant and without individualized suspicion, these simple words from our nation's past remind us that modern technology empowers the police to do amazing things that are quite inconsistent with the notions of freedom and privacy that our founders likely had in mind when they adopted the Fourth Amendment.

The revelation in the spring of 2013 that the National Security Agency was gathering enormous amounts of data by routinely tracking cell phone and internet traffic stunned many in our nation.[2] A major lawsuit was filed by the American Civil Liberties Union against the federal government based on the fact that members' phones were flagged by the data mining algorithms employed.[3] The NSA program is just the tip of the iceberg. Police agencies in major cities already have systems in place to automatically track cars by license plate, creating databases of who was where and when.[4] Many cities have cameras,[5] although few have gone as far as London in terms of the sheer number of cameras or as far as New York in terms of centralized receipt and automated analysis of the images from these cameras.[6]

Each year, millions of requests are made by local police departments for data about cell phone customers from service providers, often without a warrant.[7] The police

---

[1] The origins of the phrase can be traced to the 1960s on the East coast. *See*, Kara Kovalchik, *The Origin of "It's 10PM. Do You Know Where Your Children Are?"* MENTAL FLOSS (June 17, 2012, 6:00 PM), http://mentalfloss.com/article/30945/origin-its-10-pm-do-you-know-where-your-children-are.

[2] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Dana Priest, *NSA Growth Fueled by Need to Target Terrorists*, WASH. POST (July 21, 2013), http://www.washingtonpost.com/world/national-security/nsa-growth-fueled-by-need-to-target-terrorists/2013/07/21/24c93cf4-f0b1-11e2-bed3-b9b6fe264871_story.html.

[3] *ACLU File Lawsuit Challenging Constitutionality of NSA Phone Spying Program*, AM. CIV. LIBERTIES UNION (June 11, 2013), https://www.aclu.org/national-security/aclu-files-lawsuit-challenging-constitutionality-nsa-phone-spying-program; *See also*, Klayman v. Obama, 957 F. Supp. 2d 1, 7 (D.D.C. 2013) (describing a case in which a private citizen sued the federal government seeking an injunction against the NSA's practices and referencing other lawsuits requesting the same relief).

[4] Catherine Crump, *You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, AM. CIV. LIBERTIES UNION, 2 (July 2013), http://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.

[5] Steve Henn, *In More Cities, A Camera On Every Corner, Park And Sidewalk*, NPR (June 20, 2013, 2:57 AM), http://www.npr.org/blogs/alltechconsidered/2013/06/20/191603369/The-Business-Of-Surveillance-Cameras.

[6] Rebecca Rosen, *London Riots, Big Brother Watches: CCTV Cameras Blanket the UK*, ATLANTIC (Aug. 9, 2011), http://www.theatlantic.com/technology/archive/2011/08/london-riots-big-brother-watches-cctv-cameras-blanket-the-uk/243356/; Robin Young & Jeremy Hobson, *NYC's Web of Cameras Can Catch Unattended Bags*, HERE & NOW (Apr. 24, 2013), http://hereandnow.wbur.org/2013/04/24/nyc-surveillance-cameras.

[7] Ellen Nakashima, *Cellphone Carriers Report Surge in Surveillance Requests From Law Enforcement*, WASH. POST (July 9, 2012), http://www.washingtonpost.com/world/national-security/cellphone-carriers-report-surge-in-surveillance-requests/2012/07/09/gJQAVk4PYW_story.html; *Cell Phone Location Tracking Public Records Request*, AM. CIV. LIBERTIES UNION (Mar. 25, 2013), http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request; David Bresnahan, *Gov't Tracking Cell Phones without*

have the ability to "ping" a phone to determine its location in real-time,[8] or to pinpoint its position through access to records of its use from the carrier.[9] This last tool is often referred to as cell site location information or CSLI.[10] CSLI can be historical or prospective. In the former, the police seek the past location of a cell phone user, either by triangulating from the cell phone towers that the phone contacted in the course of completing a call or sending a text, or from actual Global Positioning System (GPS) data from the cell phone itself.[11] Prospective, or real time, CSLI means that the police intend to use the data to track the location of the suspect currently and in the future. Sixty days is a common time period for such tracking. CSLI does not include the content of any communication emanating from the phone.

Virtually all cell phones in existence have a GPS device included so that the authorities can locate the phone in case of its use to call 911 in an emergency. "Smart" phones are capable of a number of applications and uses that depend on the use of GPS information and frequently communicate their location to cell towers. As such, such devices may be very useful to the police if they want to track a suspect who is in possession of a smart phone. While a few states do require, as a matter of state law, police to obtain a warrant before gathering this kind of information,[12] as of yet there is no clear standard established in the federal courts to determine whether the warrantless use of this technology is constitutionally permissible.

The nation is faced with practices that are highly attractive to and commonly used by police, [13] but for which there is no legal standard for judicial oversight. Most people are not aware of just how much data cell phone companies are storing and for how long.[14] This state of affairs should not be allowed to exist. The purpose of this paper is to analyze the state of the law on the meaning of the Fourth Amendment in the context of the use of data from hand held devices or the network of hardware by which they function to locate a suspect. This is independent from the question of the warrantless search of a cell phone or hand-held device incident to arrest, which the Court addressed in the 2014

Court Order, NEWS WITH VIEWS (Jan. 4, 2006, 1:00 AM), http://www.newswithviews.com/BreakingNews/breaking40.htm.

[8] *See, e.g.,* Commonwealth v. Rushing, 71 A.3d 939, 946 (Pa. Super. Ct. 2013).

[9] *See, e.g.,* United States v. Graham, 846 F. Supp. 2d 384, 391-92 (D. Md. 2012). At the time of writing, the *Graham* case was under appeal to the United States Court of Appeals, 4th Circuit. *See also*, State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

[10] *See* Commonwealth v. Wyatt, No. 2011–00693, 2012 WL 4815307, at *1-2 (Mass. Super. Ct. Aug. 7, 2012).

[11] See cases cited *infra* Parts II, IV, and V for details on CSLI capabilities.

[12] Maine and Montana have passed statutes mandating that police obtain a warrant before seeking to track a suspect using his or her cell phone. Maine, ME. REV. STAT. tit. 16, § 642 (West, Westlaw through 2013 Sess.); Montana, H.B. No. 603, 63d Reg. Sess. (2013), http://leg.mt.gov/bills/2013/billhtml/HB0603.htm (last updated Apr. 22, 2013). The New Jersey Supreme Court has ruled that a warrant is required to access locational data. State v. Earls, 70 A.3d 630, 632 (N.J. 2013). The Pennsylvania Supreme Court ruled similarly. Commonwealth v. Rushing, 71 A.3d 939, 946 (Pa. 2013). Three trial courts in Massachusetts have ruled that police must obtain a warrant before accessing CSLI. *See* Commonwealth v. Augustine, 467 Mass. 230, 244 (2014); Commonwealth v. Wyatt, No. 2011–00693, 2012 WL 4815307, at *2 (Mass. Super. Ct. Aug. 7, 2012); Commonwealth v. Pitt, No. 2010–0061, 2012 WL 927095, at *11 (Mass. Super. Ct. Feb. 23, 2012).

[13] Declan McCullagh, *Cops to Congress: We Need Logs of Americans' Text Messages*, CNET (Dec. 3, 2012, 9:00 AM), http://news.cnet.com/8301-13578_3-57556704-38/cops-to-congress-we-need-logs-of-americans-text-messages/.

[14] Allie Bohm, *How Long Is Your Cell Phone Company Hanging On To Your Data?*, AM. CIV. LIBERTIES UNION (Sept. 28, 2011, 10:17 AM), http://www.aclu.org/blog/technology-and-liberty/how-long-your-cell-phone-company-hanging-your-data; *Cell Phone Location Tracking Public Records Request*, AM. CIV. LIBERTIES UNION (last visited July 29, 2013), http://www.aclu.org/protecting-civil-liberties-digital-age/cell-phone-location-tracking-public-records-request.

Term.[15] The approach used by the current Justices of the United States Supreme Court to address issues of the use of modern electronic technology by the police will be critiqued, an exhaustive analysis of lower federal court and state court decisions will be provided, and a legal standard that would provide both protection of the privacy rights of citizens and adequate guidance to the police and the lower courts will be suggested.

Part I of this paper will trace the history of Fourth Amendment jurisprudence concerning the use of new technologies to gather information about suspects, beginning with *Olmstead v. United States*,[16] continuing through *Katz v. United States,*[17] *Smith v. Maryland*[18], *United States v. Knotts*,[19] *United States v. Karo*,[20] and *Kyllo v. United States*.[21] Part II will lay out the types of cases that have been decided by the lower courts as a way of educating the reader about common police uses of locational data. Part III will provide a detailed analysis of the three most recent Supreme Court decisions in the area of the use of technology by the police, *United States v. Jones*[22] and *Florida v. Jardines*,[23] and *Riley v. California*.[24] Part IV will explain the origins of, and the conflict between, the Scalia "trespass standard" and the Harlan "reasonable expectation of privacy standard." Part V will provide an overview and analysis of the cases to date that have considered the issue of when and under what standards may the police gain access to Cell Site Location Information. Part VI will make the case for a probable cause standard that would apply to all uses of locational data. The standard will provide clear guidance to the police, a clear and easily applied set of criteria for courts to use, and greater protection to the ordinary citizen than currently exists. In order to do so, the main point that must be addressed is the definition of "property" in this context. There must be agreement on what data the customer owns, what data are owned by the service provider, and when and how the customer can use the courts to protect these rights. The Court must transcend the traditional common law notion of property as being something tangible and capable of being owned or possessed.

PART I: TRACING THE HISTORY OF FOURTH AMENDMENT JURISPRUDENCE WITH REGARD TO THE USE OF TECHNOLOGY TO LOCATE A SUSPECT

The Supreme Court's jurisprudence in this area of police use of communication and/or surveillance technology is well known. The Court first was faced with the task of applying essentially 18th Century concepts to modern communication technology in *Olmstead v. United States* in 1928, where phone tapping was analogized to trespass.[25] Later, in 1967, the Court changed course in *Katz v. U.S.* and held that courts should apply a "reasonable expectation of privacy" standard in such cases.[26] The doctrine was applied

[15] Riley v. California, 573 U.S. ___, Nos. 13-132 and 13-212 (June 25, 2014). The sweeping language in Chief Justice Roberts' majority opinion in that case is potentially relevant to the discussion of how cell phone tracking cases may be decided and will be addressed in the Parts III, V, and VI of this paper.

[16] 277 U.S. 438, 455 (1928), *overruled by* Katz v. United States 389 U.S. 347 (1967).

[17] 389 U.S. 347, 348 (1967).

[18] 442 U.S. 735, 736 (1979).

[19] 460 U.S. 276, 277 (1983).

[20] 468 U.S. 705, 706 (1984).

[21] 533 U.S. 27, 29 (2001).

[22] 132 S. Ct. 945, 948 (2012).

[23] 133 S. Ct. 1409, 1417 (2013).

[24] Riley v. California, 573 U.S. ___, Nos. 13-132 and 13-212 (June 25, 2014).

[25] Olmstead v. United States, 277 U.S. 438, 465-66 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[26] 389 U.S. at 360-62 (1967) (Harlan, J., Concurring).

in several important cases during the time between 1967 and 2012, when *U. S. v. Jones* was decided.

In *Olmstead*, the first major case where the Court ruled on the legality of using technology to gather information on a suspect, government agents were investigating a large-scale "bootlegging" operation in the city of Seattle.[27] Federal agents, without seeking a warrant, tapped the office phone, and several home phones, of the bootleggers.[28] They placed the taps along existing phone wires without physical trespass on the office spaces or homes of the conspirators.[29] After monitoring the taps for months, extensive transcriptions of the conversations were compiled and introduced into evidence at the trial.[30] In holding that the wiretaps did not violate the Fourth Amendment, the majority focused on the lack of physical trespass by the government agents.

> The United States takes no such care of telegraph or telephone messages as of mailed sealed letters. The Amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing, and that only. There was no entry of the houses or offices of the defendants.[31]

In doing so, the majority defined a search as an intrusion of a constitutionally protected place.

> "The [Fourth] Amendment itself shows the search is to be of material things, the person, the house, his papers, his effects. The description of the warrant necessary to make the proceeding lawful is that it must specify the place to be searched and the person or things to be seized."[32]

The "trespass doctrine" placed the core value of Fourth Amendment protection on constitutionally protected places. Thus, because the wiretap was done outside of the home, there was no intrusion. The end result was that the Fourth Amendment was interpreted quite narrowly and, as interpreted, was incapable of providing guidance regarding law enforcement use of any electronic technologies, like telephones.

In dissent, Justice Brandeis foreshadowed the concerns that led the Court to overrule *Olmstead* in 1967 in *Katz v. United States.*[33] Justice Brandeis was very concerned that the trespass standard would allow the government to intrude into the private affairs of citizens in ways not yet developed.

> The progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping. Ways may someday 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.[34]

---

[27] 277 U.S. at 455-57.

[28] *Id.* at 456-57.

[29] *Id.* at 457.

[30] *Id.*

[31] *Id.* at 464.

[32] *Id.*

[33] *See id.* at 471; *See* Katz v. United States, 389 U.S. 347, 352-54 (1967).

[34] *Olmstead*, 277 U.S. at 474.

Brandeis also articulated a deeper understanding of the meaning of the Fourth Amendment. To him, the Amendment did more than just protect specific places. It served as a core element of liberty.

> The protection guaranteed by the amendments is much broader in scope. The makers of our Constitution undertook to secure conditions favorable to the pursuit of happiness. They recognized the significance of man's spiritual nature, of his feelings and of his intellect. They 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 emotions and their sensations. They conferred, as against the government, the right to be let alone — the most comprehensive of rights and the right most valued by civilized men. To protect that right, 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.[35]

Brandeis' view would remain in dissent for forty years, until the Court decided *Katz v. United States.*

The facts in the *Katz* case are also simple. Mr. Katz was part of an illegal gambling operation and was conducting that business by using a pay phone in California to talk with his partners in crime in Boston and Miami.[36] The police were aware of this and placed a listening device on the outside of the phone booth, where Katz would not see it.[37] This enabled them to listen to his side of the conversations, transcripts of which were introduced at trial.[38]

Writing for the majority, Justice Stewart took the position articulated by Justice Brandeis' dissent in *Olmstead* and viewed the Fourth Amendment as a matter of privacy, rather than trespass on private property. Stewart argued that the Fourth Amendment protects people, not places, and declared that "what a person knowingly exposes to the public, even in his home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected."[39] In doing so, Stewart explicitly acknowledged that the rationale underlying the trespass doctrine had been eroded and "can no longer be regarded as controlling."[40]

It is Justice Harlan's concurrence that fleshed out the standard or test that the Court has used to answer the question whether an activity constitutes a search: "My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[41]

---

[35] *Id.* at 478.

[36] *Katz*, 389 U.S. at 348 (1967).

[37] *Id.*

[38] *Id.*

[39] *Id.* at 351 (citation omitted).

[40] *Id.* at 353.

[41] *Id.* at 361 (Harlan, J., concurring).

In the instant case, Katz had a subjective expectation that the government would not listen in on his phone conversations, and that expectation was one that society was willing to recognize as reasonable.[42] This two prong "reasonable expectation of privacy" test has persisted to the present day, although Justice Scalia argued that it should be eliminated during the oral argument of *U.S. v. Jones*[43] and he did not rely on it in either the *Jones* or *Jardines* decisions.[44] Until 2012, it was commonly understood that Justice Stewart's opinion in *Katz* over-ruled the trespass doctrine, but as we will see below, Justice Scalia has revived it in his two majority opinions in *Jones* and *Jardines.*

The *Katz* reasonable expectation of privacy doctrine was applied in several important cases during the time since 1967. These cases, oft cited by the lower courts in attempting to come to grips with challenges to the use of cell phone data, include the 1979 case of *Smith v. Maryland*,[45] the 1983 case of *U. S. v. Knotts*,[46] the 1984 case of *U. S. v. Karo*,[47] and the 2001 case of *Kyllo v. U. S.*[48] With few exceptions, such as *Kyllo,* the Court has generally ruled against individual privacy claims.[49]

Most relevant to cell phone location surveillance are the Court's decisions in *Smith v. Maryland, U.S. v. Knotts,* and *U.S. v. Karo. Smith* involved the use of a pen register device to capture the phone numbers called by the phone in question.[50] No warrant was issued to justify the use of the device.[51] The Court held that there is no legitimate expectation of privacy in the numbers one calls from a telephone on the basis that these numbers are voluntarily provided by the user to the phone company which keeps the records in the normal course of its business.[52] This idea that such information is voluntarily provided by the phone user and kept by the service provider for its own legitimate business purposes plays a large role in the thinking of a number of judges faced with the need to decide whether the Fourth Amendment protects cell phone subscribers who do not wish for the authorities to use locational data stored by cell phone service providers.[53]

For those judges who did attempt to wrestle with the Fourth Amendment's meaning in the context of the use of CSLI, there are numerous citations to both *U.S. v. Knotts*[54] and *U. S. v. Karo*.[55] Both cases involved the placement of beepers on personal property and the monitoring of those beepers to determine the location of the property. In *Knotts*, the beeper was placed in a container of chloroform upon request by the police to

---

[42] *Id.* at 360-361.

[43] Transcript of Oral Argument at 6-7, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259).

[44] *Jones*, 132 S. Ct. at 950; Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

[45] 442 U.S. 735, 738-41 (1979).

[46] 460 U.S. 276, 283 (1983) (discussing privacy expectation with phones).

[47] 468 U.S. 705, 726 (1984).

[48] 533 U.S. 27, 33 (2001).

[49] *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 91 (1998) (holding defendants did not have a legitimate expectation of privacy).

[50] 442 U.S. at 737.

[51] *Id.*

[52] *Id.* at 745-46.

[53] *See, e.g., In re* Application of the United States of America for Historical Cell Site Data, 724 F.3d 600, 611-12 (5th Cir. 2013).

[54] *See, e.g.*, United States v. Caraballo, 934 F. Supp. 2d 341, 354-56 (D. Vt. 2013) (citing United States v. Knotts, 460 U.S. 276 (1983)).

[55] *See, e.g., Caraballo*, 934 F. Supp. 2d at 354-56 (citing United States v. Karo, 468 U.S. 705 (1984)).

the private company that sold the chemical to the defendants.[56] The request had been made because the police believed the defendants were making illegal drugs.[57] The police used the beeper to follow the transport of the chemical to a remote cabin in the woods in Wisconsin.[58] After three days of watching the cabin, the police obtained a search warrant and found a drug lab in operation in the cabin.[59] In refusing to suppress the evidence derived from the use of the beeper, Justice Rehnquist wrote that the beeper served as nothing more than an enhancement of the police ability to follow the car while it was on a public thoroughfare.[60] In essence, the Court ruled that one has no reasonable expectation of privacy while on public streets because one can be observed by anyone, including the police, who happen to be on the same street.

U. S. v. Karo[61] was decided during the next Term and also involved the use of a beeper. Once again, the police suspected the defendants of using bulk chemicals to make illegal drugs and had a beeper placed in a container of ether that the defendants were planning to use to manufacture cocaine.[62] The Court, per Justice White, upheld the conviction, but did hold that the monitoring of the beeper while the container was inside a private residence would violate the Fourth Amendment.[63] Taken together, *Knotts* and *Karo* stand for the proposition that the government may use technology that enhances the senses to improve their ability to conduct surveillance in public areas without any restrictions, but to use such technology to search a private space, such as a home, would require a warrant based on probable cause.

This distinction between the type of privacy protection that one has in the home and the ones that one does not have when in a public space would be important in the decision of the last of the major cases before the 2012 *U. S. v. Jones* case, *Kyllo v. U. S.*[64] In *Kyllo* the police were using a thermal imaging camera to scan the defendant's home after becoming suspicious that he was growing marijuana.[65] The police were looking for a heat signature consistent with the use of grow lamps.[66] In overturning this search, the Court, per Justice Scalia, held that this was the type of intrusion into the home that was forbidden by the Fourth Amendment.[67] Despite expressly stating that Fourth Amendment analysis was no longer tied to any Common Law concept of trespass,[68] and despite his open acceptance of Justice Harlan's reasonable expectation of privacy standard,[69] Justice Scalia was adamant that the Fourth Amendment must protect the home from the use of technology that allows the police to gather information that could not be gathered with the unaided senses of the officers.[70]

---

[56] 460 U.S. at 277.

[57] *Id.* at 278.

[58] *Id.*

[59] *Id.* at 279.

[60] *Id.* at 285.

[61] 468 U.S. 705, 708 (1984).

[62] *Id.* at 708.

[63] *Id.* at 716.

[64] Kyllo v. United States, 533 U.S. 27, 32-33 (2001).

[65] *Id.* at 29.

[66] *Id.*

[67] *Id.* at 40.

[68] *Id.* at 32 ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property.").

[69] *Id.* at 33.

[70] *Id.* at 34.

PART II: WHAT KINDS OF CASES GIVE RISE TO CHALLENGES TO THE USE OF LOCATIONAL DATA?

There are a small but growing number of federal and state court cases in which criminal defendants are challenging the use of locational data obtained from cell phone service providers. In the federal practice, these cases often have cumbersome sounding names like *In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and Trap and Trace Device*.[71] Judges faced with deciding such cases do not have the benefit of clear guidance with regard to the standard of review, so they tend to provide a recitation of existing cases in their opinions.[72] Two important federal cases in this area are *United States v. Graham*,[73] appeal of which is currently pending in the United States Court of Appeals for the Fourth Circuit, and *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*,[74] decided in 2010 by the Third Circuit. Cases in state court have also contributed to this area of jurisprudence and in three states courts have held that their state constitutions provide greater protection for suspects than the Fourth Amendment.[75]

The 2010 Third Circuit case originated when federal law enforcement officers, investigating a suspected drug trafficker, asked a federal magistrate in Pennsylvania for an order under section 2703(d) of the Stored Communication Act directing a cell phone service provider to disclose CSLI data on the suspect.[76] The magistrate refused to grant the request on the grounds that the statute did not authorize the seizure of information to be used to track a suspect.[77] The district court judge affirmed the magistrate's decision, but the Third Circuit overturned it. The rationale for doing so hinged more on an understanding of the Stored Communications Act than on an interpretation of the Fourth Amendment itself.[78] The Court held that the statute itself does not mandate a finding of probable cause, the usual standard for determining whether to issue a warrant, but that a federal magistrate, in his or her discretion, could use that standard in determining whether to grant the warrant.[79] In doing so, they largely avoided the Fourth Amendment issue.

United States v. Graham stems from a criminal charge against two men involved in a string of burglaries in Baltimore, Maryland, in 2011.[80] The two defendants were arrested for burglarizing two fast food restaurants.[81] Their cell phones were seized and

---

[71] *E.g., In re* the Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d) to Disclose Subscriber Info. & Cell Site Info., 849 F. Supp. 2d 177 (D. Mass. 2012).

[72] *See, e.g.*, Commonwealth v. Rushing, 71 A.3d 939, 950 (Pa. Super. Ct. 2013).

[73] 846 F. Supp. 2d 384, 389 (D. Md. 2012), *appeal filed,* No. 12-4659, (4th Cir. 2012), *available at* http://dockets.justia.com/docket/circuit-courts/ca4/12-4659.

[74] 620 F.3d 304, 305 (3d Cir. 2010).

[75] State v. Earls, 70 A.3d 630, 642-44 (N.J. 2013); Commonwealth v. Rushing, A.3d 939, 961 (Pa. Super. Ct. 2013); Commonwealth v. Wyatt, 2012 WL 4815307 at *6-8 (Mass. Super. Ct. Aug. 7, 2012).

[76] *In re* the Application of the United States Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 306 (3d. Cir 2010) (citing *In re* the Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 588-89 (W.D. Pa. 2008)).

[77] *Id.* at 308.

[78] *See id.* at 315.

[79] *Id.*

[80] 846 F. Supp. 2d 384, 385-87 (D. Md. 2012).

[81] *Id.* at 385-386.

searched and the police became convinced that these two men were responsible for a series of burglaries that preceded the incidents for which they were arrested.[82] The police sought a total of 221 days of CSLI data, under the aegis of the Stored Communications Act.[83] This request was granted and Sprint/Nextel complied with the order.[84] The defendants objected, among other things, to the long length of time that the police sought to track their movements.[85] The trial court likened the records from the cell phone provider to any other business record, essentially using the doctrine laid out in *Smith v. Maryland, which* held that there is no expectation of privacy in the phone numbers one dialed.[86] In doing so, the court tied the analysis to a personal property concept more appropriately suited to paper documents, citing a series of other federal trial court decisions.[87] Once the court decided to treat cell phone records as ordinary business records, it was easy for it to rule in favor of the police. In essence, the decision to treat the locational data as a business record allowed the court to avoid the Fourth Amendment issue and rely solely on the lower statutory standard of "specific and articulable facts" that is provided in the Stored Communications Act.[88]

In contrast to the cases in the federal courts, courts in three states, including one state supreme court, have made clear statements that their state constitutions provide greater privacy protection than the Fourth Amendment when it comes to the use of cell phones to track suspects. The first of these cases is *Pennsylvania v. Rushing.* After responding to the scene of a horrific multiple murder, the police learned that the suspect was still at large and had professed the intention to commit further violence.[89] They sought and received a court order to "ping" the suspect's cell phone, and using the data along with the GPS unit in the phone itself, were able to locate and apprehend the suspect without his committing any further acts of violence.[90] The judge granted the order based on the "specific and articulable facts" standard stated in the then applicable version of the Pennsylvania Wiretap Act.[91] The suspect argued for exclusion of evidence based on the theory that the order to "ping" his cell phone should only have been issued if there was probable cause.[92] Pennsylvania Superior Court Justice Bowles' opinion in the case is very detailed and carefully crafted because "[t]he . . . issue Appellant levels on appeal presents a matter of first impression in this Commonwealth, although the federal courts have addressed the question with conflicting results."[93] The court ruled that, under Pennsylvania law, the standard of review to be followed in considering a request for locational data is probable cause.[94] This reasoning was based in part on Pennsylvania statutes, but the court stated that the Pennsylvania constitution creates greater protections for privacy than the Fourth Amendment.[95] As such, under Pennsylvania law, citizens have

[82] *Id.* at 386.
[83] *Id.* at 387.
[84] *Id.*
[85] *Id.*
[86] *Id.* at 389; Smith v. Maryland, 442 U.S. 735, 745 (1979).
[87] *Graham*, 846 F. Supp. 2d at 389.
[88] 18 U.S.C.A. § 2703(d) (West, Westlaw through 2009 sess.).
[89] Commonwealth v. Rushing, 71 A.3d 939, 946 (Pa. Super. Ct. 2013).
[90] *Id.*
[91] *Id.* at 954.
[92] *Id.* at 947.
[93] *Id.* at 954.
[94] *Id.* at 963.
[95] *Id.* at 954.

a reasonable expectation of privacy in the data contained in their cell phone records.[96] It was also made clear that the combination of probable cause and exigent circumstances, which existed in this case, was sufficient to justify a warrantless search of cell phone records for locational data.[97] The opinion is very thorough in terms of addressing the details of how triangulation is used to locate suspect as well as providing citations to, and explanations of, many federal and state cases and statutes.

The second state court case, *State v. Earls*,[98] arose in New Jersey. In that case, the Middletown Township Police were investigating a string of burglaries and had located one of the conspirators who had provided useful evidence.[99] This informant was believed to be at risk of harm from her partner in crime and the police, knowing the cell phone number of the suspect and knowing that he was using a cell phone from T-Mobile, asked T-Mobile to provide locational data, which they did.[100] No warrant was ever sought.[101] The New Jersey Supreme Court ruled unanimously that Article 1, Paragraph 7, of the New Jersey State Constitution gives a person a protected privacy interest in the location of his or her cell phone.[102] This means that the police must seek a warrant from a neutral magistrate based on probable cause before they can obtain locational data from a cell phone provider. As with the decision in *Pennsylvania v. Rushing*, the New Jersey Supreme Court was careful to fully analyze the Fourth Amendment issue and yet base their decision squarely in state law. Also, in agreement with the Pennsylvania courts, the New Jersey Supreme Court was careful to protect the interests of law enforcement by stating that probable cause and exigent circumstances would be sufficient to justify a warrantless search, i.e., a direct appeal to a cell phone company for data.[103] Lastly, the New Jersey Supreme Court limited its decision to prospective effect only, meaning that older cases with similar fact patterns would not be revisited or re-opened.[104]

In the State of Massachusetts, five cases have dealt with issues of the use of CSLI. Three ruled in favor of the defendant and two in favor of the state. *Commonwealth v. Wyatt* and *Commonwealth v. Augustine* ruled explicitly that the Massachusetts constitution provides for greater privacy protection than the Fourth Amendment in such cases and that the police must obtain a warrant based on probable cause to access CSLI.[105] In contrast, *Commonwealth v. Pitt* ruled that the Fourth Amendment itself requires a warrant based on a showing or probable cause before the police may use a cell phone to locate a suspect.[106] *Commonwealth v. Princiotta* ruled that that since the phone in question was not the suspect's phone, he lacked standing to challenge data from that account.[107] Similarly, *Commonwealth v. Willis*, held that the defendant lacked standing to challenge the use of CSLI since it was her who had called 911 and the evidence in question concerned the location of her phone when she made that call.[108] Of the cases wherein there

---

[96] *Id.* at 963.

[97] *Id.* at 965-66.

[98] 70 A.3d 630 (N.J. 2013).

[99] *Id.* at 633.

[100] *Id.*

[101] *Id.* at 634.

[102] *Id.* at 644.

[103] *See id.*

[104] *Id.* at 645.

[105] *See* Commonwealth v. Augustine, 467 Mass. 230, 244 (Mass. 2014); *See also* Commonwealth v. Wyatt, No. 2011-00693, 2012 WL 4815307, at *6 (Mass. Super. Ct. Aug. 7, 2012).

[106] No. NOCV2010-00061, 2012 Mass. Super. LEXIS 39, at *31 (Feb. 23, 2012).

[107] 31 Mass. L. Rptr. 68, 9 (Mass. Super. Ct. 2013).

[108] No. SUCR2012-10180, 2013 Mass. Super. LEXIS 114, at *6 (Mar. 8, 2013).

was a clear privacy issue raised by the facts, the Massachusetts courts have ruled that this privacy issue must be resolved in favor of a warrant requirement for the use of CSLI.[109]

In Florida, where the case of *Tracey v. State* is, at the time of this writing, pending before the Florida Supreme Court, the lower courts have ruled that there is no expectation of privacy when the search only concerns the location of a suspect while he is on the public roads.[110] In that case, the sheriff's deputy who applied for the order to access CSLI relied solely on an unsupported statement from a federal agent.[111] The appellate court held that granting the order violated the state statutes that authorize access to CSLI, but the lower court held that exclusion of evidence is not an available remedy under those statutes.[112] The opinion contained language that indicated that the court was sympathetic to the notion that cell phone users do not voluntarily and knowingly convey locational data when they possess a cell phone.[113] That the facts involve an overreach by the police could be meaningful when the Florida Supreme Court makes its decision.

In each of these cases, the authorities wanted to obtain information from a cell phone service provider to find the location of a suspect. In none of these instances was there probable cause to justify the issuance of a search warrant. In most of the cases, the state relied on statutory provisions that purport to allow a court to issue a subpoena to a cell phone service provider based on less than a probable cause standard. In some cases, the authorities simply requested data from the cell phone service providers and the request was granted without any court supervision at all.[114] These cases also show the different approaches taken by state courts, many of which base their decisions on state constitutional provisions, and federal courts, that tend to apply the Fourth Amendment or applicable statutes.

PART III: *UNITED STATES V. JONES* AND *FLORIDA V. JARDINES*, AND *RILEY V. CALIFORNIA*

Until the 2012 decision in *U. S. v. Jones*,[115] the legal standard for adjudicating claims of violations of the Fourth Amendment was clear, if not particularly predictable in terms of outcome when applied to actual cases. Justice Harlan's famous two-prong test was uniformly applied, even by Justice Scalia himself, to determine whether a search was valid.[116] *Jones* sent ripples throughout the legal and law enforcement community, not only because it placed limits on a technological tool that was coming into widespread use, but because the outcome was unanimous, and all nine justices agreed that a warrant was

---

[109] *See, e.g.*, *Pitt*, 2012 Mass. Super. LEXIS 39, at *31.

[110] Tracey v. Florida, 69 So. 3d 992, 993, 999-1000 (Fla. Dist. Ct. App. 2011), *appeal docketed*, No. SC11-2254, 2013 Fla. LEXIS 215 (Fla. Jan. 28, 2013).

[111] *Id.* at 993.

[112] *Id.* at 999-1000.

[113] *See id.* at 996 ("We acknowledge that a compelling argument can be made that CSLI falls within a legitimate expectation of privacy."); *See also id.* ("Technology evolves faster than the law can keep up, extending the search capabilities of law enforcement and transforming our concept of privacy.").

[114] See *U.S. v. Caraballo*, 963 F. Supp. 2d 341, 346 (D. Vt. 2013), for an example of when a court order made mention of a Sprint corporate procedure for requests for emergency release of such information; In other cases, it is clear that there was no court order, or none was offered by the prosecution. *See, e.g.*, State v. Earls, 70 A.3d 630, 633 (N.J. 2013); People v. Fernandez, 2011 Cal. App. Unpub. LEXIS 1931, at *6-7 (Mar. 16, 2011); Devega v. State, 689 S.E.2d 293, 299 (Ga. 2010).

[115] 132 S. Ct. 945 (2012).

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

needed, even though the justices were divided as to why.[117] To legal scholars the case raised numerous questions due to Justice Scalia's attempt to return to the long-discarded trespass doctrine while distancing the decision from the reasonable expectation of privacy standard.[118] Justice Sotomayor's concurrence is also important in that she criticized the third party doctrine that results from the application of *Smith v. Maryland*[119] to CSLI cases and she seemingly embraced the mosaic approach to the Fourth Amendment.[120]

The facts of the *Jones* case are fairly well known, even if the actual path of the case traced through the court system was convoluted and lengthy.[121] The police in the District of Columbia obtained a warrant that would allow them to place a GPS Device on a car being used by Jones.[122] The warrant allowed for the device to be placed within a ten day window.[123] It was placed on day 11, and the attachment of the device occurred in Maryland in a public parking lot.[124] Thus, the Court treated the case as if the placement of the GPS was warrantless.[125] Twenty-eight days of data were gathered and these data were used at trial to convict Jones of conspiracy to traffic in illegal drugs.[126]

Five of the Justices, led by Justice Scalia, seized on the fact that the device was placed on the car without a valid warrant.[127] In Scalia's opinion, this action constituted a trespass at common law and this was sufficient to taint the placement of the device and all evidence subsequently derived from the use of the device.[128] The other four Justices who signed the majority opinion agreed that the placement of the device was tainted, but could not all agree on Justice Scalia's trespass rationale. Justice Sotomayor agreed that the warrantless placement of the GPS device was enough to invalidate the search, and joined the majority on that basis, but wrote separately to reject Scalia's new trespass standard.[129] In her concurrence, Sotomayor applied the reasonable expectation of privacy test to hold

---

[117] The Court determined that it need not address the government's contention that Jones had no reasonable expectation of privacy and therefore there was no search "because Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation." *See Jones*, 132 S. Ct. at 950. Justice Sotomayor discusses the test that she would apply to cases of GPS monitoring given "some of the unique attributes of GPS surveillance relevant to the *Katz* analysis [which] will require particular attention." *Id.* at 955-56 (Sotomayor, J., Concurring). Justice Alito states that he would analyze the issue by asking whether the long-term monitoring of the moments of the vehicle that Jones drove violated his reasonable expectations of privacy. *Id.* at 958 (Alito, J., Concurring).

[118] *See id.* at 950-52.

[119] *See id.* at 957 (Sotomayor, J., Concurring) ("[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."); *See also* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[120] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., Concurring); *See* Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 327-28 (2012); See, also *Commonwealth v. Augustine*, Criminal Action 11-10748, 2013 WL 5612574, at *5-7 (Mass. Super. Apr. 3, 2013), vacated and remanded on other grounds by *Commonwealth v. Augustine*, 467 Mass. 230, 244 (2014), wherein the lower court expressly adopted the mosaic theory.

[121] There were two trials. *See Jones*, 132 S. Ct. at 948. The first ended in a hung jury. *Id.* There was an appeal to the United States Court of Appeals for the District of Columbia Circuit. *Id.* at 949. The Supreme Court vacated Jones' conviction. United States v. Jones, 908 F. Supp. 2d 203, 204 (D.D.C. 2012). Proceedings on remand included a hearing on a motion to suppress 120 days of CSLI. *See Jones* 908 F. Supp. 2d at 205.

[122] *Jones*, 132 S. Ct. at 948.

[123] *Id.*

[124] *Id.*

[125] *Id.* at 949 (setting out procedural posture).

[126] *See id.* at 948-49.

[127] *Id.* at 949.

[128] *See id.*

[129] *Id.* at 954-57.

that tracking the whereabouts of a person over time was not a reasonable search.[130] For her, and for the four Justices who signed Justice Alito's concurring opinion, the proper test is the reasonable expectation of privacy test.[131]

Justice Sotomayor also wrote that it is perhaps time to reconsider the third party doctrine of *Smith v. Maryland*, arguing that it is "ill suited to the digital age"[132] and expressly mentioned the fact that cell phone users routinely and automatically convey information to their providers in the course of using the phone.[133] This item of *dicta* is especially significant when attempting to decide petitions for court order to release CSLI. Some commentators interpreting the *Jones* decision have argued that taken together, the Sotomayor and Alito concurring opinions create something called the "mosaic" theory of the Fourth Amendment.[134] This approach involves taking the entire set of official behaviors in a holistic way, as opposed to examining each action taken by the government in a sequential way.[135] This type of reasoning has potential for application to cell phone tracking cases since it seemingly would allow for the context in which cell phone data are gathered to be considered free from the constraints of the third party doctrine.

Despite the lack of five votes for his new, and old, trespass standard, it was also applied to decide the case of *Florida v. Jardines*.[136] Police suspected Joelis Jardines of keeping illegal drugs inside his home and brought a K-9 unit to the defendant's front porch.[137] After the drug-sniffing dog indicated to officers that there were narcotics inside the house, they obtained a warrant using that information as part of the presentation to the judge.[138] Upon execution of the warrant, officers seized marijuana plants from inside the home.[139] Justice Scalia, writing for the majority, held that because the officers brought the drug-sniffing dog physically onto the defendant's porch, they were invading the province of his home and consequently searching it.[140] But the court did not explain why it should make a difference, for Fourth Amendment purposes, that the drug-sniffing dog had to be on the defendant's porch in order to smell the plants as opposed to detecting them from the street. Scalia's application of the trespass doctrine was particularly interesting, given the similarities in *Jardines* to the *Kyllo* thermal vision imaging case from a decade earlier, where Scalia's majority opinion relied on the reasonable expectation of privacy in one's home to disallow warrantless thermal imaging of the home.

The development of a new trespass doctrine, in effect, resurrecting *Olmstead*, while at the same time leaving the *Katz* reasonable expectation of privacy standard in place, has injected confusion and uncertainty to the Fourth Amendment. The ruling in *Riley v. California,* issued in June of 2014, did little to resolve this confusion.[141] The opinion actually decided two cases in which the police had seized a cellular phone from a suspect

---

[130] *Id.* at 956.
[131] *Id.* at 956-57, 64.
[132] *Id.* at 957.
[133] *Id.*
[134] Kerr, *supra* note 120, at 313-14.
[135] *Id.* at 314.
[136] 133 S. Ct. 1409, 1417 (2013).
[137] *Id.* at 1413.
[138] *Id.*
[139] *Id.*
[140] *Id.* at 1417-18.
[141] Riley v. California, 573 U.S. ___, Nos. 13-132 and 13-212 (June 25, 2014).

as part of a search incident to arrest.[142] In both cases, the police had proceeded to search the contents of the phone and used that evidence against the defendants in their trials.[143]

The opinion in the *Riley* case was written by Chief Justice Roberts, with only a special concurrence by Justice Alito preventing a unanimous Court. The opinion shows that the justices have educated themselves about cell phone technology, something that was long overdue given the famous reluctance of the justices to embrace information technology.[144] The court in several places expressly stated that cellular phones are fundamentally different than other types of personal property that is commonly discovered in a search incident to arrest because of the comprehensive nature of the information stored on these devices:

> Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.[145]

Additionally, the Court made it clear that cell phones can store all sorts of sensitive personal information as well as provide access to information stored in browser histories or stored in the cloud.

> Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. [146]

Lastly, concerning locations, the Court was quick to note that cell phones do allow the police to discover where a person has been with great detail.

> Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.[147]

Because of the concern for the huge amount of private data that can be accessed whenever the police seize a cellular phone, the Court held that the police must obtain a warrant before searching the information on the phone. The court even went so far as to suggest strategies for protecting evidence by securing the phone against remote wiping or data encryption.[148] It should be noted that the opinion in *Riley* did not apply Justice

---

[142] The second case was United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), cert granted, 134 S. Ct. 999 (2014).
[143] The Riley case involved as smart phone, and images and video from the phone were used as evidence. The phone in Wurie was an older flip phone, which was used to determine the location of the suspect's home and to justify a warrant to search that home.
[144] Will Oremus, *Elena Kagan Admits that Justices Haven't Quite figured Out E-Mail Yet*, (August 20, 2013, 3:33 pm), Future Tense, http://www.slate.com/blogs/future_tense/2013/08/20/elena_kagan_supreme_court_justices_haven_t_gotten_to_email_use_paper_memos.html (last visited, June 24, 2014).
[145] 573 U.S. ___, Nos. 13-132 and 13-212, slip op. at 20-21 (June 25, 2014).
[146] *Id.* at *19.
[147] *Id.* at *19-20.
[148] *Id.* at *12-14.

Scalia's trespass doctrine. The case was decided based on analysis of the two prongs, officer safety and preventing destruction of evidence, laid out in *Chimel v. California*.[149]

PART IV: DIFFICULTIES IN APPLYING AND MIXING THE TRESPASS DOCTRINE OF *JONES* AND THE REASONABLE EXPECTATION OF PRIVACY TEST FROM *KATZ*

Both standards used by the Supreme Court thus far in determining whether a search or seizure has taken place, the trespass standard and the reasonable expectation of privacy standard, have flaws, especially the former. Applying them to the modern world creates problems and complications they were not designed to address. The trespass doctrine cannot coherently address situations created by today's technology, and despite decades of jurisprudence, the reasonable expectation of privacy standard remains malleable and difficult for law enforcement to use. Applying the trespass doctrine is becoming increasingly arbitrary, as shown in the two drug sniffing dog cases that have been decided recently, *Florida v. Jardines*[150] and *Illinois v. Caballes*.[151] Further complicating this area of jurisprudence is an emerging patchwork of state constitutional provisions mimicking the Fourth Amendment, yet often providing a higher level of protection of individual rights.[152] All of these factors further muddy the water for law enforcement officers, judges, and ordinary citizens trying to determine what constitutes a violation of the rights of a suspect.

The trespass doctrine has its roots in originalism, an approach to constitutional analysis that seeks to understand what the Constitution meant at the time the provision in question was written when construing its meaning today.[153] According to originalists like Justice Scalia, the Fourth Amendment was only meant to protect physical spaces.[154] Hence a suspect's Fourth Amendment rights are not implicated unless the government has physically trespassed onto the suspect's property. This was the rationale for deciding not to suppress evidence obtained from listening devices attached to the phone lines of suspects in *Olmstead v, United States*.[155] The Court held that no search or seizure took place because there was no physical entry into the suspect's homes or office.[156] This outcome foreshadowed the problems the trespass doctrine would encounter in the future. Justice Brandeis, in dissent, was quite specific – even prophetic – in wondering what new technological developments would mean in this area of the law.[157]

As Justice Brandeis suggested, the application of the trespass doctrine is ill-suited for modern technological problems that complicate Fourth Amendment issues.[158] Physical

---

[149] 395 U.S. 752 (1969).

[150] 133 S. Ct. at 1413.

[151] 543 U.S. 405, 406-407 (2005).

[152] *See, e.g.*, Commonwealth v. Rushing, 71 A.3d 939, 954-55 (Pa. Super. Ct. 2013); *See* State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

[153] *See* United States v. Jones, 123 S. Ct. 945, 949-50 (2012) (describing the relationship between trespass and the Fourth Amendment); *See* Jack N. Rakove, *Joe the Ploughman Reads the Constitution, or, the Poverty of Public Meaning Originalism*, 48 SAN DIEGO L. REV. 575, 578 (2011) (describing the constitutional interpretation method of Originalism).

[154] *See Jones*, 123 S. Ct. at 949-50; *See* Richard H. Seamon, *Kyllo v. United States and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013, 1018 (2001).

[155] 277 U.S. 438, 465-66 (1928).

[156] *Id.* at 466.

[157] *Id.* at 474 (Brandeis, J., dissenting).

[158] *See id.*

intrusion is often unnecessary for law enforcement to track suspects. Tracking a suspect by pinging a cell phone or by obtaining CSLI from a cell phone service provider gives law enforcement the ability to record the suspect's movements over a period of time, and in private spaces, but without any physical intrusion on the suspect's person, property, or home. Situations like these seem to run contrary to Justice Scalia's announced purpose of "preserv[ing] . . . that degree of privacy against government that existed when the Fourth Amendment was adopted,"[159] before the government had the ability to gather such extensive information about its citizens without physically searching them or their effects.

The inadequacy of the trespass doctrine to grapple with modern technology can lead to arbitrary results. This discrepancy is illustrated in *Florida v. Jardines*.[160] Surely the act of sending the dog to investigate the defendant's home in the first place was of more consequence than how far away it was when it inhaled. And *Jardines* only demonstrates the complexities of applying the trespass doctrine to search and seizure cases *without* the complications added by modern technology. Imagine the difficulty in applying the trespass doctrine to a similar situation where, instead of a dog, piece of equipment such as a drone, or a satellite is sent to investigate a suspect. We already know, from *California v. Cirallo*, and *Florida v. Riley*, that over flights by manned aircraft in search of marijuana growing activities do not violate the Fourth Amendment so long as they occur in commercial air space.[161] We also know that the use of a thermal imaging device is not allowed on the grounds that it is a type of technology not in general use by the public.[162] Would the suspect care more about whether the drone was in public air space, or the availability of a device to the general public, or the fact that his every move inside the privacy of his own home is being recorded? The trespass doctrine could allow such intrusions, which is why it is ill-equipped to answer such questions. There is simply no viable reason why a home should be constitutionally protected from a dog or a thermal imaging camera, but not a drone.[163]

The combination of a trespass doctrine with the reasonable expectation of privacy standard[164] provides another layer of complications. *Jones* revived the trespass doctrine despite the fact that it was replaced in *Katz* with the reasonable expectation of privacy standard.[165] In *Jones*, Justice Scalia explained that "the *Katz* reasonable expectation of privacy test has been *added to*, not *substituted for*, the common law trespassory test."[166] But the two can often conflict. How to define a reasonable expectation of privacy is largely dependent upon judges and juries, which are in turn influenced by societal norms.

---

[159] *Jones*, 132 S. Ct. at 950 (quoting Kyllo v. United States, 533 U.S. 27, 28 (2001)).

[160] *See* 133 S. Ct. 1409, 1417 (2013) (describing an application of the trespass doctrine).

[161] California v. Ciraolo, 476 U.S. 207, 215 (1986); Florida v. Riley, 488 U.S. 445, 451-52 (1989).

[162] Kyllo v. United States, 533 U.S. 27, 34-35 (2001).

[163] Further complicating the application of the trespass doctrine are cases like *Illinois v. Caballes*, 543 U.S. 405 (2005), that *Jones* did not overrule but seemingly add wrinkles to the doctrine's application. There the defendant was stopped for speeding and officers had a drug-sniffing dog inspect his car without any indication of the presence of narcotics. *Id.* at 406. There was in fact marijuana in the car, but the Court held that the inspection was not a search for Fourth Amendment purposes because the defendant had no legitimate expectation of privacy in contraband. *Id.* at 408-09. The Court reasoned that only where such inspections have the capability to detect lawful activity is the Fourth Amendment implicated, and the drug-sniffing dog could only detect contraband. *Id.* at 409. Although the search in *Jardines* arguably had such capability, as the officers could have peered into a window from the defendant's porch, at minimum, *Caballes* obscures the trespass doctrine and makes its application even more difficult.

[164] *Jones*, 132 S. Ct. at 950, 953.

[165] *See* Katz v. United States, 389 U.S. 347, 351 (1967) (declaring that the Fourth Amendment protects people, not places).

[166] 132 S. Ct. at 952.

The invasions of privacy that are considered reasonable can change with the times and indeed, with changes in technology. As applied in *Katz*, the reasonable expectation of privacy standard depends on the difference between "what a person knowingly exposes to the public," which is not given Fourth Amendment protection, versus "what he seeks to preserve as private, even in an area accessible to the public," which may be protected.[167] The reasonable expectation of privacy standard evolves over time. It is also quite subjective. What one set of justices views as reasonable may change as the Court's membership changes and as the common uses to which a technology is put changes over time. Thus, Justice Sotomayor's concerns about re-thinking what is a reasonable expectation of privacy regarding phone calls and bank records. The trespass doctrine, on the other hand, is not so malleable. The definition of "physical invasion" does not change with a suspect's desire to preserve her privacy. The trespass doctrine is essentially stuck in the past: government actions that were considered physical invasions in the founding era are still viewed as such today. This tension was revealed in *Katz* itself, where the Court declared that a search had taken place when law enforcement eavesdropped on calls the defendant made from a phone booth.[168] Today, a well-placed camera or listening device need not even be physically near a phone booth to record the defendant's conversation. Under the reasonable expectation of privacy standard, such listening would violate the suspect's expectation of privacy. But under the trespass doctrine, such a search could be considered legitimate because the government did not physically intrude into the phone booth. The *Jones* majority does not adequately address this dilemma or explain how to apply the two tests together when each points to a different outcome.

It should be acknowledged that the reasonable expectation of privacy standard does not provide a spotless alternative. That standard, espoused in *Katz*,[169] was strongly calculated to rebut the holding in *Olmstead* that the Fourth Amendment protects only places.[170] Instead of being based on a physical/non-physical distinction, the reasonable expectation of privacy standard changes with society, and the defendant's, expectations.[171] Precisely because of its ability to change with societal expectations, it is inconsistent in application. Different judges and juries come to different conclusions about what is reasonable, which will likely produce conflicting precedents on a regular basis.[172] In addition, such uncertainty provides imperfect guidance for law enforcement officers who must apply the doctrine in real time and should (ideally) be able to reasonably predict the outcome of doing so. When a faulty search might lead to the acquittal of a guilty party, such foreseeability is extremely important.

A further complication is that the privacy expectations of cell phone users are unclear. While the data on how Americans feel about the National Security Agency's interceptions of cell phone and internet traffic data are mixed,[173] to apply a trespass

---

[167] 389 U.S. at 351.

[168] *Id.* at 353.

[169] *Id.* at 351.

[170] *Id.* at 351-54 (declaring that the Fourth Amendment protects people, not places).

[171] *See id.* ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

[172] The changes in the precision by which triangulation location can be accomplished using CSLI have caused changes in the way that such cases are judged. *Compare In re* Application of the U.S. for an Order for Disclosure of Telecomms. Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005), *with In re* Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 837 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

[173] *Majority say NSA tracking of phone records "acceptable" – Washington Post-Pew Research Center poll*, WASH. POST (June 10, 2013), http://www.washingtonpost.com/page/2010-

standard is to rule that there is no reasonable expectation of privacy in any data generated by the use of a cellular phone and stored in the databases of the service provider. The trespass standard does not construe such data as important since no trespass on any property or effect of the suspect need occur for the police to access those data. In fact, it is not clear at all that a suspect would have any protected interest at all in data held by the cell service provider. While there has been no case explicitly on the issue of who owns such data, the opinion in *New York v. Harris* reports that the trial court in that case ruled that the defendant had no standing to challenge a subpoena directed to Twitter that ordered the production of tweets written by the defendant and stored in Twitter's database.[174] Thus, the use of a trespass standard effectively allows the police to access any data that the service provider elects to turn over to them, without any protection of the rights of the user.

Further complicating modern search and seizure jurisprudence are state constitutional and statutory provisions noted above that mirror the Fourth Amendment yet provide more extensive protections for individuals.[175] If the current muddled standards continue, federal courts risk seeing this area of federal jurisprudence fade into irrelevancy as state supreme courts create their own standards that are more protective of individual privacy and would render Fourth Amendment protections redundant. *Pennsylvania v. Rushing*[176] is a prime example. There, the Pennsylvania Supreme Court ignored *Jones* and adopted the reasonable expectation of privacy standard alone when interpreting Article I, Section 8 of its own constitution.[177] The court also disregarded the "specific and articulable facts" standard used by federal courts in determining when the government can overcome a reasonable expectation of privacy and trace a suspect's location in real time.[178] Instead, the court adopted a probable cause standard.[179] As noted above, the *Earls* court had a similar holding limited to the New Jersey Constitution.[180] The danger with continuing on with the unclear standard from *Jones* is that state courts will take their cues

---

2019/WashingtonPost/2013/06/10/National-Politics/Polling/release_242.xml; *59% Oppose Government's Secret Collecting of Phone Records*, RASMUSSEN REPORTS (June 9, 2013), http://www.rasmussenreports.com/public_content/politics/general_politics/june_2013/59_oppose_government_s_secret_collecting_of_phone_records; Doug Mataconis, *Initial Polls Seemingly In Conflict On Public Opinion Of NSA Surveillance Programs*, OUTSIDE THE BELTWAY (June 11, 2013), http://www.outsidethebeltway.com/initial-polls-seemingly-in-conflict-on-public-opinion-of-nsa-surveillance-programs/; *Most disapprove of gov't phone snooping of ordinary Americans*, CBS NEWS (June 11, 2013), http://www.cbsnews.com/8301-250_162-57588748/most-disapprove-of-govt-phone-snooping-of-ordinary-americans/.

[174] People v. Harris, 945 N.Y.S.2d 505, 510 (Crim. Ct. 2012); See, for example, United States v. Meregildo, 883 F. Supp. 2d 523, 526 (S.D.N.Y. 2012), in which the court held that admission of Facebook material listed as private by defendant, but provided by Facebook friends of the defendant, was not a violation of the Fourth Amendment.

[175] Maine and Montana have passed statutes mandating that police obtain a warrant before seeking to track a suspect using his or her cell phone. ME. REV. STAT. tit. 16, § 642 (West, Westlaw through 2013 Sess.); H.B. No. 603, 63d Reg. Sess. (2013), *available at* http://leg.mt.gov/bills/2013/billhtml/HB0603.htm (last updated Apr. 22, 2013).

[176] Commonwealth v. Rushing, 71 A.3d 939, 962 (Pa. Super. Ct. 2013).

[177] *Id.*

[178] *Id.* at 961.

[179] *Id.*

[180] State v. Earls, 70 A.3d 630, 644 (N.J. 2013); See, also, the discussion in five lower court cases from Massachusetts: Commonwealth v. Augustine, No. 11-10748, 2013 WL 5612574, at *7 (Mass. Super. Ct. Apr. 3, 2013), *vacated*, 467 Mass. 230 (Mass. 2014); Commonwealth v. Princiotta, No. 2009-00965, 2013 WL 1363901, at *9 (Mass. Super. Ct. Apr. 1, 2013); Commonwealth v Willis, No. SUCR2012-10180, 2013 Mass. Super. LEXIS 114, at *5-6 (Mar. 8, 2013); Commonwealth v. Wyatt, No. 2011-00693, 2012 WL 4815307, at *7 (Mass. Super. Ct. Aug. 7, 2012); Commonwealth v. Pitt, No. 2010-0061, 2012 WL 927095, at *4 (Mass. Super. Ct. Feb. 23, 2012).

from Pennsylvania, Massachusetts, and New Jersey, developing their own standards and taking this section of search and seizure jurisprudence out of the hands of federal courts. This scenario would create yet another area of law where the rules change as one crosses state lines, an unacceptable state of affairs when often a suspect being tracked is in one state, the police tracking him are in another, and the data monitoring his movements are in a third state. In order to maintain uniformity and promote predictability, federal courts must adopt a clear standard that is more effective than the *Jones* rule.

PART V. AN ANALYSIS OF FEDERAL AND STATE CASES INVOLVING POLICE USE OF CSLI TO TRACK A SUSPECT

In order to fully explore the current state of the law with regard to police use of CSLI to track a suspect, it is necessary to find as many trial and appellate court cases as possible. The process used to do so is tedious, but the best available. The 2010 case *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*[181] was shepardized as a starting point. On January 7, 2014, that processed yielded 133 hits, 56 of which were trial court orders or appellate opinions that had cited this case. All of those orders and opinions were read and content analyzed, and any earlier cases that were cited in those orders and opinions were noted and included in the data. Trial court orders that were subsequently addressed by appellate courts were listed only under the auspices of the appellate court opinion to avoid double listing of cases. As a check to make sure that all possible cases were identified, a search on Lexis was conducted using the search term "CSLI." That search yielded 45 case hits, 11 of which were not in the data base already and involved the police using a cell phone to track the location of a criminal suspect. Reading those cases yielded one more case that had not been found through earlier efforts.

Ultimately, a database of 82 court cases in which the government's use of CSLI was at issue was compiled.[182] The earliest case was decided in 2004.[183] Of the 82 cases, only sixteen came from state courts, and only eight came from the United States Courts of Appeals. No United States Supreme Court case has addressed this issue and, at the time of this writing, no petition for certiorari has been granted. One case has been appealed to the state supreme court of Florida.[184]

In addition to case name and citation, the level of court, whether the case arose in the state or federal systems, whether the trial court suppressed the data or refused to grant the order, the length of time of the surveillance, information about the basis for the search, and the rationale of the decision was recorded. Whether the order or opinion cited to *U. S. v. Jones* and *Katz v. U. S.*, the type of crime in question, and whether the request was for historical CSLI, real time CSLI, or a ping were recorded as well.

It should be noted that most of the motions to suppress were not granted. 26 of the 82 cases, or 32 percent ultimately resulted in suppression of the evidence, which means that the government was able to use the evidence in 68 percent of the cases. It did

[181] 620 F.3d 304, 305-06 (3d Cir. 2010). This case was chosen because it was, at the time, the first United States Court of Appeals decision known to the authors on this issue.

[182] *See infra* Appendix A.

[183] U.S. v. Forest, 355 F.3d 942 (6th Cir. 2004).

[184] Tracey v. State, 69 So. 3d 992 (Fla. Dist. Ct. App. 2011), *appeal docketed*, No. SC11-2254, 2013 Fla. LEXIS 215 (Jan. 28, 2013).

not matter much whether the issue was before a state or a federal court, as the government was successful in 11 of the 16, or 69 percent, of state cases and in 45 of the 66, or 68 percent, of cases heard in federal courts. Table 1 shows the number of cases and who won by type of jurisdiction.

Table 1: Number of Cases by Who Won and Type of Jurisdiction

	Defendant Won	State Won	Total
Federal Courts	21	45	66
	(32%)	(68%)	(80%)
State Courts	5	11	16
	(31%)	(69%)	(20%)
	26	56	82
	(32%)	(68%)	(100%)

There also was no clear pattern based on the time the case was heard, but it should be noted that defendants were more successful in cases heard in 2005 (86%), 2006 (60%), and 2010 (44%) than in other years. It should also be noted that the government was successful in more than 80 percent of cases decided after 2010. Table 2 shows the distribution of cases by year.

The pattern of results is fairly clear. Criminal defendants challenging the use of CSLI were often successful in the earliest cases to be brought, but not in the most recent cases. All of the early cases came from federal courts and no clear geographic pattern appears. Defendants were successful in The District of Columbia,[185] Indiana,[186] Maryland,[187] and Wisconsin.[188] Some defendants were successful and some were not in New York[189] and Texas.[190] Defendants were not successful in Louisiana,[191] Ohio,[192] and

[185] *In re* Applications of the United States for Orders Authorizing the Disclosure of Cell Cite Info., 2005 U.S. Dist. LEXIS 43736, at *2 (D.D.C. Oct. 26, 2005); *In re* the Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 132, 133 (D.D.C. 2005).

[186] *In re* the Application of the United States for an Order: Authorizing the Installation & Use of a Pen Register, No. 1:06-MC-6, 2006 U.S. Dist. LEXIS 45643, at *14-15 (N.D. Ind. July 5, 2006).

[187] *In re* Application for an Order Authorizing the Installation & Use of a Pen Register, 439 F. Supp. 2d 456, 457 (D. Md. 2006); *In re* the Application of the United States for Orders Authorizing Installation & Use of Pen Registers, 416 F. Supp. 2d 390, 391 (D. Md. 2006); *In re* the Application of the United States for an Order Authorizing Installation & Use of a Pen Register, 402 F. Supp. 2d 597, 605 (D. Md. 2005).

[188] *In re* the Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MISC-004 2006 U.S. Dist. LEXIS 73324, at *22 (E.D. Wis. Oct. 6, 2006).

[189] *Compare In re* Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device, 396 F. Supp. 2d 294, 322-23 (E.D.N.Y. 2005), *and In re* the Application of the United States for an Order Authorizing Installation & Use of a Pen Register and/or Trap & Trace for Mobile Identification No. (585)111-1111, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006), *with In re* Application of United States for an Order for Disclosure of Telecomms. Records, 405 F. Supp. 2d 435, 450 (S.D.N.Y. 2005).

[190] *Compare In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005), *and In re* the Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, 441 F. Supp. 2d 816, 836-37 (S.D. Tex. 2006), *with In re* the Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 433 F. Supp. 2d 804, 806 (S.D. Tex. 2006).

[191] *In re* the Application of United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, 411 F. Supp. 2d 678, 682-83 (W.D. La. 2006).

[192] United States v. Forest, 355 F.3d 942, 951-52 (6th Cir. 2004).

West Virginia.[193] In those early cases in which the evidence was allowed to be used, often the judges cited the lack of precision of the data,[194] the lack of standing of the defendant,[195] or the fact that the defendant's location was only tracked while he was on public streets.[196]

Table 2: Cases by Year Decided[197]

	Defendant Won	State Won	Total
2004	0 (0%)	1 (100%)	1
2005	6 (86%)	1 (14%)	7
2006	6 (60%)	4 (40%)	10
2007	1 (25%)	3 (75%)	4
2008	1 (33%)	2 (67%)	3
2009	1 (20%)	4 (80%)	5
2010	4 (44%)	5 (56%)	9
2011	2 (20%)	8 (80%)	10
2012	2 (13%)	13 (87%)	15
2013	3 (13%)	15 (83%)	18
	26 (32%)	56 (68%)	82 (100%)

One thing that does appear in cases decided before 2009 are rulings on an apparently concerted effort by the Justice Department to craft arguments that no warrant is required in order for the government to access CSLI. The notion was that the Stored Communications Act,[198] together with the Pen Register Statute[199] and the

[193] *In re* the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register with Caller Identification Device, 415 F. Supp. 2d 663, 666 (S.D.W. Va. 2006).

[194] *See, e.g., In re* Application of the United States for an Order for Disclosure of Telecomms. Records, 405 F. Supp. 2d 435, 438 (S.D.N.Y. 2005); *See, e.g., In re* the Application of the United States or an Order, 411 F. Supp. 2d at 680.

[195] *In re* the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register, 415 F. Supp. 2d at 664-66.

[196] *Forest*, 355 F.3d at 950-51.

[197] While the limits of the Chi-Square statistic do not allow for the calculation of an accurate measurement of the probability that the distribution of cells occurred randomly when so many cells have very small numbers of cases, the authors did collapse the year variable into three categories – 2004 to 2006, 2007 to 2010, and 2011 to 2013, and ran a chi-Square analysis of that contingency table. The result was statistically significant at the .001 level. We are convinced that the differences by year were not random. There is a strong association between time and outcomes.

[198] 18 U.S.C.A. §§ 2701-2712 (West 2014).

[199] 18 U.S.C.A. §§ 3121-3127 (West 2014).

Communications Assistance for Law Enforcement Act,[200] would justify access to pretty much any type of cell phone data. Most courts rejected this "hybrid theory,"[201] although two courts in New York did not.[202] The tone of one DC judge's order was notable in admonishing the prosecutors, "I am afraid that I find the government's chimerical approach unavailing. Indeed, and to keep the animal metaphor going, it reminds one of the wag who said a camel is a horse planned by a committee."[203]

Many of these judges in early cases were convinced by arguments that the use of CSLI is the same as the use of a tracking device such as was used in the *Karo* and *Knotts* cases.[204] This argument lost its potency as more of these kinds of cases made their way through the courts, but no obvious reason has emerged from our analysis for why this changed. It is entirely possible that as judges have become more familiar with such cases, they have changed the way that they perceive the culpability of criminals who use their cellular phones in the pursuit of their criminal goals, resulting in more denials of motions to suppress. It is also plausible that judges have come to believe that cell phone users are aware of the data collection that occurs with their use and accept this reality when making decisions about what expectations of privacy are reasonable. Regardless of the reason, the trend in this area of the law in federal court is in favor of the state.

Given the comments made by Justices Sotomayor and Alito in their concurring opinions in *U. S. v. Jones* that the long term tracking of the suspect was of constitutional significance, the question of whether the length of the surveillance in question is well worth an investigation.[205] In the 43 cases for which this information was known, the average length of surveillance for the twelve cases in which the defendant was successful in getting evidence suppressed was 44 days. For the 31 cases for which this information was known and in which the defendant was not successful in getting the evidence suppressed, the average length of time of the surveillance was 66 days. If the courts are concerned that long term surveillance is a violation of the privacy of suspects, one would

---

[200] 47 U.S.C.A. §§ 1001-1010 (West 2014).

[201] *See, e.g.*, *In re* the Application of the United States for an Order Authorizing Installation & Use of a Pen Register and/or Trap & Trace for Mobile Identification No. (585)111-1111, 415 F. Supp. 2d 211, 219 (W.D.N.Y. 2006); *In re* the Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, 441 F. Supp. 2d 816, 828, 836 (S.D. Tex. 2006); *In re* the Application of the United States for an Order Authorizing Installation & Use of a Pen Register & a Caller Identification Sys. On Tel. Nos. [Sealed] & [Sealed], 402 F. Supp. 2d 597, 600 (D. Md. 2005).

[202] *In re:* Application of the United States for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006); *In re* an Application of the United States for an Order Re-Authorizing (1) The Use of a Pen Register & a Trap & Trace Device with Prospective Cell-Site Info., No. M-08-533, 2009 U.S. Dist. LEXIS 55739, at *3 (E.D.N.Y. Jan. 12, 2009).

[203] *In re* the Application of the United States for an Order Authorizing the Release of Prospective Cell Site Info., 407 F. Supp. 2d 132, 133 (D.D.C. 2005).

[204] *See, e.g.*, *In re* the Application of the United States for an Order Authorizing (1) Installation & Use of a Pen Register & Trap & Trace Device or Process, 441 F. Supp. 2d at 837; *See, e.g.*, *In re* the Application of the United States for an Order Authorizing the Installation & Use of a Pen Register &/or Trap & Trace for Mobile Identification No. (585) 111-1111, 415 F. Supp. 2d at 216.

[205] In his opinion in *U. S. v. Graham*, Judge Bennett, in referring to his interpretation of the opinions in *U.S. v. Jones*, said, "Accordingly, it appears as though a five justice majority is willing to accept the principle that government surveillance over time can implicate an individual's reasonable expectation of privacy." 846 F. Supp. 2d 384, 394-404 (D. Md. 2012) (referencing 132 S. Ct. 945 (2012)); *See, also, In re* an Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., No. 11-MC-0113, 2011 U. S. Dist. LEXIS 15457 (E.D.N.Y. Feb. 16, 2011) (explaining that length of time of continuous monitoring is key in determining whether probable cause is required to justify the release of CSLI.)

hypothesize that longer periods of continuous surveillance would result in the courts being more reluctant to approve the search. This hypothesis is not supported by this analysis.[206]

One point that is worth mentioning is how these lower courts have responded to the decision in *U. S. v. Jones*. Interestingly, the trespass standard that Justice Scalia advocated has been of virtually no import to the lower court judges deciding these cases.[207] U.S. Magistrate Judge Orenstein (S.D.N.Y.), well known and often cited for his early opinions in this area of the law, explicitly argued that cell phone tracking cases needed to be re-examined after the DC Circuit issued its decision in *United States v. Maynard*, the case that would become *United States v. Jones*. The factors that were of the most import to these re-examinations of the cell phone tracking jurisprudence were: 1) the idea that use of the phone to track a person over an extended period of time was of greater constitutional significance than a ping or tracking over a brief time period; and 2) the distinction between historical and real time, or prospective, CSLI.[208] Several cases arising in New York, Massachusetts, and Texas did address the issue of tracking over time,[209] but no consensus has emerged regarding the length of time that triggers the treatment of cell phone CSLI in the same way as the installation of a GPS tracking device.[210]

Several of the cases in the data made specific points about the distinction between historical CSLI and real time CSLI. For example, in *U. S. v. Moreno-Navarez*, the judge stated, "This Court joins the Third and Fifth Circuits, as well as the majority of the courts to address this issue . . . in concluding that there is no 'reasonable expectation of privacy' in historical cell site data."[211] In *U. S. v. Graham*, the court went to great lengths to argue that the instant case was very different that the facts in *U. S. v. Jones*[212] and that historical CSLI can be handled differently than real time CSLI or a tracking device.[213] By contrast, some courts have ruled that where the police intend to use a cell phone to track the location of suspect using the global positioning function of the phone or if they intend to use CSLI to triangulate the location of a suspect, then that is the same as the use of a dedicated tracking device such as was used in *U. S. v. Jones*.[214] At least one

---

[206] A difference of means test was conducted and the difference between the two means was not statistically significant.

[207] *Jones* was only cited by 24 of the 36 of the cases in the database that were decided after January of 2012, when the decision in *Jones* was issued. Some criminal defendants attempted to get new hearings on suppression motions in the aftermath of the *Jones* decision. *See, e.g.*, United States v. Gordon, No. 09-153-02, 2012 U.S. Dist. LEXIS 188445, at *2 (D.D.C. 2012).

[208] *In re* Application of the United States for an Order Authorizing the Release of Historical Cell Site Info., 736 F Supp 2d 578, 582 (E.D.N.Y 2010).

[209] *See, e.g., id.* at 578-79 (58 days); *See, e.g., In re* an Application of the United States for an Order Authorizing the Release of Historical Cell Site Info., 809 F. Supp. 2d 113, 114 (E.D.N.Y. 2011) (113 days); *See, e.g., In re* an Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., 2011 U. S. Dist. LEXIS 15457, at *6 (21 days); *See, e.g., In re* the Application of the United States for an Order Pursuant to Title 18, U.S.C. § 2703(d) to Disclose Subscriber Info. & Cell Site Info., 849 F. Supp. 2d 177 (D. Mass. 2012) (210 days); *See, e.g., In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 840 (S.D. Tex. 2010) (60 days).

[210] It should be noted that on remand, Antoine Jones's motion to suppress 120 days of CSLI evidence was not granted. United States v. Jones, 908 F. Supp. 2d 203, 216 (D.D.C. 2012). The court refused to decide the issue on the merits, citing to the Good Faith exception to the Exclusionary Rule. *Id.* at 215.

[211] No. 13-CR-0841-BEN, 2013 U. S. Dist. LEXIS 143900, at *4-6 (S.D. Cal. 2013).

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

[213] 846 F. Supp. 2d 384, 394-404 (D. Md. 2012).

[214] *See, e.g., In re* the Application of the United States for an Order: (1) Authorizing the Use of a Pen Register & Trap & Trace Device, 727 F. Supp. 2d 571, 579-80 (W.D. Tex. 2010); *In re* the Application of the United States for an Order Authorizing the Disclosure of Prospective Cell Site Info., No. 06-MICS-004, 2006 U.S. Dist. LEXIS 73324, at *13-16 (E.D. Wis. 2006).

federal court has ruled that access to prospective, or "real time" CSLI always requires a warrant,[215] and one court expressly stated that citizens have a reasonable expectation of privacy in their movements.[216]

Table 3 shows the cross-tabulation of the type of information sought by the government with the outcome of the motion to suppress.

Table 3: Success of Motion to Suppress by Type of Information Requested[217]

	Defendant Won	State Won	Total
Historical CSLI	7 (21%)	27 (79%)	34
Real time CSLI	18 (49%)	19 (51%)	37
	25 (35%)	46 (65%)	71 (100%)

$X^2 = 6.115$, $p<.05$*

The differences are statistically significant. In the aggregate, judges are more reluctant to grant access to real time CSLI than historical CSLI data. The reasons for this seem fairly clear. Access to locational data wherein the suspect is in a private space can be protected by a judge via redacting those parts of the CSLI records when the order is initially granted. By contrast, an order for real time or prospective CSLI inherently grants access to the suspect's location for the entire time of the order, regardless of whether the suspect is in a private space or not. Some courts have used the terms like "intimate portrait" to describe the consequences of granting the government complete access to a person's location during a given time period.[218] Regardless, the key difference seems to be the ability to protect against access to a person's location when he or she is in a private space.

But the quantitative analysis does not reveal the full story of this area of the law. As with all analysis of case opinion data, sometimes the quantitative analysis leaves out important parts of the story. In this case, there are several interesting points. For example, there were a number of cases in which the court considered the application of the good faith exception to the exclusionary rule to cell phone tracking cases.[219] Because the police often had little idea what was allowed and what the legal standards are in this area of the law, once they had relied in good faith on a court order, the courts often allowed the evidence to be admitted, even when they had doubts about the validity of the search.[220]

---

[215] *In re* the Application of the United States for an Order Relating to Target Phone 2, 733 F. Supp. 2d 939, 940 (N.D. Ill. 2009).

[216] *See In re* the Application of the United States for an Order Directing Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 534 F. Supp. 2d 585, 591 (W.D. Pa. 2008) *vacated*, 620 F.3d 304 (3d Cir. 2010).

[217] For purposes of computing the Chi-Square statistic, cases in which only a ping was involved were omitted and cases in which both historical and real time CSLI were sought we treated as requests for real time CSLI.

[218] *See, e.g.*, United States v. Maynard, 615 F.3d 544, 563 (D.C. Cir. 2010); *See also*, *In re* an Application of the United States for an Order Authorizing Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 582 (E.D.N.Y. 2010) (depicting the tracking motion of an individual as an "intimate picture" of his movements).

[219] *See, e.g.*, United States v. Leon, 468 U.S. 897, 924-26 (1984).

[220] *See* United States v. Barajas, 710 F.3d 1102, 1110-11 (10th Cir. 2013); *See* United States v. Espudo, 954 F. Supp. 2d 1029, 1043-44 (S.D. Cal. 2013); *See* United States v. Powell, 943 F. Supp. 2d 759, 793 (E.D. Mich. 2013); *See* People v. Moorer, 959 N.Y.S. 2d 868, 879-80 (Monroe Cnty. Ct. 2013).

Additionally, some courts simply used the concept of good faith to avoid deciding the Fourth Amendment issue.[221]

A key split of authority in this area of the law has to do with the impact of *Smith v. Maryland.*[222] The holding in that case was that suspects have no reasonable expectation of privacy in information voluntarily provided to third parties, such as phone service providers, that is not considered content.[223] Thus, phone numbers dialed and cell towers contacted are not subject to any limits in terms of police use. A number of judges have declared that cell phone users have no privacy interests in the numbers they dial, the location of the cell towers that their phones contact, or in historical cell site location information.[224] All of these judges have relied heavily on the S*mith v. Maryland* opinion.[225] Many rely heavily on the idea that these location data have been voluntarily given to the service provider who keeps them as a business record and that the defendant has no standing to argue for the exclusion of the evidence.[226]

The decision in *Riley v. California*[227] may shed some light on this issue. The Court dismissed the claim that accessing the call logs stored on a cell phone is no different than using a pen register as was done in *Smith v. Maryland.*[228] Coupled with the Court's detailed description of the qualitative difference between a cell phone and other types of personal possessions, the third party doctrine is potentially weakened by the decision.

Earlier cases had held that cell phone service subscribers did not have full knowledge of the extent to which they were providing data to the cell phone service provider.[229] More recently, a trial court judge in Texas held that the changes in the technology are such that the courts should rethink the issue of reasonable expectation of privacy in the context of cell phone usage.[230] The issue boils down to two real questions:

---

[221] See, for example, United States v. Jones, 908 F. Supp. 2d 203, 214 (D.D.C. 2012), which was a subsequent proceeding to the famous case of the same name; *See also* United States v. Muniz, H-12-221, 2013 WL 391161, at *4 (S.D. Tex. Jan. 29, 2013).

[222] 442 U.S. 735 (1979).

[223] *Id.* at 744-46.

[224] *See, e.g.*, United States v. Moreno-Nevarez, No. 13-CR-0841-BEN, 2013 U.S. Dist. LEXIS 143900, at *3-5 (S.D. Cal. Oct. 1, 2013) (historical CSLI); *See, e.g.*, *In Re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 610-11 (5th Cir. 2013); *See, e.g.*, United States v. Madison, No. 11.60285-CR-ROSENBAUM, 2012 U.S. Dist. LEXIS 105527, at *22-27 (S.D. Fla. July 30, 2012); *See, e.g.*, United States v. Graham, 846 F. Supp. 2d 384, 385 (D. Md. 2012) (historical CSLI); *See, e.g.*, State v. Marinello, 49 So. 3d 488, 509-10 (La. Ct. App. 2010) (historical CSLI & numbers dialed); *See, e.g.*, United States v. Benford, No. 2:09 CR 86, 2010 U.S. Dist. LEXIS 29453, at *7-8 (N.D. Ind. Mar. 26, 2010) (cell towers); *See, e.g.*, Mitchell v. State, 25 So. 3d 632, 634-35 (Fla. Dist. Ct. App. 2009) (historical CSLI); *See, e.g.*, United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 U.S. Dist. LEXIS 111622, at *24-28 (N.D. Ga. Mar. 26, 2008) (cell towers & historical CSLI).

[225] *See* cases cited *Supra* note 224 excluding *Moreno-Nevarez*.

[226] United States v. Ruby, No. 12-1073, 2013 U.S. Dist. LEXIS 18997, at *17-18 (S.D. Cal. Feb. 12, 2013). The most unexamined statement of this point found in these cases was made in *United States v. Gordon*, No. 09-153-02, 2012 U.S. Dist. LEXIS 188445, at *4-5 (examining the reasonable expectation of privacy when voluntarily revealing information to a third party).

[227] Riley v. California, 573 U.S. ___, Nos. 13-132 and 13-212 (June 25, 2014).

[228] *Id.*, slip op. at *24.

[229] See, for example, Judge Orenstein's oft cited opinion in the case of *In re an Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device*, 396 F. Supp. 2d 294, 322-23 (E.D.N.Y. 2005) ("Unlike dialed telephone numbers, cell site data is not 'voluntarily conveyed' by the user to the phone company. As we have seen, it is transmitted automatically during the registration process, entirely independent of the user's input, control, or knowledge.").

[230] *See In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 845-46 (S.D. Tex. 2010).

1) just how much do cell phone users really know about the data they are providing to the government via their cell phones; and, 2) just how much choice does anyone have if they want to stay connected with the rest of the world. The answer to that second issue has as much to do with what subjective expectations of privacy we have in a world that is increasingly interconnected by all sorts of hand held devices that are capable of communicating with the internet and with the rest of the world. It is the issue that Justice Sotomayor raised in her concurrence in *Jones,* when she said "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."[231] Chief Justice Roberts expressly addressed the potential for invasion of privacy with regard to browser history in his opinion in *Riley v. California.*[232] He wrote fairly extensively about the pervasiveness of cell phones in Americans' lives.[233] He also cited Justice Sotomayor's opinion in *Jones* favorably on the issue of location information.[234]

In the absences of any clear standard on this issue, federal courts turn to the good faith doctrine[235] to avoid the issue or find enough facts to rule in favor of the government based on the absence of any search of a public space[236] or they rely on the third party doctrine to argue that the suspect has no expectation of privacy in records maintained by the cell phone service provider.[237] One state trial court has held that warrantless use of CSLI by the police was a violation of the Fourth Amendment.[238] One state supreme court,[239] one state appellate court,[240] and two state trial courts in Massachusetts,[241] have decided that their state constitutions provide enough protection to mandate that police establish probable cause before using a cell phone to track a suspect. Other state courts have ruled that the suspect did not have a reasonable expectation of privacy while traveling on public streets.[242] One state appellate court has held that there is no reasonable expectation of privacy in historical CSLI.[243]

How you fare as a criminal defendant seeking to suppress evidence of your location gained from a warrantless search of your cell phone records depends on where you are. Admittedly, there does not seem to be any clear pattern based on region or political culture of the state. Defendants in Maine, Massachusetts, Montana, New Jersey, or Pennsylvania enjoy greater privacy rights.[244] Defendants in state courts in California,[245]

---

[231] United States v. Jones, 132 S. Ct. 945, 957 (2012).

[232] Riley v. California, 573 U.S. ___, Nos. 13-132 and 13-212, slip op. at *19 (June 25, 2014).

[233] *Id.*

[234] *Id.*, slip op. at *20.

[235] It should be noted that some of these courts have expressed doubts about the validity of the searches in question. *See, e.g.*, United States v. Powell, 943 F. Supp. 2d 759, 783 (E.D. Mich. 2013).

[236] *See, e.g.*, United States v. Skinner, 690 F.3d 773, 781 (6th Cir. 2012) (giving an example of how some judges have ruled that the CSLI did not cover any time in which the suspect was in a private space and that thus there was no reasonable expectation of privacy).

[237] *See, e.g.*, U. S. v. Ruby, 2013 U. S. Dist. LEXIS 18997, at *15 (S.D. Cal. Feb. 12, 2013); *Contra*, State v. Earls, 70 A.3d 630, 644 (N.J. 2013) (showing that the New Jersey Supreme Court expressly rejected the third party doctrine).

[238] Commonwealth v. Pitt, No. NOCV2010-00061, 2012 Mass. Super. LEXIS 39, at *19 (Feb. 23, 2012).

[239] *Earls*, 70 A.3d at 644.

[240] Commonwealth v. Rushing, 71 A.3d 939, 954-55 (Pa. Super. Ct. 2013)

[241] Commonwealth v. Wyatt, 2012 Mass. Super. LEXIS 248, at *28 (Mass. Super. Ct. Aug. 7, 2012); Commonwealth v. Augustine, 2013 Mass. Super. LEXIS 116, at *15 (Mass. Super. Ct. Apr. 3, 2013).

[242] *See, e.g.*, Tracey v. State, 69 So. 3d 992, 993 (Fla. Dist. Ct. App. 2011); *See also*, People v. Hall, 86 A.D.3d 450, 451 (N.Y. App. Div. 2011).

[243] Louisiana v. Marinello, 49 So. 3d 488, 510 (La. Ct. App. 2010)

[244] *See* cases cited *supra* note 12.

Florida,[246] Georgia,[247] Louisiana,[248] Nevada,[249] or New York,[250] have not fared as well, depending on the facts of their cases. In the federal courts, judges in the Eastern District of Michigan[251] and the Northern District of Illinois[252] have ruled in favor of defendants, but not so in Georgia,[253] Maryland,[254] or Ohio.[255] In the Southern District of California it may depend on whether you are trying to suppress historical or real time CSLI.[256] The Third[257] and Fifth[258] Circuits have expressly ruled that there is no reasonable expectation of privacy in historical CSLI, although there are some judges in Texas that are more sympathetic.[259] In federal court in New York, it may depend on the judge you get.[260]

---

[245] People v. Fernandez, No. B214476, 2011 Cal. App. Unpub. LEXIS 1931, at *1 (Cal. Ct. App. Mar 16, 2011).

[246] Tracey v. State, 69 So. 3d 992, 1000 (Fla. Dist. Ct. App. 2011); Mitchell v. Florida, 25 So. 3d 632, 633 (Fla. Dist. Ct. App. 2009).

[247] Devega v.State, 689 S.E.2d 293, 301 (Ga. 2010).

[248] *Marinello*, 49 So. 3d at 490.

[249] Zuniga v. State, No 58267, 2012 Nev. Unpub. LEXIS 1626, at *5-6 (Nev. Nov. 29, 2012). Please note that this is an unpublished opinion which, according to the header, has no precedential value.

[250] People v. Hall, 86 A.D.3d 450, 451-52 (N.Y. App. Div. 2011); People v. Moorer, 959 N.Y.S.2d 868, 881 (N.Y. Cnty. Ct. 2013).

[251] United States v. Powell, 943 F. Supp. 2d 759, 764 (E.D. Mich. 2013).

[252] *In re* the Application of the United States for an Order Relating to Target Phone 2, 733 F. Supp. 2d 939, 939 (N.D. Ill. 2009).

[253] United States v. Booker, No. 1:11-cr-00255-TWT-RGV, 2012 U.S. Dist. LEXIS 188404, at *3 (N.D. Ga. Sept. 6, 2012); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 U.S. Dist. LEXIS 111622, at *1 (N.D. Ga. Mar. 26, 2008).

[254] United States v. Graham, 846 F. Supp. 2d 384, 385 (D. Md. 2012).

[255] United States v. Dye, No. 1:10CR221, 2011 U.S. Dist. LEXIS 47287, at *25 –26 (N.D. Ohio Apr. 27, 2011).

[256] *See* United States v. Moreno-Navarez, No. 13-CR-0841-BEN, 2013 U.S. Dist. LEXIS 143900, at *4–5 (S.D. Cal. Oct. 1, 2013) (denying motion to suppress the warrantless search of historical CSLI); United States v. Espudo, 954 F. Supp. 2d 1029, 1034–1045 (S.D. Cal. 2013) (denying a motion to suppress the warrantless search of CSLI data by holding that, although a warrant to obtain real-time CSLI data must be supported by probable cause, the good faith exception to the exclusionary rule applied in this case); United States v. Ruby, No. 12CR1073 WQH, 2013 U.S. Dist. LEXIS 18997, at *18–21 (S.D. Cal. Feb. 12, 2013) (denying motion to suppress evidence obtained with a warrant for historical cell phone records); United States v. Reyes, No. 09CR2487-MMA, 2012 U.S. Dist. LEXIS 134866, at *7–11 (S.D. Cal. Sept. 20, 2012) (denying the defendant's argument that if his attorney had moved to suppress the historical CSLI, it was reasonably likely that the court would have granted the motion).

[257] *In re* the Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 312–13 (3d Cir. 2010).

[258] *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 608–15 (5th Cir. 2013). The Tenth Circuit has not directly ruled, but has stated in dicta that a ping is a search within the meaning of the Fourth Amendment. United States v. Barajas, 710 F.3d 1102, 1108 (10th Cir. 2013). The Sixth Circuit has ruled that tracking a suspect through his pay-as-you-go cell phone while on public roads, but not while the suspect was in any private places, was not a Fourth Amendment violation. United States v. Skinner, 690 F.3d 771, 777–81 (6th Cir. 2012).

[259] *See, e.g.*, *In re* the Application of the U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 840–45 (S.D. Tex. 2010), *vacated*, 724 F.3d 600 (5th Cir. 2013).

[260] *Compare, e.g.*, *In re* the Application of the United S. for Release of Historical Cell-Site Info., 736 F. Supp. 2d 578, 578–79, 595–96 (E.D.N.Y. 2010) (requiring the government to obtain a warrant before acquiring an order for CSLI), *with In re* Smartphone Geolocation Data Application, 13-MJ-242, 2013 U.S. Dist. LEXIS 62605, at *12–22 (E.D.N.Y. May 1, 2013) (holding that a warrant can issue if the government has probable cause to believe that geolocation data would aid in a defendant's apprehension, and defendant has no reasonable expectation of privacy if they agreed with their carrier that their geolocation information could be provided without consent), *and* United States v. Gilliam, No. 11 Crim. 1083, 2012 U.S. Dist. LEXIS 130248, at *5 (S.D.N.Y. Sept. 12, 2012) (denying motion to suppress CSLI evidence because the Stored Communications Act permits disclosure in emergency situations), and *In re* Application of United States for Release of Historical Cell-Site Info., No. 11-MC-0113, 2011 U.S. Dist. LEXIS 15457, at *3–7 (E.D.N.Y. Feb. 16, 2011) (granting an order for CSLI data without a warrant because the records requested were from different phones in short durations of time, instead of one long period), *and In re* Application of Order Re-Authorizing the Use of a Pen Register & Trap & Trace Device, 2009 U.S. Dist. LEXIS 55739, at *2–3 (E.D.N.Y. Jan. 12, 2009) ("[T]he

Federal courts in Utah and New York have allowed warrantless access to CSLI under the exigent circumstances provisions of the Stored Communications Act.[261] The Good Faith argument fades in usefulness over time because more and more cases are being decided in the federal districts and the authorities are more and more aware of the evolving legal arguments. This is not an acceptable state of affairs on such an important issue. The legitimacy of the courts is at stake.

PART VI: A CLEAR LEGAL STANDARD THAT PROTECTS THE RIGHTS OF CITIZENS AND INFORMS THE POLICE WHAT THEY CAN AND CANNOT DO

It is very clear that the current state of affairs is undesirable. The police are not sure what they can and cannot do. Judges faced with requests to grant orders directing cell phone service providers to release CSLI data, or with motions to suppress evidence, are not sure what the legal standard is, but have a wealth of conflicting precedents to follow. The federal courts have been highly likely to grant access to such information in the last three years based largely on the notion that everyone knows that they are giving locational data to their cell phone provider, but there is an argument to be made that the continued practice of allowing, as most federal courts do, access to historical CSLI virtually on demand goes against the grain of our history with regard to privacy. Do we really, as a society, want to make giving the government permission to track our movements on demand a condition for the use of a cell phone? It is not at all clear that doing so is in accord with public opinion. Chief Justice Roberts' extensive section on the pervasiveness of cell phones and the unique and sensitive nature of the information that can be accessed if one controls a person's cell phone in *Riley v. California*[262] is encouraging for advocates of digital freedom, but the legal standard for determining when and on what basis the police may obtain access to CSLI is still unclear. Within a day of the ruling, the news media reported that the authorities in Chicago, Illinois, were contemplating what the ruling means for their current warrantless use of cell site simulators to track the locations of the cell phones of suspects.[263]

This is not the case in five states. By statute in Maine and Montana, and by court decision in Massachusetts, New Jersey, and Pennsylvania, the courts know that such orders may only issue based on probable cause and that exclusion of evidence in the appropriate remedy. There is no confusion in these jurisdictions. They do not have to distinguish between historical CSLI, real time CSLI, and locational pings, all of which can plausibly be adjudicated based on differing standards in the current practice outside of those five states.

Additionally, the issue of who owns data generated by the use of a cell phone needs to be addressed. If the courts simply argue that all historical CSLI is a business record maintained and owned by the service provider, the cell phone user is left with little or no recourse. Abuses of government authority under the various statutes that might be used do not have a remedy. Several courts have expressly held that the remedy for

---

government may obtain prospective cell-site information without a showing of probable cause under the 'hybrid theory,' a combination of the authority of the Pen Register Statute and the Stored Communications Act.").

[261] United States v. Takai, 943 F. Supp. 2d 1315, 1323 (D. Utah 2013); *Gilliam*, 2012 U.S. Dist. LEXIS 130248, at *5.

[262] 573 U.S. ___, Nos. 13-132 and 13-212, slip op. § III(B)(1) at *17-21 (June 25, 2014)..

[263] Stacy St. Clair and Jeremy Gorner, *Court Ruling May Affect Cell Tracking by Chicago Police*, Chicago Tribune (June 25, 2014, 10:22 pm), (last visited, June 27, 2014) http://www.chicagotribune.com/news/local/ct-chicago-cell-side-met-20140626,0,4653045.story.

violation of the Stored Communications Act does not include exclusion of evidence.[264] Moreover, cell phone users do not routinely scan the minutiae of their contract with the provider to find the buried provision relating to who owns the data or whether the service provider will release said data to law enforcement or any other third party.[265] What this approach leaves is a system in which the government can access CSLI on virtually any cell phone user on a showing of less than probable cause. One has to question the values implicit in a doctrine of law that permits the government to snoop on private citizens with little or no oversight by the courts.[266] While the *Katz* reasonable expectation of privacy standard has problems, a clear statement that Americans have a reasonable expectation of privacy in their cell phone records, something that Justice Bowes did say in his opinion in *Pennsylvania v. Rushing*,[267] would be much more consistent with core Fourth Amendment values.

One might argue that requiring a warrant and limiting the application of *Smith v. Maryland* would potentially leave people in danger. In cases like *Pennsylvania v. Rushing* where an innocent person was in great danger of harm if the armed and murderous suspect could not be located and apprehended quickly, it makes sense to allow cell phone service providers to offer such access to the police immediately. The courts in both Pennsylvania and New Jersey have made it abundantly clear that the public safety exception, as laid out in *New York v. Quarles*,[268] would allow for the admission of such evidence based on probable cause and exigent circumstances, and two federal courts have allowed the use of CSLI under an exigent circumstances rationale.[269] In the majority opinion in *Riley v. California*, Chief Justice Roberts was clear in stating that the *Smith v. Maryland* precedent would not be binding on the issue of accessing call logs stored on a cell phone,[270] but also included a section on exigent circumstances.[271]

Perhaps the most compelling argument for a clear standard to be established is the need for the courts to come to terms with the set of expectations that Americans have with regard to the nature of data generated by cell phones and with the impact that cellular phone technology has on our democracy. It is very hard in today's world to exist without a cell phone and getting harder to actually own anything other than a smart phone, which poses greater privacy risks than a traditional flip phone. A decision to continue to adhere to the third party records doctrine of *Smith v. Maryland*[272] means that the government has the ability to track the location of virtually everyone over the age of 12 in the country with almost no legal recourse on the part of the person being tracked. The sweeping opinion in *Riley v. California* is not inconsistent with this point of view.

---

[264] *E.g.*, United States v. Booker, No. 1:11-cr-00255-TWT-RGV, 2012 U.S. Dist. LEXIS 188404, at *47–48 (N.D. Ga. Sept. 6, 2012); United States v. Suarez-Blanca, No. 1:07-CR-0023-MHS/AJB, 2008 U.S. Dist. LEXIS 111622, at *10–11 (N.D. Ga. Mar. 26, 2008).

[265] But see *U.S. v. Carabello*, 963 F. Supp. 2d 341, 348-49 (D. Vt. 2013), in which the court cited to service provider Sprint's terms and conditions and privacy policy regarding when they would release locational data in emergency circumstances, as a factor in favor of ruling for the government.

[266] *See, e.g.*, Steven J. Schulhofe. *More Essential than Ever: The Fourth Amendment in the Twenty-First Century*. New York: Oxford University Press 2012.

[267] 71 A.3d 939, 961 (Pa. Super. Ct. 2013).

[268] New York v. Quarles, 467 U.S. 649, 655–58 (1984) (finding a "public safety" exception to the requirement that police read Miranda rights to a suspect).

[269] *See* cases cited *supra* note 261.

[270] 573 U.S. ___, Nos. 13-132 and 13-212, slip op. at 24 (June 25, 2014).

[271] *Id.* at *26-27.

[272] *See* 442 U.S. 735, 742–43 (1979).

We are not enamored of arguments that purport to decipher the collective intent of the founders, but it is hard to imagine that a nation founded on the principles of liberty and freedom would countenance a society in which the pre-condition for participation in the social and business life of the nation is to give to the government the ability to track your location at all times. We are certain that the trespass standard that Justice Scalia would apply to such rulings is poorly adapted to the task, inconsistent with the line of cases that have been decided since 1967, and would result in the loss of freedom for Americans since it would result in the government gaining the ability to track the locations of anyone with a cell phone with little or no judicial supervision.

We are also not unsympathetic to the potential for conservative commentators to argue that we are simply proposing another way for activist judges to further a liberal agenda. It is true that one could argue that this is a policy matter that should be handled by the Congress. A statutory standard like that enacted in Maine and Montana would certainly accomplish the same goal of predictability and protection of rights without unduly hampering the ability of the police to enforce the criminal laws. Given the current state of affairs in the U. S. Congress, it seems unlikely that any such legislation will result any time soon. In addition, a Supreme Court interpretation of the Constitution is preferable because it will have more staying power in that shifts in the political winds would not change how the standard is applied.[273] Subsequent Congresses would be unable to repeal such a decision. In the meantime, however, the courts will be faced with an increasing number of these cases and judges must decide them as best they can.

[273] Justice Alito, in section II of his concurring opinion in Riley v. California, makes the opposite argument, that the privacy of cell phone data is a matter potentially well suited to action by Congress.

Appendix A

List of Cell Phone Tracking Cases[274]

US v. Forest	2004	355 F.3d 942; 2004 U.S. App. LEXIS 1139; 2004 FED App. 0032P (6th Cir.)
In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information	2005	396 F. Supp. 2d 294; 2005 U.S. Dist. LEXIS 27480 (ED NY)
In Re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace	2005	405 F. Supp. 2d 435; 2005 U.S. Dist. LEXIS 33754 (SD NY)
In Re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority	2005	396 F. Supp. 2d 747; 2005 U.S. Dist. LEXIS 24497 (SD TEX)
In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers [sealed] and [sealed] and the Production of Real Time Cell Site Information	2005	402 F. Supp. 2d 597; 2005 U.S. Dist. LEXIS 29883 (MD 2005)

[274] Table created with the findings from the research described *supra* Part V.

In the Matter of the Application of the United States of America for an Order Authorizing the Release of Prospective Cell Site Information	2005	407 F. Supp. 2d 132; 2005 U.S. Dist. LEXIS 34616 (DDC)
In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and/or Trap and Trace for Mobile Identification Number (585) 111-1111 and the Disclosure of Subscriber and Activity Information under 18 U.S.C. § 2703	2005	415 F. Supp. 2d 211; 2006 U.S. Dist. LEXIS 7653 (WD NY)
In the Matter of Applications of the United States of America for Orders Authorizing the Disclosure of Cell Cite Information	2005	2005 U.S. Dist. LEXIS 43736 (DC)
In the Matter of the Application of the United States for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; and (2) Authorizing Release of Subscriber Information and/or Cell Site Information	2006	411 F. Supp. 2d 678; 2006 U.S. Dist. LEXIS 3392 (WD LA)
In re: Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone	2006	460 F. Supp. 2d 448; 2006 U.S. Dist. LEXIS 76822 (SD NY 2006)

In the Matter of the Application of the United States of America for an order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information	2006	433 F. Supp. 2d 804; 2006 U.S. Dist. LEXIS 40856 (SD TEX)
In the Matter of the Application for an Order Authorizing the Installation and Use of a Pen Register and Directing the Disclosure of Telecommunications Records for the Cellular Phone Assigned the Number [SEALED]	2006	439 F. Supp. 2d 456; 2006 U.S. Dist. LEXIS 59845 (MD)
In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information	2006	2006 U.S. Dist. LEXIS 73324 (ED WI)
In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking	2006	441 F. Supp. 2d 816; 2006 U.S. Dist. LEXIS 56332 (SD TEX)

In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location Based Services; In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device; (2) Authorizing the Release of Subscriber and Other Information; and (3) Location of Cell Site Origination and/or Termination	2006	2006 U.S. Dist. LEXIS 45643 (ND Indiana)
In re Application of the United States for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone	2006	2006 U.S. Dist. LEXIS 11747 (SD NY)
In the Matter of the Application of the United States of America for Orders Authorizing the Installation and Use of Pen Registers and Caller Identification Devices on Telephone Numbers [Sealed] and [Sealed]	2006	416 F. Supp. 2d 390; 2006 U.S. Dist. LEXIS 7345 (MD)
In the Matter of the Application of the united States of America for an Order Authorizing the Installation and use of a Pen Register with Caller Identification Device and Cell Site Location Authority on a Certain Cellular Telephone	2006	415 F. Supp. 2d 663; 2006 U.S. Dist. LEXIS 6976 (SD WV)

In re Application of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d)	2007	509 F. Supp. 2d 76; 2007 U.S. Dist. LEXIS 68339 (Mass 2007)
In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register Device, a Trap and Trace Device, and for Geographic Location Information.	2007	497 F. Supp. 2d 301; 2007 U.S. Dist. LEXIS 52009 (Puerto Rico 2007)
In re Application for an Order Authorizing the Extension and Use of a Pen Register Device, etc.	2007	2007 U.S. Dist. LEXIS 11692 (ED Cal 2007)
In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information	2007	622 F. Supp. 2d 411; 2007 U.S. Dist. LEXIS 77635 (SD TEX)
In the Matter of an Application of the United States of America for an Order Authorizing the Use of Two Pen Register and Trap and Trace Devices	2008	632 F. Supp. 2d 202; 2008 U.S. Dist. LEXIS 97359 (ED NY)
U. S. v. Suarez-Blanca	2008	2008 U.S. Dist. LEXIS 111622 (ND GA 2008)
In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government	2008	534 F. Supp. 2d 585; 2008 U.S. Dist. LEXIS 13733 (2008 WD PA)
U. S. v. Jenious	2009	2009 U.S. Dist. LEXIS 132385 (Ed WI)

In the Matter of the Application of the United States of America for an Order Relating to Target Phone 2	2009	733 F. Supp. 2d 939; 2009 U.S. Dist. LEXIS 130713 (ND IL)
U.S. v. Navas	2009	640 F. Supp. 2d 256; 2009 U.S. Dist. LEXIS 37464 (SD NY)
In the Matter of an Application of the United States of America for an order Re-authorizing (1) The Use of a Pen Register and a Trap and Trace Device with Prospective Cell Site Information; (2) The Release of historical Cell Site and Subscriber Information; and (3) Authorizing the Release of Subscriber Information, Including Tower/Sector & Msc Records	2009	2009 U.S. Dist. LEXIS 55739 (ED NY)
Mitchell v. State of Florida	2009	25 So.3d 632 (2009)
In re US for an Order Directing Provider of Elec. Commun. To Disclose Records to the Govt	2010	620 F3d 304 (3rd cir PA)
In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell Site Information	2010	736 F. Supp. 2d 578; 2010 U.S. Dist. LEXIS 88781 (ED NY)
In re Application of the United States of America for Historical Cell Site Data	2010	747 F. Supp. 2d 827; 2010 U.S. Dist. LEXIS 115529 (SD TX)
U. S. v. Benford	2010	2010 U.S. Dist. LEXIS 29453 (ND Indiana, 2010)
In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Use of a Pen Register and Trap and Trace Device; (2) Authorizing Release of Subscriber and Other Information; and (3) Authorizing the Disclosure of Location Based Services	2010	727 F. Supp. 2d 571; 2010 U.S. Dist. LEXIS 77319 (WD TEX 2010)

U. S. v. Redd	2010	2010 U.S. Dist. LEXIS 103385 (KANSAS 2010)
Mitchell v. Vogel	2010	2010 U.S. Dist. LEXIS 123188 (MD FL Fort Myers Division 2010)
Louisiana v. Marinello	2010	49 So. 3d 488; 2010 La. App. LEXIS 1331
Devega v. The State.	2010	286 Ga. 448; 689 S.E.2d 293; 2010 Ga. LEXIS 107; 2010 Fulton County D. Rep. 248; 49 Comm. Reg. (P & F) 635
U. S. v. Dye	2011	2011 U.S. Dist. LEXIS 47287 (ED OH)
In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell Site Information	2011	809 F. Supp. 2d 113 (ED NY)
In the Matter of the Application of the United States of America for an Order Authorizing Disclosure of Historical Cell Site Information for Telephone Number [text redacted by the court]	2011	2011 U.S. Dist. LEXIS 156744 (DC)
In the Matter of an Application of the United States of America for an Order Authorizing Disclosure of Location Information of a Specified Wireless Telephone	2011	849 F. Supp. 2d 526; 2011 U.S. Dist. LEXIS 85638 (Md)
In Re In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information	2011	2011 U.S. Dist. LEXIS 15457 (ED NY)
U. S. v. Powell	2011	444 Fed Appx 517, 2011 U. S. App LEXIS 18957 (3rd Cir NJ 2011)

In re: Application for a Court Order Authorizing AT&T to Provide Historical Cell Tower Records ; In re: AT&T Sim Card #89014103211858609369; In re: AT&T Black Samsung Flip Phone Model #SGH-A197, FCC ID#A3LSGHA197, SIN RQBZ917758D; In re: Application for a Court Order Authorizing Sprint/Nextel Corporate Security to Provide Historical Cell Tower Records	2011	55 V.I. 127; 2011 V.I. LEXIS 65 (Superior Court of the Virgin Islands, Division of St. Thomas and St. John)
People v. Fernandez	2011	2011 Cal. App. Unpub. LEXIS 1931
Tracey v. Florida	2011	69 So. 3d 992; 2011 Fla. App. LEXIS 14054; 36 Fla. L. Weekly D 1961
The People of the State of New York v. Alexander Hall	2011	86 A.D.3d 450; 926 N.Y.S.2d 514; 2011 N.Y. App. Div. LEXIS 5807; 2011 NY Slip Op 5936
In the Matter of the Application of the United States of America for an Order Pursuant to Title 18, United States Code, Section 2703(d) to Disclose Subscriber Information and Cell Site Information	2012	849 F. Supp. 2d 177; 2012 U.S. Dist. LEXIS 42779 (Mass)
U. S. v. Skinner	2012	690 F.3d 772 (6th cir TN)
U. S. v. Pascual	2012	502 Fed. Appx. 75; 2012 U.S. App. LEXIS 23272 (2nd cir NY)
U. S. v. Madison	2012	2012 U.S. Dist. LEXIS 105527 (SD Florida)
U. S. v. Graham	2012	846 F. Supp. 2d 384; 2012 U.S. Dist. LEXIS 26954 (MD 2012)
U. S. v. Hardrick	2012	2012 U.S. Dist. LEXIS 147940 (ED LA 2012)
U. S. v. Booker	2012	2012 U.S. Dist. LEXIS 188404 (ND Ga 2012)
U. S. v. Jones	2012	908 F. Supp. 2d 203; 2012 U.S. Dist. LEXIS 177294 (DC)
U. S. v. Gordon	2012	2012 U.S. Dist. LEXIS 188445 (DC 2012)
U. S. v. Reyes	2012	2012 U.S. Dist. LEXIS 134866 (Sd Cal)
U. S. v. Gilliam	2012	2012 U.S. Dist. LEXIS 130248 (SD NY

		2012)
Smarr v. The State	2012	317 Ga. App. 584; 732 S.E.2d 110; 2012 Ga. App. LEXIS 768; 2012 Fulton County D. Rep. 2802
Commonwealth of Massachusetts v. Francis Wyatt	2012	30 Mass. L. Rep. 270; 2012 Mass. Super. LEXIS 248
Commonwealth v. Zeph Pitt	2012	29 Mass. L. Rep. 445; 2012 Mass. Super. LEXIS 39
Zuniga v. Nevada	2012	2012 Nev. Unpub. LEXIS 1626 (2012)
U. S. v. McCullough	2013	2013 US App LEXIS 8108 (2nd cir NY)
U. S. v. Caraballo	2013	2013 U.S. Dist. LEXIS 112739 (VT)
In re: Application of the United States of America for Historical Cell Site Data	2013	724 F.3d 600 (5th cir TX)
In re Smartphone Geolocation Data Application	2013	2013 U.S. Dist. LEXIS 62605 (ED NY)
U. S. v. Muniz	2013	2013 U.S. Dist. LEXIS 12162 (SD TX 2013)
U. S. v. Powell	2013	943 F. Supp. 2d 759; 2013 U.S. Dist. LEXIS 64804 (ED Michigan)
U. S. v. Moreno-Navarez	2013	2013 U.S. Dist. LEXIS 143900 (SD Cal 2013)
U. S. v. Espudo	2013	2013 U.S. Dist. LEXIS 104502 (SD Cal 2013)
U. S. v. Steve Ruby	2013	2013 U. S. Dist. LEXIS 18997 (SD Cal 2013)
U.S. v. Barajas	2013	710 F 3d 1102 (10th Cir Kan 2013)
U. S. v. Wilson	2013	2013 U. S. Dist. LEXIS 37783 (ND Ga 2013)
U. S. v. Takai	2013	943 F. Supp. 2d 1315; 2013 U.S. Dist. LEXIS 61698 (Utah, Central Division 2013)
Commonwealth v. Princiotta	2013	31 Mass. L. Rep. 68; 2013 Mass. Super. LEXIS 32
State v. Earls	2013	214 N.J. 564, 70 A.3d 630, 2013 N.J. LEXIS 735 (2013)
Commonwealth v. Rushing	2013	2013 PA Super 162; 71 A.3d 939; 2013 Pa. Super. LEXIS 1605
The People of the State of New York v. Moorer	2013	39 Misc. 3d 603; 959 N.Y.S.2d 868; 2013 N.Y. Misc. LEXIS 632; 2013 NY Slip Op 23048
Commonwealth v. Willis	2013	31 Mass. L. Rep. 436; 2013 Mass. Super. LEXIS 114
Commonwealth v. Augustine	2013	31 Mass. L. Rep. 415; 2013 Mass. Super. LEXIS 116