SEARCHING FOR A LIMITING PRINCIPLE: CELL PHONE TRACKING, THE FOURTH AMENDMENT, AND THE DRAGNET SEARCH DOCTRINE

Usman Ahmed
Hannah Murray Naltner
Luke Pelican

Available at: https://works.bepress.com/usman_ahmed/1/
SEARCHING FOR A LIMITING PRINCIPLE: CELL PHONE TRACKING, THE FOURTH AMENDMENT, AND THE DRAGNET SEARCH DOCTRINE

By Usman Ahmed, Hannah Murray Naltner, & Luke Pelican

Table of Contents

Introductions ................................................................................................................................................. 2

I. The Third Party Doctrine & Cell-Site Searches ..................................................................................... 8
   A. The Third Party Doctrine and Electronic Surveillance: Four Connected Cases, One Remaining Inquiry....................................................................................................................................................... 8
      i. On Lee v. United States (1952) – Knowing Exposure ................................................................. 10
      ii. Katz v. United States (1964) – A Third Party Doctrine Case...................................................... 12
      iii. White v. United States (1971) – Method of Acquisition............................................................ 15
      iv. Smith v. Maryland (1979) – Voluntary Conveyance.................................................................. 18
      v. One Remaining Premise: Voluntary Conveyance ....................................................................... 22
   B. The Application of the Third Party Doctrine to Cell-Site Searches ................................................ 25

II. Application of the Third Party Doctrine ............................................................................................. 30
   A. The Third Party Doctrine Does Not Apply: There is No Voluntary Conveyance.......................... 34
   B. The Third Party Doctrine Applies: “But…” ................................................................................... 38
   C. The Third Party Doctrine is Misplaced in the CSLI context .......................................................... 43

III. Searching for a Limiting Principle .................................................................................................... 54
   A. Limiting Legislation ....................................................................................................................... 55
      i. CSLI Bills in the 113th Congress ................................................................................................. 55
      ii. Potential Obstacles to Legislation .............................................................................................. 62
   B. A Jurisprudential Limiting Principle – Reviving the Dragnet Search Doctrine ............................. 64
      i. Academic Proposals To Limit High-Technology Searches Provide Additional Precision........ 67
      ii. Problems With A Judicially Limited Approach .......................................................................... 72

IV. Conclusion......................................................................................................................................... 74

---

1 Usman Ahmed is currently a Policy Counsel at eBay, Inc. Hannah Murray Naltner is currently in private practice at an international law firm. Luke Pelican is an associate with a private law firm. All graduated from the University of Michigan Law School. This piece solely reflects the views of the authors acting in their individual capacities. The authors wish to especially thank David Faustch for his help in development of this article. The authors would also like to thank Professors Eve Brensike Primus and Samuel R. Gross.
"The whole scope of privacy in public changes when you're not just talking about who within a few blocks might see you, but rather who might be tracking you from miles away."

- Lee Tien\(^2\)

Imagine that a town in New York City has seen a recent rise in hospitalizations for overdoses from cocaine. The police have a tip that the drugs are being handed out at parties that are organized through a social networking website. The police discover the location of the next party and arrest several of the party guests. None of the guests, however, are able to provide the name of the dealer who supplied the drugs. The only information the police obtain is a phone number that was used to contact the drug dealer. Without obtaining a warrant, the police contact the dealer’s cell phone service provider. The provider is able to identify the cell phone tower that is currently providing service to the suspect’s cell phone; this information allows the police to locate the suspect. The police find the dealer in his home having an intimate dinner with his family. They immediately arrest him.

Now imagine that in another town, this one a small rural city just outside of Santa Fe, an elderly gentleman who owns a hardware store has just purchased his first cell phone. He primarily uses his phone as a means to communicate with his grandchildren. One night, a murder occurs inside the hardware store, and the police believe that the elderly gentleman is a suspect because he is the only person who has a key to the store. The police are unable to locate the elderly gentleman as he is in Albuquerque visiting his son and grandchildren. The police

discover his cell phone number from interviewing local residents and, without obtaining a warrant, take this information to the elderly gentleman’s cell phone service provider. The provider is able to identify the three cell phone towers closest to the elderly gentleman’s cell phone signal. This information is used to triangulate his location. The police arrest the elderly gentleman at his son’s house in Albuquerque.

In order to properly analyze these hypotheticals, an outline of the technology involved is required. Cell phone service providers own and operate cell towers, also known as cell-sites, around the country. In order for a cell phone user to obtain and maintain service, the cell phone must constantly communicate with these cell-sites. Each cell phone is embedded with unique codes that allow a cell phone tower to identify it and communicate with it. As a cell phone changes locations, it automatically communicates with the closest cellular towers – this information is known as cell-site location information (CSLI). The police can access CSLI by requesting it from the cell phone service provider. CSLI provides police with an accurate location of a suspect.

---


The use of CSLI searches will likely increase in the wake of the Supreme Court’s 2012 decision in *Jones v. United States*. 9 In *Jones*, the court held that attaching a GPS device to a suspect’s car was a trespass of the suspect’s effects and, therefore, constituted a search under the Fourth Amendment.10 This new “trespass test” will undoubtedly raise a host of Fourth Amendment questions.11 Moreover, the Government was immediately forced to abandon thousands of government installed GPS tracking devices after the *Jones* decision.12 Cell phone searches, on the other hand, do not seem to implicate the notion of a trespass because there is no need for police to attach a physical device to a suspect’s effects. Instead, the suspect provides electronic signals with information on his location directly to a service provider. The Court

---


seemed to hint that a mere transfer of electronic signals would not constitute a trespass.\textsuperscript{13} Thus, rather than procure a warrant and attach a location device to a suspect, police could simply acquire location information from companies that already track such data.

This article addresses a question that was left open by \textit{Jones} and that courts throughout the country are struggling to answer: should the government be able to conduct warrantless surveillance of a criminal suspect by tracking the prospective CSLI received from a suspect’s cell phone?\textsuperscript{14} The importance of this question has been magnified as a result of the recently discovered National Security Agency (NSA) program, which collected the metadata of telephone records of customers of Verizon.\textsuperscript{15} The NSA’s program did not, however, collect cell phone location information.\textsuperscript{16} The NSA program was reviewed, and approved, by the Foreign Intelligence Surveillance Act Court, which is mandated by statute to ensure that investigations “be conducted in a manner consistent with the fourth amendment to the Constitution of the United States.”\textsuperscript{17}

\textsuperscript{13} US v. Jones, slip opinion, 565 U.S. ___ at 11 (2012) (“Situations involving merely the transmission of electronic signals without trespass would remain subject to Katz analysis”).

\textsuperscript{14} There are two types of cell-site data search tactics utilized by the police. Retroactive cell-site data involves the service provider releasing records of the cell phone owner’s past “pings” of cell phone towers. Prospective cell-site data provides the police with instant location data based on the “ping” of the suspect’s cell phone. This paper will focus only the Fourth Amendment analysis of prospective cell-site data searches.


\textsuperscript{17} Foreign Intelligence Surveillance Act of 1978 SEC. 702. (b)(5)
An analysis of the open CSLI question under Fourth Amendment doctrine would employ the reasonable expectation of privacy test, which considers the suspect’s subjective expectation of privacy under the circumstances and whether society would view that expectation as objectively reasonable. A court would weigh the objective and subjective expectation of privacy an individual has in his CSLI. This can be a difficult question to analyze, as the two above hypotheticals indicate.

The Supreme Court’s doctrine on a person’s expectation of privacy in his or her location entails an analysis of several interrelated rules. One rule, often claimed to be clear and definitive, is that a person has an absolute expectation of privacy when he or she is inside his home. When police use a technology to determine whether or not a person is inside his home, they violate the Fourth Amendment. Under this rule, the dealer in the first hypothetical had his Fourth Amendment rights violated, whereas the elderly gentleman in the second hypothetical did not.

18 See Christopher Slobogin, Symposium: The Search and Seizure of Computers and Electronic Evidence: Transaction Surveillance by the Government, 75 MISS. L.J. 139, 161 (2005). (finding that the issue of prospective cell site data does not raise questions under the SCA because prospective cell site data is not an “existing record” at the time of the request, or the ECPA because location information is not addressed by the statute).


20 See David A. Couillard, Note: Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing, 93 MINN. L. REV. 2205, 2206 (2009) (arguing that the expectation of privacy test fails to provide clear answers in the case of emerging technologies); But See Sam Kamin, The Private is Public: The Relevance of Private Actors in Defining The Fourth Amendment, 46 B.C. L. REV. 83, 140 (2004) (arguing that judges can, and should, discover societal expectation of privacy based on empirical research by social scientists).


22 United States v. Karo, 468 U.S. 718 (1984) (holding that use of an electronic beeper to discover that the suspect was inside his home violated the Fourth Amendment).
This result seems counter-intuitive and arbitrary. Arguably, the elderly gentleman has a subjective expectation of privacy in his CSLI because he is not aware that his cell phone transmits information on his location on a near real time basis. When the same subjective expectation of privacy test is applied to the tech-savvy drug dealer, who does or should understand that his cell phone regularly emits location data, there is a different result. Moreover, the question of an objective expectation of privacy in cell phones – whether society in general recognizes an expectation of privacy in its cell phones – is a hotly debated question with no discernable answer.  

This article considers whether the application of a concurrent doctrinal tool, the third party doctrine, may moot the analysis rooted in the reasonable expectation of privacy test. Application of the third party doctrine turns on an individual eliminating his reasonable expectation of privacy in particular information by providing that information to a third party. In the context of cell phones and location information, the application of the third party doctrine proceeds as follows: A user powers on his cell phone. The cell phone necessarily transmits CSLI to a cellular service provider. The cell phone user can no longer claim to have a reasonable expectation of privacy in the information once he has provided location information to the cellular service provider (a third party).  

---

23 Compare In the Matter of an Application of the United States of America for an Order Authorizing the Release of Historical Cell-Site Information, 2010 U.S. Dist. LEXIS 88781 (E.D.N.Y., 2010) (arguing that there is an expectation of privacy in CSLI); In re Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register, 402 F. Supp. 2d 597, 605 (D. Md., 2005) (“cell phone possessors’ expectation of privacy, at least when they are in a non-public place, seems altogether reasonable”) with In re United States for Order for Disclosure of Telecommunications Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y., 2005) (holding that there is no Fourth Amendment concerns with CSLI searches because of the third party doctrine); Stephen E. Henderson, Learning From All Fifty States: How to Apply the Fourth Amendment and its State Analogs to Protect Third Party Information From Unreasonable Search, 55 CATH. U.L. REV. 373, 388 (2006). (“it seems unlikely that one could realize he or she is able to receive cell phone calls wherever located without recognizing that the service provider must know his or her location”).
I. The Third Party Doctrine & Cell-Site Searches

The Supreme Court has a rich history of cases over the past century discussing the intersection of technology and personal privacy.\textsuperscript{25} It is essential to discuss these cases in order to understand why CSLI falls directly within the ambit of the third party doctrine.

A. The Third Party Doctrine and Electronic Surveillance: Four Connected Cases, One Remaining Inquiry

Over the course of a quarter-century the Court defined the third party doctrine in relation to surveillance technology. A concept initially designed to aid police officers in conducting necessary fieldwork\textsuperscript{26} has become an unbounded tool allowing police to access phone records,\textsuperscript{27} e-mail account records,\textsuperscript{28} and internet service provider records.\textsuperscript{29}

Before diving into the cases that shaped the third party doctrine in the realm of electronic surveillance, a proper definition of third party doctrine must be provided. The third party


\textsuperscript{26} United States v. Lee 274 US 559, 563 (1927) (utilizing third party doctrine to justify the search of the deck of a boat); \textit{See also} Susan Freiwald, \textit{Online Surveillance: Remembering the Lessons of the Wiretap Act}, 56 ALA. L. REV. 9, 16-17 (2004).

\textsuperscript{27} Smith v. Maryland, 442 U.S. 735, 742-45 (1979).

\textsuperscript{28} United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) (holding that information given to an ISP in order to establish an e-mail account is not protected by the Fourth Amendment).

doctrine is essentially an application of the common law doctrine of assumption of risk to the Fourth Amendment\textsuperscript{30}: by knowingly exposing information to a third party, a person assumes the risk that the third party will turn the information over to the government.\textsuperscript{31} In other words, there is no Fourth Amendment protection for information knowingly exposed to the public.\textsuperscript{32}

The major policy argument supporting the continued application of the third party doctrine is that without it, the police would be handcuffed by the Fourth Amendment from using a number of essential investigative techniques (\textit{e.g.}, undercover agents, accessing records, and tracking suspects).\textsuperscript{33} Moreover, the third party doctrine provides a clear rule whereby police officers know that the Fourth Amendment will not be implicated if the information or item they obtain has been revealed to a third party.\textsuperscript{34} There have been harsh academic criticisms of this doctrine, but it continues to be a governing rule in Fourth Amendment law.\textsuperscript{35}

\textsuperscript{30} Smith v. Maryland, 442 U.S. 735, 744-745 (1979); Amanda Yellon, \textit{Note: The Fourth Amendment's New Frontier: Judicial Reasoning Applying the Fourth Amendment to Electronic Communications}, 4 MD. J. BUS. & TECH. L. 411, 418 (2006); \textit{But see} Susan Freiwald, \textit{First Principles of Communications Privacy}, 2007 STAN. TECH. L. REV. 3, 41 (2007) (arguing that the assumption of risk analogy is not logical when used to extend third party doctrine to areas such as bank records or e-mails).

\textsuperscript{31} Thomas P. Crocker, \textit{From Privacy to Liberty: The Fourth Amendment After Lawrence} 57 UCLA L. REV. 1, 34 (2009) (“the Supreme Court has repeatedly held that we have no Fourth Amendment expectation of privacy in what we voluntarily disclose to others”); Stephen E. Henderson, \textit{Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search}, 56 MERCER L. REV. 507, 546 (2005) (“…once information is given to any one party for any one purpose, it is treated as if it were given to every person for any possible purpose as far as the Fourth Amendment is concerned”).


i. On Lee v. United States (1952) – Knowing Exposure

Professor Orin Kerr describes On Lee as the case that established the third party doctrine for cases of Secret Agents (government informants).\(^\text{36}\) The case was one of the first to tackle the issue of government informants utilizing a wire to transmit information to the police.

The facts of On Lee surround a series of conversations between the suspect, On Lee, and an old acquaintance of his, Chin Poy.\(^\text{37}\) The first conversation occurred at the front desk of a Laundromat owned by Mr. On Lee. Several customers passed through the Laundromat during the course of their conversations. The second conversation took place on a crowded sidewalk in New York.\(^\text{38}\) Mr. On Lee was unaware that Mr. Poy had become a cooperating agent for the government and was wired for sound. A police officer stationed nearby was able to hear the

---


\(^{35}\) See Paul Ohm, Symposium Cyberspace & the Law: Privacy, Property, and Crime in the Virtual Frontier: Probably Probable Cause: The Diminishing Importance of Justification Standards, 94 MINN. L. REV. 1514, 1556-57 (2010) (claiming that Professor Kerr stands alone in academia in his defense of third party doctrine); Orin S. Kerr, The Case for the Third Party Doctrine, 107 Mich. L. Rev. 561, 563 n. 5 (2009) (outlining a number of academic criticisms of third party doctrine); Jed Rubenfeld, The End of Privacy, 61 STAN. L. REV. 101, 113 (2008) (arguing that if the third party doctrine is taken to the extreme it will render the Fourth Amendment toothless); Sam Kamin, The Private is Public: The Relevance of Private Actors in Defining The Fourth Amendment, 46 B.C. L. REV. 83, 117 (2004) (arguing that to determine the current scope of Fourth Amendment protection, the suspect must consider if his information has been exposed to others); See also Andrew E. Taslitz, Enduring and Empowering: The Bill of Rights in the Third Millennium: The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions, 65 LAW & CONTEMP. PROB. 125, 131 (2002) (arguing that third party doctrine no longer makes sense in the modern technological world where we often reveal information to one party without assuming the risk that it will be broadcast to any and all parties).


\(^{38}\) Id.
conversations through a receiving set. Mr. On Lee made several incriminating statements.

At trial, Mr. Poy was unable to testify; the judge, however, allowed the police officer to testify as to the contents of the conversations between Mr. On Lee and Mr. Poy. Mr. On Lee argued that the method by which this testimony was obtained constituted an illegal search and seizure. Mr. On Lee’s arguments were phrased in the language of the then oft-used “trespass” doctrine. The major inquiry under the trespass doctrine was whether the surveillance technique caused a physical penetration of a protected area. Mr. On Lee argued that Mr. Poy was a trespasser since he had fraudulently represented himself in order to gain entry to Mr. On Lee’s Laundromat. Moreover, Mr. On Lee claimed that the police officer was a trespasser because his listening device penetrated the walls of the establishment through an electronic aid. The Court rejected both of these arguments, distinguishing electronic interceptions from cases where tangible property was intercepted by clear physical trespass.

After requesting that the Court reinterpret its Fourth Amendment doctrine in the area of intercepted conversations, Mr. On Lee made a public policy argument. He claimed that the government utilized an improper tactic by tricking him into thinking he could trust Mr. Poy. The Court resoundingly rejected this argument, stating, “No good reason of public policy occurs to us

---

39 Id. at 749-750.
40 Id. at 750.
43 Id. at 752-753.
44 Id. at 753; See also Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 ALA. L. REV. 9, 22 n. 72 (2004).
why the Government should be deprived of the benefit of On Lee's admissions because he made them to a confidante of shady character." Moreover, the tactic of using electronic surveillance was lawful because Mr. Poy had voluntarily agreed to transmit the information to the government. The result would have been the same had the police officer heard the information with his own ears.

On Lee established a strong principle; once a suspect transmitted information to a third party, he could no longer claim Fourth Amendment protection over that information.

ii. Katz v. United States (1964) – A Third Party Doctrine Case

Katz is considered the corner stone case of modern Fourth Amendment law. It is commonly cited for its famous quote, “the Fourth Amendment protects people not places.” The impetus for this quote came from the Court’s decision to move away from a Fourth Amendment analysis focused on whether the defendant was located in a “protected area” that had been physically trespassed, to one which considered the defendant’s “reasonable expectation of privacy.” The traditional narrative has described Katz as establishing the reasonable

46 Id. at 744; See also Orin S. Kerr, The Case for Third-Party Doctrine, 107 MICH. L. REV. 561, 567 (2009).
47 Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 ALA. L. REV. 9, 27 (2004) (“The majority saw no meaningful difference between the government agent listening to the conversation using an electronic receiver and hearing the conversation with his own ears”).
48 Smith v. Maryland, 442 U.S. 735, 739 (1979) (“In determining whether a particular form of government-initiated electronic surveillance is a "search" within the meaning of the Fourth Amendment, our lodestar is Katz”).
50 Ric Simmons, From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies, 53 HASTINGS L.J. 1303, 1303, 1311 (2002) (describing the “paradigm shift” in Katz, from the
expectation of privacy test as the crux of the Fourth Amendment inquiry.\textsuperscript{51} \textit{Katz} was also a case that involved electronic surveillance as well as the third party doctrine.\textsuperscript{52}

Mr. Katz was charged with conveying wagering information by telephone wire over interstate lines, in violation of a federal statute.\textsuperscript{53} The FBI suspected him of utilizing a public telephone booth in Los Angeles to transmit information to an illegal gambling ring in Boston and Miami.\textsuperscript{54} The FBI attached a listening device to the outside of the public telephone booth and recorded the conversations that Mr. Katz was having with his associates.\textsuperscript{55} Mr. Katz claimed that that the method used by the FBI violated his Fourth Amendment rights.

The government maintained that its tactics did not run afoul of the Fourth Amendment because the listening device did not actually penetrate the walls of the telephone booth and the telephone booth was not a protected area. Mr. Katz responded by claiming that a phone booth was in fact a protected area.\textsuperscript{56} The Court ignored both of these arguments and viewed the case using the new expectation of privacy paradigm.\textsuperscript{57} The Court held that Mr. Katz did have an

\textsuperscript{51}But see Orin S. Kerr, \textit{The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution}, 102 MICH. L. REV. 799, 807 (2004) (arguing that the expectation of privacy test has not proven to be a revolution in practice).

\textsuperscript{52}See Jed Rubenfeld, \textit{The End of Privacy}, 61 STAN. L. REV. 101, 115 (2008) (claiming that if the third party doctrine is read expansively then the Katz decision itself does not make sense since the suspect in Katz exposed information to a third party).


\textsuperscript{56}David A. Sullivan, \textit{Note: A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology}, 44 ARIZ. L. REV. 967, 973-74 (2002) (“At the outset of the appeal, both sides tried to characterize the issues in ways that the Court ultimately rejected”).
expectation of privacy in the telephone booth, which was violated by the use of the listening device.

*Katz* is not typically discussed as a case applying third party doctrine, but certain facts of *Katz* arguably mirror those of *On Lee*. In both cases, the suspect knowingly exposed information to a third party and, without his knowledge, the police utilized electronic surveillance to record his statements. Nevertheless, the Court in *Katz* seemed to overlook the factual similarities with *On Lee*, instead focusing on expectation of privacy of the suspect. The suspect in *Katz* had closed the door of a telephone booth and therefore, “is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.” This ruling is in direct conflict with *On Lee*’s reasoning that information knowingly exposed to a third party is no longer subject to Fourth Amendment. Information was disclosed in both cases and the Court gives no reason for distinguishing them.

The two cases are further muddled by *Katz*’s reaffirmation of the rule that information knowingly exposed to a third party, even in his home, is not subject to the Fourth Amendment. The Court attempted to place a limit on this rule by claiming that when a person seeks to

---

60 *See* Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1311 (2002) (describing the lack of guidance in the *Katz* decision).
61 *Katz* v. United States, 389 U.S. 347, 351 (1967); *See also* United States v. White, 436 F.2d 1243, 1247 (7th Cir., 1970) (relying on this language in *Katz* to approve of warrantless tracking of a suspect’s car phone conversations because anyone with a similar car phone or FM transmitter could tune into the same radio frequency the suspect was using and overhear that conversations).
preserve some information as private, then it may be subject to Fourth Amendment protection.\(^{62}\)

The key in *Katz* was that the suspect wished to keep out the uninvited ear; he manifested that wish by closing the door to the telephone booth.\(^{63}\) But, there is little doubt that the suspect in *On Lee* wished to block any uninvited ears from the conversation he had with his associate.\(^{64}\) The conversations that took place in *On Lee* occurred in the suspect’s privately owned place of business.\(^{65}\) It is difficult to explain *Katz*’s reasoning in the light of *On Lee*.\(^{66}\)

Seven years passed before the Court would clarify the distinction between *On Lee* and *Katz* for the purposes of the third party doctrine.

iii. **White v. United States (1971) – Method of Acquisition**

Justice Harlan’s concurrence in *Katz* noted that the Court’s decision would not affect the holding in *On Lee*, but the majority seemed to overlook the potential conflict between the two cases.\(^{67}\) The confusion between *On Lee* and *Katz* led the Seventh Circuit Court of Appeals to rule in *United States v. White* that *On Lee* had been overruled by *Katz*.\(^{68}\) The Supreme Court accepted certiorari and ruled that both *On Lee* and *Katz* remained good law.\(^{69}\)


\(^{65}\) *Id.* at 749.


\(^{68}\) *United States v. White*, 405 F.2d 838, 848 (1969) (“On the basis of the constitutional principles set forth in *Katz*… we are of the opinion that the surreptitious monitoring of the defendant’s conversations was a naked violation of his rights…”).
In *White*, the suspect was convicted for illegal narcotics transactions.\(^{70}\) The evidence used to convict the suspect, James A. White, included testimony from police officers about a series of conversations he had with a government informant named Harvey Jackson. Mr. Jackson had a number of meetings with Mr. White concerning the sale of drugs; these meetings took place in Mr. Jackson’s home, Mr. Jackson’s car, Mr. White’s home, and a local restaurant.\(^{71}\) Mr. Jackson was wired for sound in a number of these meetings. The lower court held that the surreptitious recording of Mr. White’s private conversations violated his Fourth Amendment rights. Thus, *On Lee* had been overruled. The government represented an uninvited ear, and the Fourth Amendment protected Mr. White’s right to privacy in his conversations.\(^{72}\)

When the case came before the Supreme Court it was noted that the conversations in question took place before *Katz* had come down, and thus the Court could have ruled that the reasoning *Katz* was inapplicable.\(^{73}\) Instead, the Court sought to create a rule that reconciled both *On Lee* and *Katz*.\(^{74}\)

The Court distinguished *Katz* from both *On Lee* and *White* by focusing on the method by which the Government obtained information in each of these cases: “*Katz* involved no revelation to the Government by a party to the conversations with the defendant.”\(^{75}\) The problem in *Katz*

---


70 *Id.* at 748.

71 *Id.*


74 See Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 976 (2007) (arguing that a revolution in Fourth Amendment doctrine based on the Court’s holding in *Katz* was prevented by the third party doctrine).

was that the Government circumvented the third party and directly recorded the suspect’s conversation. The Court further emphasized the importance of distinguishing the cases based on method by once again reaffirming the rule that no Fourth Amendment protection exists against a third party cooperating and communicating with the authorities.  

A warrant is required when the Government makes a direct recording of a conversation, but not when a third party working for the Government makes the same recording. Presumably, if the police in Katz had contacted the third party on the other side of the telephone line and had him agree to transmit the information at issue, then they would have been able to acquire the contents of the same private conversation. This is a very strange distinction to make considering an agent acting for the Government is considered akin to the Government itself in Fourth Amendment cases. If the Government is restricted from using an improper method to obtain information, it should not be able to utilize an agent to circumvent the limits placed on them. Nonetheless, the Court in White appears to have created a two-part inquiry in cases involving third party doctrine and

---

76 Id.; Hoffa v. United States, 385 U.S. 293, 303 (1966) ("When one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard. The Fourth Amendment does not protect against unreliable (or law-abiding) associates").


79 United States v. Jacobsen, 466 U.S. 109, 113-14 (1984) ("This Court has also consistently construed this protection as proscribing only governmental action; it is wholly inapplicable "to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official." Walter v. United States, 447 U.S. 649, 662 (1980) (BLACKMUN, J., dissenting)"; See also David A. Sullivan, Note: A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology, 44 ARIZ. L. REV. 967, 975 (2002) (arguing that post-Katz technology cases are often counterintuitive).

80 But see Christopher Slobogin, Symposium Cyberspace & The Law: Privacy, Property, and Crime in the Virtual Frontier: Proportionality, Privacy, and Public Opinion: A Reply to Kerr and Swire, 94 MINN. L. REV. 1588, 1592 (2010) (arguing that the third party doctrine allows the government to engage in activities that private actors would otherwise be barred from by law).
electronic surveillance: 1) was there a knowing exposure of information; and 2) did the
Government utilize a valid method in acquiring the information.

The extent of this two pronged inquiry would be tested in the case that frames modern
third party doctrine; Smith v. Maryland.

iv. Smith v. Maryland (1979) – Voluntary Conveyance

Patricia McDonough was the victim of a robbery. She had given police a basic
description of the robber along with the make and model of car he drove. The police were able
to discover the owner of the car, Michael Lee Smith. After the robbery Ms. McDonough began
to receive threatening phone calls. The police suspected that the calls were coming from Mr.
Smith. The police, without obtaining a warrant, requested that the phone company attach a pen
register, a device which records the outgoing phone numbers dialed, to Mr. Smith’s home phone
line. The phone company’s central office recorded the numbers dialed from Mr. Smith’s phone
and discovered that he had been dialing Ms. McDonough’s number. This evidence was used to
convict Mr. Smith at trial.

Mr. Smith alleged that the recording of the phone numbers dialed from his home phone
violated the Fourth Amendment. The Court held that it did not. The Court framed its opinion
in the light of Katz, answering the question of whether a person has an expectation of privacy in


82 Stephen E. Henderson, Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment

83 Id. at 520-21 (“That device recorded all phone numbers dialed from the defendant’s residence, thus, verifying that
he was the caller of interest”).

the phone numbers dialed from a home phone.85 The opinion also analyzes, and ultimately bases its decision upon, the third party doctrine.86

The Court found that there was a voluntary conveyance of information when Mr. Smith dialed phone numbers.87 Notably, the Court replaced the term “knowing exposure” from On Lee and White with the synonym “voluntary conveyance”.88 The question of voluntary conveyance is an objective one and ignores the claims of the individual suspect. The Court found that phone users must realize that they convey their numbers to the telephone company in order to place a call.89 Once a user has dialed the phone number he has voluntarily conveyed that information to the telephone company, and the information is no longer subject to Fourth Amendment protection.

Smith argued that even if there was a voluntary conveyance of information, the method utilized by the Government in acquiring the information was improper. A pen register is a surreptitious form of electronic surveillance that records information the police would otherwise be unable to obtain; it is akin to the technology utilized in Katz. Moreover, Smith was utilizing his home phone and thus had demonstrated that he wished to keep out any uninvited eyes or ears

85 Achal Oza, Note: Amend the ECPA: Fourth Amendment Protection Erods as E-mails Get Dusty, 88 B.U.L. REV. 1043, 1048 (2008) (describing the Smith case as primarily addressing the expectation of privacy question).

86 See Jed Rubenfeld, The End of Privacy, 61 STAN. L. REV. 101, 112 (2008) (arguing that most of modern Fourth Amendment doctrine can be analyzed through the third party).

87 Nathan Petrashek, The Fourth Amendment and the Brave New World of Online Social Networking, 94 MARQ. L. REV. 1495, 1519 (2010) (“telephone users had to convey the phone numbers to the telephone company to complete the calls”).

88 These two terms have been used interchangeably in modern third party doctrine cases. Compare California v. Ciraolo, 476 U.S. 207, 213 (1986) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); Florida v. Riley, 488 U.S. 445, 449-450 (1989); with United States v. Bynum, 604 F.3d 161, 164 (4th Cir., 2010) (Bynum voluntarily conveyed all this information to his internet and phone companies); Mangum v. Action Collection Serv., Inc., 575 F.3d 935, 942-43 (9th Cir., 2009).

89 Smith v. Maryland, 442 U.S. 735, 742 (1979); See also Achal Oza, Note: Amend the ECPA: Fourth Amendment Protection Erods as E-mails Get Dusty, 88 B.U.L. REV. 1043, 1048 (2008).
Finally, the calls to Ms. McDonough were local calls, and the phone company did not have a practice of recording the numbers dialed in local telephone calls. The government acted improperly by requesting the company to take a specialized action solely for the purpose of surveillance. The Court rejected this argument wholesale.

The Court held that pen registers were a common type of technology used by the telephone company in many non-law enforcement scenarios. The fact that the suspect used the phone in his home was immaterial since he had to convey numbers to the telephone company no matter where the call originated; he had assumed the risk of this disclosure. The Court also found that the telephone company’s practices for recording numbers were not of constitutional significance. If they were, then a suspect could claim Fourth Amendment protection from record local calls but not long distance calls. The Court refused to circumscribe police practices based on such an arbitrary distinction. The mere fact that the numbers could potentially be logged – the third party had the technological capacity to do so – was sufficient.

After finding that there was no problem with the method by which the Government obtained its information, the Court mooted its entire inquiry by claiming that the sole legal and factual question is that of voluntary conveyance. The Court stated, “Regardless of the phone

---

91 Id. at 742-43.
92 Id. at 743-44.
93 Id. at 745.
94 Id.; See also Matthew D. Lawless, The Third Party Doctrine Redux: Internet Search Records and the Case for a “Crazy Quilt” of Fourth Amendment Protection, 2007 UCLA J.L. & TECH. 2, 13 (2007) (“The accepted understanding is that the third party doctrine requires knowledge of the mere technological capacity for exposure…”)
95 Achal Oza, Note: Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty, 88 B.U.L. REV. 1043, 1049 (2008) (arguing that in order to determine if an individual knowingly transmitted information to a third
company's election, petitioner \textit{voluntarily conveyed} to it information that it had facilities for recording and that it was free to record. In these circumstances, petitioner assumed the risk that the information would be divulged to police."\textsuperscript{96} In Katz, the type of technology, who authorized its use, and how it was used were the determining factors in finding that the Fourth Amendment had been violated.\textsuperscript{97} In Smith, the governing inquiry involved whether there was a voluntarily conveyance of information,\textsuperscript{98} how the information was obtained was no longer of central importance.\textsuperscript{99} Subsequent cases would all but eliminate the inquiry into the method of acquisition used by the police.\textsuperscript{100}
v. One Remaining Premise: Voluntary Conveyance

The third party doctrine began to receive criticism when it was expanded into the realm of business records.¹⁰¹ Yet, with the exception of certain carved out intimate relationships, the doctrine has only expanded in its reach.¹⁰² The inquiry into the police’s method of acquisition, however, appears to have fallen by the wayside.¹⁰³ The sole inquiry in modern third party doctrine cases has been whether the suspect voluntarily conveyed information to the public.¹⁰⁴

¹⁰¹ Orin S. Kerr, Symposium: Security Breach Notification Six Years Later: Defending the Third-Party Doctrine: A Response to Epstein and Murphy, 24 BERKELEY TECH. L.J. 1229, 1235 (2009) (claiming that these cases represent the more controversial applications of the third party doctrine); Andrew E. Taslitz, Enduring and Empowering: The Bill of Rights in the Third Millennium: The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions, 65 LAW & CONTEMP. PROB. 125, 140 (2002) (discussing Justice Marshall’s dissent in Smith, which argued that the ruling left citizens with no alternatives since they have to utilize certain business services, but by doing so they are subjecting themselves to limitless government intrusion).


¹⁰³ Joseph T. Thai, Symposium: The Jurisprudence of Justice Stevens: Panel I: Criminal Justice: Is Data Mining Ever a Search Under Justice Stevens’s Fourth Amendment?, 74 FORDHAM L. REV. 1731, 1745 (2006) (describing how there is no longer a difference between conveying information directly to police or conveying information to a third party under third party doctrine); Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 799, 829 (2004) (“Once a user discloses information to the provider, the user relinquishes any Fourth Amendment protection in the information by virtue of losing the right to exclude”).

¹⁰⁴ Thomas P. Crocker, From Privacy to Liberty: The Fourth Amendment After Lawrence, 57 UCLA L. REV. 1, 48 (2009) (“The third-party doctrine constructs a particular form of personal identity as an individual, not as a person who inhabits thick intersubjective social relations and forms of life with others. Rather, this jurisprudence protects persons who are conceptually understood to live in social isolation”); Alexander Scolnik, Note: Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment, 78 FORDHAM L. REV. 349, 355-56 (2009) (describing how the court has expanded third party doctrine based upon the voluntary conveyance inquiry); But see Matthew D. Lawless, The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection, 2007 UCLA J.L. & TECH. 2, 48-50 (2007) (arguing that modern courts have also taken into account the operational realities of the third party in determining whether to apply the third party doctrine).
In *California v. Greenwood*, the Court held that no Fourth Amendment violation occurred when police searched through suspects’ garbage cans.\(^{105}\) It was of no consequence that the police themselves opened the sealed bags and searched through them. The dispositive factor was that the suspects, “placed their refuse at the curb for the express purpose of conveying it to a third party…”\(^{106}\) In *United States v. Knotts*, the police placed a radio tracking beeper in a chloroform drum, which was purchased by one of the suspect’s co-defendants and allowed the police to track the suspect’s movements.\(^{107}\) The Court stated that the suspect, “voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction” and that therefore his location was not protected by the Fourth Amendment.\(^{108}\) The fact that the police had surreptitiously placed a beeper in a can was not relevant to the inquiry.

More recent cases before lower courts have seen the third party doctrine enter new technological fields. Prior to congressional legislation occupying the field, several lower courts held that government interception of cordless phone calls failed to implicate any Fourth Amendment concerns.\(^{109}\) A number of circuit courts have relied on third party doctrine to find that employees have no Fourth Amendment protection from searches of their office computers.\(^{110}\) In *US v. Reese*, the court held that video recordings of meetings between the

---


\(^{106}\) *Id.* at 40.


\(^{108}\) *Id.* at 281-82.


\(^{110}\) *United States v. Barrows*, 481 F.3d 1246, 1248 (10th Cir., 2007) (holding that an employee could not claim Fourth Amendment interest in his work computer because he had knowingly networked with other computers);
suspect and a confidential informant were admissible under the third party doctrine. A district court in Nevada held that the Fourth Amendment was not implicated when an undercover police officer logged in to a peer-to-peer file sharing program and downloaded child pornography videos shared by the suspect since these videos were shared with other users. Finally, a recent Fourth Circuit opinion relied on the third party doctrine to justify acquisition of the internet search records from an individuals’ home computer.

Renewed academic criticism has come as a result of courts extending the reach of third party doctrine in the Internet age. It is difficult to foresee, however, where the Court would, or could, draw the line to reign in cases governed by third party doctrine; although several commentators have attempted to guide the way.

---


114 See Joshua L. Simmons, Note: Buying You: The Government’s use of Fourth-Parties to Launder Data About “The People”, 2009 COLUM. BUS. L. REV. 950, 971 (2009) (arguing that a direct import of third party doctrine may have undesirable consequences in the internet age, because there is no alternative but to transmit information through third parties); Patricia Bellia and Susan Freiwald, Law in a Networked World: Fourth Amendment Protection for Stored E-mail, 2008 U CHI LEGAL F 121, 147-48 (2008) (arguing that the third party doctrine does not port well onto e-mail searches and criticizing the TPD in general for being a false assumption that trusting a bank means that you are giving up your expectation of privacy); WILLIAM G. STAPLES, ENCYCLOPEDIA OF PRIVACY, 458 (2007) (describing the difficulties inherent in a broad interpretation of third party doctrine in the internet age where countless companies have access to private information); Daniel J. Solove, Panel VI: The Coexistence of Privacy and Security: Fourth Amendment Codification and Professor Kerr’s Misguided Call for Judicial Deference, 74 FORDHAM L. REV. 747, 753 (2005) (arguing that the Fourth Amendment, as governed by the third party doctrine, is no longer effective to protect people’s privacy in the internet age).

B. The Application of the Third Party Doctrine to Cell-Site Searches

When a court considers the legality of government usage of prospective CSLI, there is no applicable statute, only case law will illuminate the analysis. CSLI appears to be akin to the numbers dialed in *Smith*. Location based coverage is a component of cell phone plans as evidenced by the emphasis CSPs put on advertising the comprehensiveness of their coverage. The coverage plans implicitly indicate that the location of the cell phone impacts the ability of the user to effectively use the phone. Because presumably a user seeks to use his or her device


116 See Achal Oza, *Note: Amend the ECPA: Fourth Amendment Protection Erodes as E-mails Get Dusty*, 88 B.U.L. REV. 1043, 1054 (2008) (citing In re Askin, 47 F.3d 100, 105-06 (4th Cir. 1995)).


and thus selects a CSP that provides coverage compatible with the user’s geographical demands. Indeed many users switch CSPs based on the network coverage. As a result, it seems only logical that a user understands that location impacts the effectiveness of his or her cell phone and as a consequence the location of the cell phone must be known to the CSP. By using the cell phone, we conclude then, that the user voluntarily conveys his or her CSLI to the CSP. The information provided from CSLI requests has allowed police to efficiently fight crime and even prevent crimes before they happen. Cellular service providers, in much the same way as home phone companies, have a strong interest in maintaining the privacy of their customers. CSLI requests provide information gathered by a third party. Moreover, the third party has the technological capacity to triangulate and track a person’s location through CSLI.

119 Geography in this context might mean selecting a service provider that provides better coverage in Montana than in Maine. It might also mean selecting a service provider that provides better coverage on one city block versus the next. Cellular providers are aware that their coverage can vary even within a several block radius and take steps to combat poor coverage locations. See Joseph Thornton, AT&T MicroCell = Perfect 3G Coverage, JTJDT.COM, http://jtjdt.com/atandt-microcell-perfect-3g-coverage (no date) (discussion of “horrible” apartment coverage that became “flawless” with the addition of a AT&T MicroCell).

120 See Robert Scoble, AT&T-T-Mobile: Verizon Forced This Marriage!, BUSINESS INSIDER, Mar. 20, 2011, http://www.businessinsider.com/one-bad-company-buying-another-att-buys-tmobile-verizon-forced-this-marriage-2011-3 (providing a tongue in cheek analysis of the major competitors coverage in the author’s home area, replete with mentions of coverage areas and dead zones and the author’s assertion that “lots of people will switch when their contracts are up” in order to join a carrier with improved coverage); see also Terrence O’Brien, Verizon iPhone: Slower Data, Better Coverage, SWITCHED, Feb. 3, 2011, http://www.switched.com/2011/02/03/verizon-iphone-4/ (discussing the “vastly improved” coverage available by switching from AT&T to Verizon).

121 See Anne Barnard, Growing Presence in the Courtroom: Cellphone Data as Witness, N.Y. TIMES at A16, July 6, 2009 (discussing the role cell phone tracking now plays in law enforcement investigations); Timothy Stapleton, Note: The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More Than the Sum of its Parts, 73 BROOKLYN L. REV. 383, 383-384 (2007) (describing the effective use of CSLI searches across the country); Caryn Tamber, Probable cause still rules for cell location data, Kansas City Daily Record (August 7, 2006) (citing a US attorney who describes CSLI searches as a “crucial crime-fighting tool”).


There are differences between CSLI and the numbers dialed in Smith, but the legal questions arising from these differences have been answered by the Court’s third party doctrine jurisprudence. A cell phone user signs a detailed privacy agreement with his service provider, whereas a home phone user in the early 70’s may not have signed one. The fact that a confidential relationship existed with the third party, however, does not change the analysis according to the Supreme Court’s holding in *United States v. Miller*. A cell phone user could argue that CSLI is distinguishable from the numbers dialed in Smith because it is not in the normal course of business for a cell phone company to record CSLI or triangulate the location of the cell phone by using multiple cell phone towers. The fact that the cell phone company potentially could triangulate a user’s location or record the cell phone tower data is enough according to the Court in Smith. Again, the Smith court did not look to the level of defendant’s knowledge of the phone company’s practices with regards to record dialed numbers, but rather whether the defendant voluntarily conveyed that information to the phone company. CSLI could provide information that a person is inside his home, a location deemed to be protected from government search under the Fourth Amendment. The Court in *Katz* explicitly

---


125 Supra Note 71; But See Matthew D. Lawless, *The Third Party Doctrine Redux: Internet Search Records and the Case for a “Crazy Quilt” of Fourth Amendment Protection*, 2007 UCLA J.L. & TECH. 2, 44 (2007) (arguing that Katz’s holding was premised upon the fact that the company did not normally record the contents of phone calls from pay phones and this gave the suspect a reasonable expectation of privacy in his conversation).

126 Thomas P. Crocker, *From Privacy to Liberty: The Fourth Amendment After Lawrence*, 57 UCLA L. REV. 1, 54-55 (2009) (outlining how a CSLI search could lead to information placing a suspect in his or her home and
stated, “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”127 All of these criticisms arise from concerns based in the Court’s Fourth Amendment expectation of privacy doctrine. What is essential to remember, however, is that the Fourth Amendment is not implicated when information is disclosed to a third party.128

Justice Sotomayor, in her concurrence to Jones acknowledged the Fourth Amendment implications of disclosure to a third party and indicated that it might be time to reevaluate the third party doctrine.129 Justice Sotomayor’s concurrence as well as Justice Alito’s concurrence intimated that the duration of an electronic surveillance method might be a distinguishing factor to consider in future Fourth Amendment cases.130 Thus, if a location-device is utilized for X amount of time, then the tracking method will become a search under the Fourth Amendment. Putting aside the line drawing problems with this argument, the Court already decided that method of acquisition was no longer a relevant portion of the Fourth Amendment inquiry in Smith.131

The sole question to ask is after Smith is: do cell phone users voluntarily convey their location information?

---


130 Id. at

131 Id. at 12 (describing the line drawing problems)
The answer is yes. A user of a cell phone, at least implicitly, understands that his cell phone is constantly transferring information to a cell phone tower in order to retain service. The proliferation of location-based applications for cell phones in the past five years has only made this claim stronger. A cell phone user has the capability to turn off his cell phone if he doesn’t wish to convey CSLI to his service provider. Cell phone users voluntarily convey their location information to their service provider. Therefore, CSLI searches do not implicate the Fourth Amendment.

Despite the clear similarities between CSLI and the numbers dialed in Smith, lower courts have held that CSLI searches, conducted without a warrant, violate the Fourth Amendment. These courts have either ignored the third party doctrine completely,
misinterpreted the voluntary conveyance requirement, or claimed that another Fourth Amendment consideration controls. 137

II. Application of the Third Party Doctrine

The current state of Fourth Amendment jurisprudence allows the Government to acquire CSLI absent a showing of probable cause pursuant to the third party doctrine. The number of federal courts addressing this issue continues to expand. Although magistrate judge reports and recommendations and district court opinions are the most common, circuit courts are finally addressing the question, 138 and the Supreme Court has now touched on a related issue in Jones, with one concurrence pondering the implications of cell phones. 139 This paper does not review every relevant decision, and it need not because many courts never reach the constitutional question, instead accepting or rejecting the government’s application for CSLI on purely statutory grounds. 140 This section examines how several courts that have reached the constitutional question have addressed the ramifications of the third-party doctrine.

Many, and perhaps even the majority, of CSLI application decisions avoid considering the application of the third party doctrine altogether. 141 Some courts that have omitted any mention of the doctrine have gone on to grant the government’s request for CSLI despite the lack of any

137 In re United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov’t, 534 F. Supp. 2d 585, 614-616 (W.D. Pa., 2008) (holding that CSLI is automatically transmitted during the registration process and therefore is not voluntarily conveyed); See also Timothy Stapleton, Note: The Electronic Communications Privacy Act and Cell Location Data: Is the Whole More Than the Sum of its Parts, 73 BROOKLYN L. REV. 389 n. 45 (2007) (describing two district courts with divergent rulings on the voluntary conveyance of CSLI).


140 Courts rely on a variety a statutes depending on the facts. We note that there is currently no federal statute that directly addresses the standard the government must meet to obtain prospective CSLI.

141 We note that published decisions are much more likely when a court denies the government’s request for CSLI.
showing of probable cause.\textsuperscript{142} And, at least one court has inferred that there may not be any constitutional implications from procuring a suspect’s location information via CSLI.\textsuperscript{143} Absent a Fourth Amendment question, it would be unnecessary for a court to consider and apply the third party doctrine, because the third party doctrine concerns whether an individual retains a reasonable expectation of privacy in the information at issue.\textsuperscript{144}

Nonetheless, other courts have raised Fourth Amendment concerns relative to government applications for CSLI and, yet, have still chosen to ignore the implications of the third party doctrine. Indeed, many courts proceed without any mention of the third party doctrine.\textsuperscript{145} Others explicitly decline to decide or apply the doctrine. For example, Judge Kaplan in a 2006 case in the Southern District of New York declined to decide whether the third party doctrine applied.\textsuperscript{146} He declined to determine whether the Smith principle applies to CSLI because, given the manner the government’s application presented the question, the


\textsuperscript{143} \textit{CSLI: Boston 2007}, 509 F.Supp.2d at 81 (cautioning that any decision about the constitutionality of tracking an individual via cell phone was premature and noting that even assuming the government tracked the individual into his or her home, it is not clear that the Fourth Amendment would be implicated whatsoever).

\textsuperscript{144} See 355 F.3d 942, 951 (holding that there is no “legitimate expectation of privacy in the cell-site data because the DEA agency could have obtained the same information by following [the defendant’s] car”). \textit{See also}, 2006 WL 468300 (S.D.N.Y. 2006) (rejecting government’s application for CSLI because it is not authorized by statute and never discussing constitutional concerns); 416 F.Supp.2d 390 (D. Md. 2006) (same); \textit{In re Application Of The U.S. For An Order Authorizing The Installation And Use Of A Pen Register}, 415 F.Supp.2d 211 (W.D.N.Y. 2006) (same); \textit{In re . . . , 412 F.Supp.2d 947 (E.D. Wis. 2006) (same); 396 F.Supp.2d 294, 322-23 (rejecting the government’s petition on statutory grounds, although acknowledging and rejecting the voluntary information conveyance of a cell phone user);

\textsuperscript{145} \textit{See In re Application Of U.S. For An Order}, 411 F.Supp.2d 678 (W.D. La. 2006) (discussing the Fourth Amendment concerns raised by CSLI, especially if the user were to be tracked into his private residence but omitting any discussion of the third party doctrine).

constitutional implications remained abstract. Nevertheless, the court cautioned that although Smith bars a reasonable expectation of privacy in the numbers dialed from a cell phone, “it does not necessarily follow that a cell user abandons any legitimate expectation of privacy in his or her location by carrying a cell phone that signals its presence in the network to the service provider.” Further, under the court’s analysis it is uncertain that should a constitutional violation arise—for example, if CSLI indicated the user were located in his house—the third party doctrine would stand as an antidote.

In other cases, the facts make application of the third party doctrine unnecessary. For example, in United States v. Forest, the Sixth Circuit considered whether the government violated the defendant’s constitutional rights by using CSLI to identify his location while he was traveling on a public road. However, the Forest court concluded its analysis before applying the third party doctrine. In Forest, the defendants were part of a drug trafficking scheme operating in Ohio. DEA agents tracked the defendants prior to their arrest using visual surveillance. When, however, visual contact was lost, an agent dialed the cell phone of one of the defendants and used the CSLI corresponding to the call to locate the defendants.

The Forest court found that the Government had utilized the CSLI in a manner essentially congruent to that of the data collected in Knotts. As a result, the Forest court determined that the defendant had no reasonable expectation of privacy in his location.

---

147 Id.

148 Id.

149 Id. (“Assuming arguendo that a cell phone user maintains at least some expectation of privacy in location, the government could violate Karo if it used cell site information to surveil a target in a private home that could not be observed from public spaces.”)

150 United States v. Forest, 355 F.3d 942 (6th Cir. 2004).
Nevertheless, the court noted that the defendant made a persuasive case that he had not voluntarily conveyed, “his cell site data to anyone,” because, unlike the defendant in Smith, the Forest defendant did not call anyone; instead, the agent called him and relied on CSLI associated with that phone call to aid in his apprehension. Yet, because the court deemed the government’s actions to intrude no more than those in Knotts, it concluded there was no violation of the defendant’s reasonable expectation of privacy and, therefore, declined to decide whether the defendant had voluntarily conveyed his location information through the operation of his cell phone.

When the courts do consider the third party doctrine, a broad spectrum of opinions has emerged as to the application of the doctrine to CSLI and the continued breadth of results indicates consensus may not be near. Acknowledgment by the courts of the third party doctrine does not always result in its application. Some courts acknowledge the doctrine but conclude it is not applicable under the typical facts of a CSLI application. Many courts apply the third party doctrine, but hesitantly, grudgingly, or with any number of caveats. Other courts acknowledge the third party doctrine, but conclude either explicitly or implicitly that it, given the ramifications to privacy—which we readily admit are immense—conclude that the doctrine is “misplaced” in the context of CSLI. Rarely do courts confront the third party doctrine in this

---

151 Id. at 951.

152 Id. at 952. The Forest court appears only to be considering CSLI generated during a particular phone call and not CSLI automatically generated by the phone; it quotes the defendant’s brief for the proposition that “the dialing caused Garner’s phone to send out signals.” Id. This approach is not necessarily consistent with the current understanding of CSLI, where location information generated by the cell phone could be available to the government regardless of whether any calls are placed or received by the defendant.

153 Id. at 951-952.

context without expressing some level of discomfort as to the implications of its application. We consider these various approaches here.

A. The Third Party Doctrine Does Not Apply: There is No Voluntary Conveyance

As outlined more extensively above, the third party doctrine applies when an individual voluntarily conveys information to another party.\(^{155}\) In the context of cellular phones, the third party doctrine would come into play when a cell phone user voluntarily sends his location information to his cellular service provider (CSP) in order to use his cellular telephone.\(^{156}\) Yet, despite a user’s apparent interest in allowing the CSP to facilitate communication between him and other entities via his cellular phone—evinced by powering on his phone—many courts have held that the user does not voluntarily convey his location information so as to implicate the third party doctrine.

In a recent appeal, the Third Circuit considered a government application for CSLI pursuant to the Stored Communications Act (SCA).\(^{157}\) The appellate court reversed the district court, granting the government’s application and holding that the government need not establish probable cause to compel as CSP to disclose the information.\(^{158}\)

In reaching this decision the Third Circuit did not rely on the third party doctrine for support, determining instead that the statutory language of the SCA permits disclosure of CSLI


\(^{156}\) Using a cell phone today is not just about making or receiving phone calls, as many phones are capable of text messaging, email and internet functionality, and operating a host of applications. Many of these applications provide location-based messaging, specifically advertisements, which been the focus of an increasing amount of press coverage. See *Wall Street Journal*, Apr. 22, 2011; Jan. 31 2011 articles.

\(^{157}\) *In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010) [hereinafter CSLI: Pittsburgh 2010].

\(^{158}\) Id.
Moreover, based on the court’s decision, it appears unlikely that it would have reached a similar result—permitting disclosure of CSLI—under the third party doctrine alone. In fact, the court specifically rejected the government’s assertion that compelling CSLI could never implicate constitutional concerns because the cell phone user had voluntarily shared the information with the CSP. To support this rejection, the court contrasted the cell phone user with the individuals in *Smith* and *Miller*, individuals who had voluntarily conveyed information, telephone numbers and bank records respectively, to another party:

A cell phone customer has not “voluntarily” shared his location information with a cellular provider in any meaningful way. . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn’t voluntarily exposed anything at all.

Interestingly, the court acknowledged that CSPs were required to be able “to locate phones within 100 meters of 67% of calls and 300 meters for 95% of calls” by 2012 to comply with an FCC order. Thus, even if the average user today cannot be expected to know that his cell

---

159 Id. at 313. The Third Circuit did go on to explain that the SCA provides only a minimum requirement or “floor.” Thus, a judge has the discretion to require the government to meet a higher standard. *Id.*

160 *Id.*

161 *Id.* at 317-318 (internal citation and quotation marks omitted).

phone communicates location information to his CSP, in the face of the FCC regulation and the bedrock legal principle that ignorance is no defense of the law, conclusions that cell phone users are unaware of how their phones operate may not be plausible for long, if indeed they are plausible at all. Yet, the court skirts this discussion by stating it “cannot predict the capabilities of future technologies.”

Indeed, the underlying magistrate judge’s report and recommendation (which concluded probable cause was necessary), also rejected any finding of voluntary user conveyance. The magistrate judge explained that unlike the numbers dialed in Smith, CSLI is not “voluntarily conveyed by the user to the phone company.” Rather, “[i]t is transmitted automatically during the registration process, entirely independent of the user’s input, control, or knowledge.” By focusing on the nature of the transaction, the magistrate judge was able to classify the conveyance of CSLI information as involuntary, or at least “not [voluntary] in the way of transactional bank records or dialed telephone numbers.”

The Southern District of Texas reached a similar conclusion in its 2005 Houston CSLI decision. The government sought a court order compelling a CSP to disclose CSLI,

163 Id.

164 In re: Application Of The U.S. For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government, 534 F.Supp.2d 585, 614 (W.D. Pa. 2008) (vacated by CSLI: Pittsburgh 2010). Magistrate Judge Lenihan, who first considered the application, rejected the government’s position and wrote an opinion, which was joined, interestingly, by the other court’s other magistrate judges, setting forth a warrant requirement.

165 Id.

166 Id. at 615. The magistrate also tried to distinguish the types of records to further distinguish Miller and Smith. The magistrate closes with a very interesting argument, which essentially asserts that the third party doctrine cannot apply because the information is the “subject of express Congressional protection.” Id. at 616.

analogizing the location information to the dialed telephone numbers in *Smith*.\(^{168}\) The court rejected this contention and concluded that even though cell phone users may voluntarily convey the numbers they dial, CSLI is not voluntarily given to the CSP, rather, “it is transmitted automatically during the registration process, entirely independent of the user’s input, control, or knowledge.”\(^{169}\) Yet, the court fails to mention that registration only occurs once a user has voluntarily powered on his phone or discuss how this act is distinguishable from user “input” or “control.” The court also looks to *Forest* in support of the idea that “cell site data is triggered by law enforcement’s dialing of the particular number.”\(^{170}\) The reliance on the reasoning in *Forest* is in conflict with the court’s pronouncement of automatic registration, which occurs “even when the phone is idle.” Despite the lack of a more robust analysis, the court’s point and the basis for dismissing the third party doctrine is clear: the user does not control his CSLI in any way other than powering on his cell phone\(^{171}\) and does not “know” that it is occurring.

The cell phone users described in these cases exist in sharp contrast to the Internet users who are deemed to have voluntarily conveyed information in a related body of law.\(^{172}\) And, perhaps an even sharper contrast may be drawn with the defendant in *United States v. Dantzler*, who was deemed to have a sound understanding (or so should have) that vehicles equipped with the OnStar® system, which allows a driver to contact a call-center in the event assistance is

\(^{168}\) *Id.* at 756.

\(^{169}\) *Id.* at 756-57. Magistrate Judge Smith affirmed this view in *In re Application of the United States*, 747 F. Supp. 2d 827 (S.D. Tex. 2010) [hereinafter *CSLI: Houston 2010*].

\(^{170}\) *Id.* at 757.

\(^{171}\) *Id.* at 751.

\(^{172}\) See *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir.2008); *United States v. Beckett*, 544 F.Supp.2d 1346 (S.D. Fla. 2008); 497 F.Supp.2d 117; *United States v. Warshak*, 490 F.3d 455 (6th Cir. 2007) (determining that an email user’s reasonable expectation of privacy turns at least in part on user agreements and audit policies and not merely on the idea that the email user does not know that he sends an email through an ISP).
needed, are perpetually conveying location information to the service provider. In *Dantzler*, the Western District of Louisiana denied the defendant’s attempt to suppress evidence seized as a part of traffic stop. The police requested and received support from OnStar in locating the vehicle, which, the defendant asserted, raised Fourth Amendment concerns. The court rejected this contention explaining that:

[T]he officers merely accessed information that defendant’s rented vehicle had transmitted to a third-party monitoring service.

Furthermore, [the defendant] either knew or should have known that he was renting an OnStar equipped vehicle that was capable of transmitting the vehicle’s location to a monitoring service. As a result, defendant accepted the risk that the information that the tracking system transmitted to the third-party monitoring service could be forwarded to others.

There is nothing in the court’s analysis that can be used as a guide to distinguish why a driver of a vehicle containing the OnStar system ought to understand that location information is being provided to a third party so as to enable that third party to provide information and assistance to the driver, when that same driver can not be expected to understand that his cell phone is providing similar location information to a different third party for the same or similar purposes.

B. The Third Party Doctrine Applies: “But…”

The continuing stream of court decisions on applications for CSLI without a warrant, demonstrates that the government is actively seeking this information. The state of the law is

---


175 In fact the specter of the pervasive effort by government to obtain CSLI has caused the American Civil Liberties Union to issue over 350 Freedom of Information Requests to local law enforcement agencies seeking information on the extent of the governments requests. http://www.aclu.org/technology-and-liberty/aclu-seeks-details-government-mobile-phone-tracking-massive-nationwide.
currently in flux.\textsuperscript{176} In fact, one magistrate judge observed that “caselaw developments have been outstripped by advancing technology.”\textsuperscript{177} Perhaps this uncertainty explains the caveats that so often accompany the granting of an application for CSLI to the government when there is no assertion of probable cause.

For example, Southern District of New York Magistrate Judge Gorenstein allowed the government to access prospective CSLI on the specific and articulable facts standard of the SCA.\textsuperscript{178} However, in this 2005 decision, the magistrate judge began his Fourth Amendment discussion by asserting that the government is not seeking a “virtual map” of a user’s movements but instead seeks only to identify a nearby cellular tower and possibly the face of the tower.\textsuperscript{179} Further the Magistrate Judge dismissed constitutional concerns related to Government tracking of the suspect, but asserted that government only seeks this information when the user makes or receives a phone call.\textsuperscript{180} Magistrate Judge Gorenstein, relying on \textit{Smith}, found that the “individual has chosen to carry a device and to permit transmission of its information to a third party, the carrier.”\textsuperscript{181} The magistrate judge hedged this position by declining to reach the question of whether the third party doctrine applies to CSLI obtained in the absence of a call.\textsuperscript{182}

\textsuperscript{176} See, e.g., Texas district court decisions where judge changes position over course of years.

\textsuperscript{177} \textit{CSLI: Houston 2010}, 747 F.Supp.2d 827, 830 (S.D. Tex. 2010).


\textsuperscript{179} \textit{Id.} at 449.

\textsuperscript{180} \textit{Id.} at 449.

\textsuperscript{181} \textit{Id.}

\textsuperscript{182} \textit{Id.} at 450.
Magistrate Judge Gorenstein’s 2005 opinion set the stage for other courts to agree to CSLI applications absent probable cause. In a 2006 case in the Western District of Louisiana, a magistrate judge looked to Gorenstein’s 2005 opinion and agreed to grant the government’s application seeking prospective CSLI.\(^{183}\) The magistrate judge explained that cell phones are “carried . . . and used voluntarily” and that “users know that third party service providers are aware of their general location vis-à-vis the nearest tower,” thus, if the user does not wish to convey CSLI he or she “can simply not make a call or he can turn his cell phone off.”\(^{184}\) Yet, the magistrate heavily caveated his grant to the government, allowing it to obtain CSLI only when a call was in progress and from a single tower, which was all the government sought in this instance.\(^{185}\)

The magistrate judge’s recommendation in *United States v. Suarez-Blanca*, to deny the defendant’s motion to suppress historical CSLI exhibited similar caveats. In *Suarez-Blanca*, the government obtained two cell phones during a drug seizure. It then filed an application for the release of historical cell site information for five cell phone numbers. When the defendant challenged the government’s failure to demonstrate probable cause, the court *sua sponte* looked to the third party doctrine to support its finding that the government did not violate the defendant’s Fourth Amendment rights.\(^{186}\) Starting its analysis with *Smith* and detailing the many applications of the third party doctrine from bank records to credit card, utility, motel, cell phone, and employment records, the court determined that there was “little distinction between


\(^{184}\) *Id.* at 683.

\(^{185}\) *Id.* at 679-80.

historical cell site information retained as business records and the records from banks and utilities."\(^{187}\) Relevant to our analysis, it determined that “a cell phone user voluntarily dials a number and as a result voluntarily uses the cell phone provider’s towers to complete the number.” By voluntarily using the equipment, the cell phone user runs the risk that the records concerning the cell phone call will be disclosed to police."\(^{188}\) Because the court concluded that CSLI was just like any other record, it determined that “individuals do not have an expectation of privacy” and “there can be no Fourth Amendment violation based on law enforcement’s decision” to seek these records.\(^{189}\) Like the other decisions detailed above, the Suarez-Blanca court also took the time to add several caveats: namely, that any concerns about the government calling the targeted phone numbers, a la Forest, or about automatic transmission were not present here because the government sought only information tied to specific calls made by the user from the targeted phones.\(^{190}\) Accordingly, there was no doubt that the defendants voluntarily conveyed the information sought. Further, the Suarez-Blanca court noted that there had been no showing the government used the CSLI to triangulate the location of the defendant while he was in private quarters and thus, it was not clear that the Fourth Amendment was implicated at all.\(^{191}\)

C. The Third Party Doctrine is Alive and Well

\(^{187}\) Suarez-Blanca, 2008 WL 4200156 at *8.

\(^{188}\) Id.

\(^{189}\) Id.; see also United States v. Benford, No. 2:09-CR-86, 2010 WL 1266507 (N.D. Ind. 2010) (relying on Suarez-Blanca to deny a motion to suppress CSLI acquired by the government without a showing of probable cause).

\(^{190}\) Id. at *9.

\(^{191}\) Id. at *10. The Suarez-Blanca court implies that a different analysis might be appropriate if the police had instigated contact. This line of reasoning would be supported by the Sixth Circuit’s holding in Forest, which emphasized the fact that the defendant had been telephoned by the police. Yet, Smith, appears to indicate that the method of conveyance is not relevant to the analysis.
In late 2012, the Sixth Circuit decided *United States v. Skinner*. Although never explicitly naming the third party doctrine, the court stated clearly that the defendant lacked a reasonable expectation of privacy in data given off by his voluntarily procured cell phone and relied on *Smith*.

In *Skinner*, DEA authorities “continuously ‘pinged’” the pay-as-you-go cell phone of a yet-unidentified drug runner. Using the location data from the phone, DEA authorities determined that the drug runner had stopped somewhere near Abilene, Texas. Agents were dispatched to a truck stop in the area and identified the motorhome thought to contain the drugs. The authorities approached the motorhome, knocked on the door, and spoke to the defendant, who declined to let the agents enter the motorhome. Following an alert from a drug dog, the agents entered the motorhome and discovered over 1,100 pounds of marijuana, two cellular telephones, and two semi-automatic weapons. On appeal, the defendant challenged the use of his location information as a warrantless search that violated his Fourth Amendment rights. The court squarely rejected his argument, stating, “[t]here is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone.”

The court was unequivocal that the defendant suffered no constitutional violation, decrying his position by saying, “[t]he law cannot be that a criminal is entitled to rely on the expected untrackability of his tools.”

---


193 It is unclear from the court’s opinion whether the DEA authorities involved were relying on CSLI or GPS data. See *id.* at 776 (describing “pinging” the phone, a technique often associated with generating CSLI data, and also referring to GPS).

194 With respect to the defendant’s Fourth Amendment rights, the district court adopted the magistrate judge’s report and recommendation, which concluded that the defendant lacked standing to bring a Fourth Amendment challenge because the cell phone was not subscribed to him (it was pay as you go), and further opined that because the defendant had no reasonable expectation of privacy because the cell phone was utilized on public roads and was bought by a drug supplier and provide to the defendant. *Id.* at 776.

195 *Id.* at 777.

196 *Id.*
its point, the court compared a contrary holding to barring dogs from tracking fugitives when fugitives do not know that the hounds have his scent, or preventing authorities from using a license plate to track a vehicle when the driver does not know that his plate has been spotted.\textsuperscript{197} The Sixth Circuit explained that its decision was directly supported by \textit{Knotts} and \textit{Smith}. And although the \textit{Skinner} court never explicitly mentions the third party doctrine, the \textit{Skinner} court endorses its reasoning. The \textit{Skinner} court explains that the Supreme Court in \textit{Smith} compared the technology at issue--automated dialing--to giving numbers to a telephone operator, where numbers given to a telephone operator could not later be claimed confidential. As discussed above, the Supreme Court declined to hold that there was constitutional protection simply because the phone company had automated its system, i.e. the defendant did not have constitutional protection in the information he gave to the phone company simply because he was not giving it directly to a person. Considering this holding in \textit{Smith}, the \textit{Skinner} court applied the principal and stated, “[s]imilar reasoning compels the conclusion here that Skinner did not have a reasonable expectation of privacy in the location of his cell phone while traveling on public thoroughfares.”\textsuperscript{198}

Post \textit{Skinner}, certainly courts in Michigan, Ohio, Kentucky, and Tennessee will be more apt to find that a defendant lacks Fourth Amendment protections in location information generated by his cellular phone.

D. Or Is It? - The Third Party Doctrine is Misplaced in the CSLI context

Courts that concede a user voluntarily conveys CSLI to the CSP when his phone is powered on, but which choose not to wholeheartedly endorse the third party doctrine, may find

\textsuperscript{197} \textit{Id.}
\textsuperscript{198} \textit{Id.} at 778.
some cover in the D.C. Circuit’s discussion and analysis in *United States v. Maynard*. The judgment of which was affirmed by the Supreme Court in *Jones*.\(^\text{199}\)

In *Maynard*, the court was confronted with a twenty-four hour, four week long surveillance project made possible by a GPS unit the government installed on the defendant’s vehicle without a valid warrant.\(^\text{200}\) The defendant argued that the GPS surveillance violated his reasonable expectation of privacy under *Katz*, while the government maintained that *Knotts* controlled the analysis.\(^\text{201}\)

The *Maynard* court rejected the government’s contention and determined that *Knotts* was not controlling. Explaining that the Supreme Court had “explicitly distinguished between the limited information discovered by use of the beeper—movements during a discrete journey—and more comprehensive or sustained monitoring of the sort at issue in this case” the *Maynard* court emphasized that the Court “specifically reserved the question whether a warrant would be required in a case involving ‘twenty-four hour surveillance . . . .’”\(^\text{202}\) “In short, *Knotts* held only that ‘[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another,’ not that such a person has no reasonable expectation of privacy in his movement whatsoever, world without end, as the Government would have it.”\(^\text{203}\)

Although several other appellate courts had held that the tracking of suspects with GPS without a warrant was permissible pursuant to *Knotts*, the *Maynard* court squarely

---


\(^{201}\) *Id.*

\(^{202}\) *Id.* at 556.

\(^{203}\) *Id.* at 557 (quoting *United States v. Knotts*, 460 U.S. 276, 281 (1983)).
rejected using the opinions as persuasive precedent on the grounds that the courts misconstrued the question actually withheld by the Supreme Court in \textit{Knotts}—that of prolonged surveillance.\textsuperscript{204}

Without \textit{Knotts} directing the panel’s holding, it looked to \textit{Katz}. Focusing on whether the defendant had exposed the information to the public in order to determine whether he had a reasonable expectation of privacy, the panel emphasized two considerations as evidence that a reasonable expectation of privacy existed under the circumstances.\textsuperscript{205} First, the panel concluded that “unlike one’s movements during a single journey, the whole of one’s movements over the course of a month is not actually exposed to the public because the likelihood anyone will observe all those movements is effectively nil.”\textsuperscript{206} The court was explicit that a reasonable person does not expect another to follow him day in and day out, week after week, or in the court’s more colorful language, no one anticipates being dogged like prey, such that his entire life is exposed.\textsuperscript{207} Moreover, even if each of the suspect’s individual movements was actually exposed to the public, via public location, public forum, etc., that would not necessarily constitute “exposure” to the public sufficient to eliminate the suspect’s reasonable expectation of privacy. Because, “[w]hen it comes to privacy . . . precedent suggests that the whole may be more revealing than the parts.”\textsuperscript{208} The \textit{Maynard} court explained that:

\textsuperscript{204} \textit{Id.} at 558 (“In each of these three cases the court expressly reserved the issue it seems to have thought the Supreme Court reserved in \textit{Knotts}, to wit, whether ‘wholesale’ or ‘mass’ electronic surveillance of many individuals requires a warrant. \textit{Marquez}, 605 F.3d at 610; \textit{Pineda-Moreno}, 591 F.3d at 1216 n.2; \textit{Garcia}, 474 F.3d at 996. As we have explained, in \textit{Knotts} the Court actually reserved the question of prolonged surveillance.”)

\textsuperscript{205} \textit{Id.}

\textsuperscript{206} \textit{Id.}

\textsuperscript{207} \textit{Id.} at 561.

\textsuperscript{208} \textit{Id.}
Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one’s not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts.\(^{209}\)

As a result, the Maynard court concluded that the prolonged surveillance at issue revealed more than a reasonable person expects others to know or observe.\(^{210}\) So despite the potentially public nature of the defendant’s conduct, he had not exposed his life or his actions, at least cumulatively, to the public.

Further, the court concluded that the defendant had a reasonable expectation of privacy in the “mosaic” of information comprising his life. The Maynard court reminded readers that Katz stands for the proposition that an individual may preserve privacy even in public areas,\(^{211}\) and, thus, determined that, because the prolonged use of the GPS device of the suspect for week after week “reveal[ed] an intimate picture of the subject’s life that he expects no one to have,” the invasion violates society’s reasonable expectation of privacy.\(^{212}\) Indeed, the Fourth Amendment provides a privacy zone for each person that is “‘bounded by the individual’s own reasonable

\(^{209}\) Id. at 562 (footnote omitted).

\(^{210}\) Id. at 563.

\(^{211}\) Id. at 564 (citing Katz, 389 U.S. at 351); see also id. at 564 (citing Reporters Comm. For Freedom of Press v. A.T. T., 593 F.2d 1030, 1042-42 (1978) (“Fourth Amendment . . . secur[es] for each individual a private enclave, a ‘zone’ bounded by the individual’s own reasonable expectations of privacy.”)).

\(^{212}\) Id. at 563-64.
expectations of privacy.’”  

Moreover, the court concluded that “[s]ociety recognizes Jones’s expectation of privacy in his movements over the course of a month as reasonable.”

As noted previously, in Jones the Supreme Court affirmed the judgment in Maynard, but did not rely on, or affirm, the reasoning used by the Third Circuit. And while the majority relied only on the physical trespass committed by the police in placing the GPS unit on the defendant’s vehicle, five justices expressed some concern about the duration of police surveillance. Thus, this idea of a time based, or “mosaic based” trigger, may remain as courts consider the third party doctrine.

Magistrate Judge Orenstein of the Eastern District of New York considered the implication of the Maynard decision to CSLI requests. Before the court was an ex parte application filed by the government that sought an order requiring a CSP to disclose CSLI for a cellular phone over a 58-day period. While the government submitted that the facts of the case indicated it had probable cause to support its request, the government chose to rely

---


214 Id. at 563.


The court’s analysis is provided to demonstrate how courts are addressing this issue. This decision was overturned and the government application was granted by a separate order. 2010 WL 5814659.

217 Id.
exclusively on the authority of the SCA, which requires the lesser showing of specific and articulable facts.\(^{218}\)

Magistrate Judge Orenstein acknowledged that although he had previously granted similar requests, the evolving legal landscape required him to change his position and deny the request.\(^{219}\) He explained that while the federal appellate courts had allowed these requests pursuant to *Knotts*, he was now unwilling to grant government applications for historical CSLI.\(^{220}\) However, Magistrate Judge Orenstein noted that the *Maynard* decision eliminated the uniformity with which federal appellate courts have treated the *Knotts* precedent and is reflective of “a growing recognition, at least in some courts, that technology has progressed to the point where a person who wishes to partake in social, cultural, and political affairs of our society has no realistic choice but to expose to others, if not to the public as a whole, a broad range of conduct and communications that would previously have been deemed unquestionably private.”\(^{221}\)

Magistrate Judge Orenstein deemed persuasive the *Maynard* court’s reasoning that *Knotts* reserved judgment not “as to whether wholesale or mass electronic surveillance of many individuals requires a warrant,” but instead reserving the question of the legality of prolonged surveillance.\(^{222}\) Nevertheless, he acknowledged the factual differences between acquiring

\(^{218}\) *Id.* at 579.

\(^{219}\) *Id.* at 580.

\(^{220}\) *Id.* at 581 (citing *United States v. Marquez*, 605 F.3d 604 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010), reh’g en banc denied, 617 F.3d 1120 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007)).

\(^{221}\) *Id.* at 582 (citing *Maynard*, 615 F.3d at 561, &n.*, 564-65; *Warshak v. United States*, 490 F.3d 455, 473 (6th Cir. 2007); 534 F.Supp. 2d at 610-16.

\(^{222}\) *Id.* at 583 (citing *Maynard*, 615 F.3d at 556 (citing *Knotts*, 460 U.S. at 283-85)); see also *id.* at 584.
information from a government placed GPS unit and seeking information conveyed to a third-party CSP. Indeed, the government attempted to distinguish *Maynard* on this ground, arguing that “it seeks nothing from [the suspect], but instead seeks information that [the suspect] necessarily revealed to the mobile communication service provider when he used the subject telephone” and relying on *Miller* and *Smith* in support.\(^{223}\)

Magistrate Judge Orenstein begins his discussion of the third party doctrine by acknowledging straight-away that “*Maynard* provides no answer to [the government’s assertion of the third party doctrine] but other equally persuasive cases do.”\(^{224}\) Specifically, Magistrate Judge Orenstein relies on *Warshak* and *CSLI: Houston 2005*.\(^{225}\)

In *Warshak*, the government appealed a preliminary injunction that prohibited it from acquiring the contents of personal email accounts maintained by a particular ISP without first providing notice to the subscriber.\(^{226}\) Although acknowledging that voluntarily conveying information to a third party likely negates any reasonable expectation of privacy,\(^{227}\) the Sixth Circuit set forth a two-part inquiry to determine whether an email user maintained a reasonable expectation of privacy.

---

\(^{223}\) *Id.* at 586.

\(^{224}\) *Id.* at 586.

\(^{225}\) *Warshak v. United States*, 490 F.3d 455 (6th Cir. 2007), vacated en banc on other grounds, 532 F.3d 521 (6th Cir. 2008); *CSLI: Houston 2005*.

\(^{226}\) In *Warshak*, the government appealed a preliminary injunction, which prohibited it from acquiring the contents of personal email accounts maintained by a particular ISP without first providing notice to the subscriber. The Sixth Circuit affirmed the district court’s injunction on the basis that the district court had “correctly determined that e-mail users maintain a reasonable expectation of privacy in the content of their e-mails.” *Warshak*, 490 F.3d at 482.

\(^{227}\) *Id.* at 469 (citing *Miller*, 425 U.S. at 442; *S.E.C. v. Jerry T. O’Brien, Inc.*, 467 U.S. 735, 743 (1984)).
expectation of privacy in his email content.\textsuperscript{228} First, a court “must specifically identify the party with whom the communication is shared, as well as the parties from whom disclosure is shielded.”\textsuperscript{229} Second, the court must inquire into “the precise information actually conveyed to the party through whom disclosure is sought or obtained.”\textsuperscript{230}

Magistrate Judge Orenstein appears to include each step of the \textit{Warshak} court’s inquiry in order to provide the reader with a reason to view with skepticism the government’s third-party doctrine argument. He reasons that in \textit{Warshak} the Sixth Circuit explained “that sharing information with an intermediary that merely has the ability to access the information cannot erode all expectations of privacy” and lists “the contents of phone conversations, letters, and safe deposit boxes” as examples of this position.\textsuperscript{231} Further “simply because the phone company or the ISP \textit{could} access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course.”\textsuperscript{232}

Further, Magistrate Judge Orenstein observes that other courts have been explicit in their rejection of the third-party doctrine in the CSLI context. In particular he relies on \textit{CSI: Houston} (2005), which rejected the third-party doctrine, as described above, on the grounds that the user does not voluntarily convey location information as this information is transmitted

\textsuperscript{228} \textit{Id.} at 469 (“The distinction between \textit{Katz} and \textit{Miller} makes clear that the reasonable expectation of privacy inquiry in the context of shared communications must necessarily focus on two narrower questions than the general fact that the communication was shared with another.)

\textsuperscript{229} \textit{Id.} at 470.

\textsuperscript{230} \textit{Id.} at 470.


\textsuperscript{232} \textit{Id.}
automatically. Magistrate Judge Orenstein also notes that the Wireless Communication and Public Safety Act of 1999 “expresses legislative approval for the idea that a caller should expect her location information to remain private notwithstanding the unavoidable need to share it with a third-party service provider.” Correspondingly, Orenstein concludes that “it is questionable to assume, as a general matter, that a person can never have a reasonable expectation of privacy in information that by its nature, must be shared with a third-party service provider,” and more so in the cell phone context. Thus, Orenstein further concludes that the differences between GPS tracking and CSLI location information did not foreclose applying Maynard in the CSLI context.

It is worth noting, that Judge Orenstein concludes his analysis with a discussion about users and technology. He explicitly states that he does “not assume that persons who use mobile telephones are unaware of the fact that by doing so they expose themselves to location tracking.” In fact, Orenstein outlines how the increasing use of location based applications like social check-in services, mobile advertising, and GPS applications as well as the corresponding privacy-alerts affiliated with these programs make it unlikely that consumers are unaware that their mobile device generates location information. Yet, Orenstein asserts that companies “by focusing consumer awareness on privacy concerns about location-tracking [via privacy alerts] and simultaneously seeking to reassure people about that concern, the companies providing such services appear to be fostering an actual-and to my mind reasonable-expectation

233 Id. at 588 (citing 396 F. Supp. 2d at 756).

234 Id. at 589. Magistrate Judge Orenstein notes the tension that exists between his construction of the Congressional “expression” and the Supreme Court’s construction of the third party doctrine: “If [Miller] means that there can never be a reasonable expectation of privacy in any form of information that, by its nature, must be shared to some extent with a third party to make it usable, then the government’s position here is correct-but it is also irreconcilably at odds with the notion that the Fourth Amendment allows our society to continually develop and refine its definition of the privacy claims it wishes to endorse.”

235 Id. at 589.

236 Id. at 592.
that such information will remain private to the extent a subscriber chooses to make it so."\textsuperscript{237} In other words, Orenstein contends that the interaction between CSPs and customers is actually fostering the idea that location information is private.\textsuperscript{238} It is no surprise then that Magistrate Judge Orenstein concludes that the government’s reliance on the third-party doctrine is misplaced in the context of CSLI.\textsuperscript{239}

Yet, despite Magistrate Judge Orenstein’s thorough opinion, there remains disagreement over whether the third party doctrine has a place in CSLI application requests. Recently, the Maryland District Court issued an order and opinion in \textit{CSLI: Maryland 2012}, which grants the government’s application for CSLI based on the third party doctrine.\textsuperscript{240} In \textit{CSLI: Maryland 2012}, acknowledged Magistrate Judge Orenstein’s analysis, but concluded that CSLI is a business record voluntarily conveyed to the CSP and thus falls within the ambit of the third party doctrine. Although the court was careful to note that its order applied only to the application, which requested historical cell site information, it explained that this information fell clearly within the bounds of \textit{Smith} and \textit{Miller} as records collected in the normal course of business,

\textsuperscript{237} \textit{Id.} at 593 n.19.

\textsuperscript{238} As we will discuss in some additional detail below, the amount of information available to consumers through their CSPs and in the media about location information, causes us to view with skepticism any claim that cell phone uses are unaware that the location information is generated by their cell phones. So we are heartened to see someone like Magistrate Judge Orenstein thoughtfully reach a similar conclusion. We note with some curiosity that this conclusion appears to conflict with decisions like \textit{CSLI: Houston 2005} (upon which Magistrate Judge Orenstein relied) that claim there is a reasonable expectation of privacy in CSLI in part because users do not understand that they are conveying location information whenever the phone is powered on.

Additionally, we observe (based on only our own perceptions) that the social discussion about privacy as it relates to cell phones, cell phone applications, and other related electronic and web based applications does not provide any reassurance that entities privy to the intimate details of our lives are committed to fostering a level of privacy we might wish for or even expect. \textit{See}, e.g., Julia Angwin and Jeremy Singer-Vine, \textit{Selling You On Facebook}, (Apr. 8, 2012), available at: http://online.wsj.com/article/SB10001424052702303302504577327744009046230.html.


which may end up in the hands of law enforcement. The opinion acknowledged that a time
based trigger or mosaic trigger may well end up becoming a required consideration under the
Fourth Amendment, but, despite the five justices who would seem to support it in Jones, it is not
the current law. Thus, until the third party doctrine is expressly limited with respect to CSLI, it
requires that government be able to access CSLI records from CSPs without a warrant.

As one of the first post-Jones, CSLI opinions, it is clear that the CSLI: Maryland 2012
court understands the tension created by Jones with respect to CSLI applications. The majority
and the concurrences make clear that the Jones’s decision does not apply in circumstances where
there is no physical trespass. 241 Justice Sotomayor’s concurrence emphasizes that prolonged,
electronic surveillance is problematic under the Fourth Amendment’s reasonable expectation of
privacy test and perhaps especially problematic given the proliferation of cell phones. And,
indeed, the concurrence’s discussion may breathe life into the Maynard analysis, which is
otherwise no longer controlling law. Furthermore, the Maynard mosaic analysis and its CSLI
progeny appear to be bolstered by the Supreme Court’s analysis in Katz and the majority’s
affirmation that Katz remains good law in situations lacking a physical trespass. As discussed
previously, the Katz Court set forth the now axiomatic instruction that the Fourth Amendment
protects people, not places, and affirmed that what an individual “seeks to preserve as private,
even in an areas accessible to the public, may be constitutionally protected.” 242 If it is true that
the Court was able to recognize Katz’s expectation of privacy, merely because he shut the door
to the telephone booth, it seems plausible that an individual, going about his daily life, who
repeatedly takes affirmative action to shield himself from prying eyes and ears, could similarly


242 Katz, 389 U.S. at 351-52.
uphold the reasonable expectation of privacy in the face of CSLI tracking. The Jones concurrences highlight this point and make clear that the question of whether the Fourth Amendment’s protection of a reasonable expectation of privacy remains open in the case of electronic surveillance of cell phones. And as a result, the question of whether the third party doctrine applies also remains at play.

III. Searching for a Limiting Principle

As Part II demonstrates, courts are uncomfortable applying the third party doctrine to modern electronic surveillance using CSLI. Some courts have avoided the constitutional question in favor of an alternative statutory approach, while others have questioned the degree of voluntariness necessary to trigger the third party doctrine, and still others have argued that the third party doctrine is anathema to the kind of continuous and pervasive surveillance permitted by CSLI.243 Thus, Part III begins by asking whether the legislative branch can provide a solution to this dilemma. With the federal courts in disarray over how to approach to the third party doctrine and law enforcement’s collection and use of CSLI, Congress may be well positioned to decisively answer what standard must be required of law enforcement. Following that discussion, we suggest that the Supreme Court reinvigorate the dragnet doctrine as a means of limiting the use of warrantless CSLI searches, and identify two alternative proposals, one that addresses CSLI through applying a proportionality test, and another, which limits the applicability of the third party doctrine. We outline the merits of these approaches, and conclude by discussing the likelihood and merits of potential legislation and the aforementioned approaches.

243 Supra Section II.
A. Limiting Legislation

This article has largely assumed that courts will delineate the boundaries of the Fourth Amendment relative to CSLI applications and, thus, establish whether probable cause is required. Congress, however, has increased its attention to mobile privacy in recent years. One bill, introduced by Rep. Ed Markey of Massachusetts during the 112th Congress, would have imposed transparency requirements on CSPs and device manufacturers related to how they collect information from their customers and what tools they use to do so.244 Another bill, sponsored by Sen. Al Franken of Minnesota during that same session, solely addressed the collection of CSLI by private individuals like mobile application developers and CSPs, ignoring the collection of that information by government entities.245

Meanwhile, other legislators have offered substantive bills designed to directly address the government’s warrantless collection of CSLI and that would determine, independently from the courts, what level of proof the government must provide when demanding this information from CSPs.

i. CSLI Bills in the 113th Congress

Senator Ron Wyden of Oregon and Representative Jason Chaffetz of Utah co-authored the Geolocation Privacy and Surveillance (GPS) Act, introducing it in March of 2013. The GPS Act is designed to follow the approach already used in the regulation of electronic communications surveillance.246 The bill would establish a warrant requirement for the collection or required disclosure of location-related data, such as CSLI, and impose an

exclusionary rule on illegally obtained data.\textsuperscript{247} Moreover, it would allow cell phone companies and other service providers to use location information for applications, but not without the consent of the user and not beyond the scope of that consent.\textsuperscript{248} The GPS Act, like the other federal laws that govern electronic communications surveillance, permits the government to collect location-related information after obtaining a warrant based on a finding of probable cause.\textsuperscript{249}

The GPS Act is an important legislative proposal because of its sweeping coverage. The bill addresses location-related information services pertaining to a range of devices, from vehicle navigation devices and other GPS devices to cell phones and laptops, and also includes within its proscriptive scope all individuals - private and government alike.\textsuperscript{250} Despite such broad limitations on the collection or compelled disclosure of this information, the government is still able to use an emergency exception.\textsuperscript{251} Under that exception, the government may gather location-related information if the principal prosecuting attorney reasonably concludes that an emergency exists, which involves the threat of serious injury to a person, or a conspiracy relating to national security or organized crime.\textsuperscript{252} The attorney would be required to file an application for a court order permitting that interception within 48 hours after the “interception has occurred or begins to occur.”\textsuperscript{253} Inclusion of this type of provision may be critical to the eventual passage

\textsuperscript{247} Geolocational Privacy and Surveillance Act, H.R. 1312, 113th Cong. (2013) (hereinafter GPS Act). This bill was first introduced in the previous session of Congress but did not proceed out of committee.

\textsuperscript{248} \textit{Id.} at §2.

\textsuperscript{249} \textit{Id.}

\textsuperscript{250} \textit{Id.}

\textsuperscript{251} \textit{Id.}

\textsuperscript{252} \textit{Id.}

\textsuperscript{253} \textit{Id.}

56
of the bill, as it is unlikely that Congressional members would support legislation that crippled law enforcement from using every available tool to seek and locate missing or endangered persons.254

Sen. Wyden and Rep. Chaffetz are not alone in working to devise a legislative solution to this contentious issue. California Congresswoman Zoe Lofgren introduced the Online Communications and Geolocation Protection Act in March of 2013. Rep. Lofgren’s bill is aimed at reforming the Electronic Communication Privacy Act (ECPA) in its entirety. A law enacted in 1986, ECPA governs law enforcement’s acquisition of the wire and electronic communications of American citizens.255 Rep. Lofgren’s legislation specifically includes provisions related to the collection and use of CSLI.256 Devices covered by the geolocation information provisions include cell phones, GPS devices, laptop and tablet computers, and similar equipment or devices.257 The bill requires law enforcement to obtain a warrant before either seeking CSLI from a CSP or intercepting such information itself.258 It also contains an exigent circumstances exception for the warrant requirement that is identical to the one found in the GPS Act.259 A notable difference between the Online Communications Act and the GPS Act however is that the former primarily focuses on government entities, while, as noted above, the GPS Act covers both

255 Supra, note 244.
256 Online Communications and Geolocation Protection Act H.R. 983, 113th Cong. (2013) [hereinafter Online Communications Act]. A previous iteration of Lofgren’s bill, called the ECPA 2.0 Act of 2012, was introduced in September 2012 but died in committee.
257 Id. at § 3.
258 Id.
259 Id.
governmental and private entities. However, the Online Communications Act does contain a provision forbidding service providers from divulging CSLI to government entities, unless that information is obtained in accordance with the Act or Section 222(d) of the Communications Act, or with the consent of the person in question, or is obtained inadvertently by the service provider but nevertheless “appears to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.”

In addition to Rep. Lofgren’s efforts, Sen. Leahy has been an ardent proponent of ECPA reform, and advocated legislation that included a warrant requirement for law enforcement acquisition of geolocation information. In May of 2011, Sen. Leahy introduced the Electronic Communications Privacy Act Amendments Act of 2011, a comprehensive reform package, but for a year after its introduction he was unable to secure a hearing on the bill. The ECPA Amendment Acts required law enforcement to obtain a warrant before compelling service providers to disclose contemporaneous or prospective CSLI, but not for historical CSLI. In March 2013, Senator Leahy introduced a revised version of his bill, though this bill removed all provisions related to geolocation information. During the bill’s markup session in the Senate Judiciary Committee, Senator Grassley remarked that although references to geolocation information were absent from the ECPA Amendments Act, the bills in the House included such provisions and that their addition to the Senate bill would necessitate a hearing to further study

260 Id.

261 Id.


263 ECPA Amendments Act at § 6.

the issue. Nevertheless, the Judiciary Committee voted to advance the bill to the full Senate for consideration.\textsuperscript{265}

In many respects, the GPS Act and the Online Communications Act are well-measured solutions to the growing privacy concerns relating to CSLI. First, the two bills fit neatly into the existing framework for regulating electronic information. This means that law enforcement and courts will not be starting from scratch. Second, the bills balance the interests of the government, industry, and private citizens. The legislation takes into consideration the fact that location-related information has become inseparable from many peoples’ lives. By permitting companies to continue to collect and store such information, the bills avoid interfering with the ability of companies to continue providing services that consumers are increasingly demanding. For instance, Section 2602 of the GPS Act provides that companies may continue to collect geolocation information so long as the customer consents to such use.\textsuperscript{266} Yet mere fact that a customer has consented to such use does not obviate the government’s warrant requirement, however. Section 2602(h) explicitly states that “[a] governmental entity may...require disclosure by a provider of covered services of geolocation information only pursuant to a warrant...”\textsuperscript{267} As noted above, since the Online Communications Act largely focuses on law enforcement’s collection of CSLI, it thereby evades concerns that businesses may be prevented from providing popular services to their customers.

Despite the bipartisan support received by the GPS Act and support for similar bills, the likelihood of passing legislation of this nature is uncertain. The House Judiciary Subcommittee

\begin{footnotesize}
\begin{itemize}
\item[\textsuperscript{265}] Brendan Sasso, \textit{Senate Judiciary Panel Votes To Require Warrants For Police Email Searches}, \textit{The Hill’s Hhillicon Valley}, Apr. 25, 2013, available at \url{http://thehill.com/blogs/hillicon-valley/technology/296149-senate-committee-votes-to-require-warrant-for-email-searches}.
\item[\textsuperscript{266}] GPS Act §2.
\item[\textsuperscript{267}] \textit{Id.} (notwithstanding the exigent circumstance exception found in the amended Section 2604).
\end{itemize}
\end{footnotesize}
on Crime, Terrorism, and Homeland Security held a hearing on the GPS Act in May of 2012. During that hearing, the Subcommittee’s Chairman Rep. James Sensenbrenner said that by setting “uniform legal authorities” for acquiring CSLI, the GPS Act “does what the Supreme Court invited, or challenged, the legislative branch to do when they decided the *Jones* case earlier this year,” further noting that the bill strikes the right balance between the needs of law enforcement and privacy interests of Americans.” Rep. Dan Lungren, another Republican, was somewhat less persuaded of the bill’s merits, pointing to society’s apparent cognitive dissonance on privacy, with many people readily sharing information on Facebook while maintaining a different expectation of privacy in other matters like the geolocation of their cell phone.

Representatives from law enforcement expressed concerns over the bill during the hearing. State’s Attorney for Harford County, Maryland Joseph Cassilly, speaking on behalf of the National District Attorneys Association, argued that while uniform rules are necessary, the probable cause standard set by the GPS Act is too high and would hurt law enforcement’s investigative efforts. Jon Ramsey, National Vice President of the Federal Law Enforcement Officers Association echoed Cassilly’s sentiments, stating that “[l]aw enforcement should not be further hindered during their investigation of time sensitive cases that may involve the threat of serious bodily harm or death by imposing additional legal hurdles.” Although ECPA reform

---


269 *Id.* at 71. This is understandable given the rapid pace of technological development. *See*, *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (discussing how “dramatic technological change may lead to periods in which popular expectations [of privacy] are in flux and may ultimately produce significant changes in popular attitudes.”).

270 GPS Act Hearing, *supra* note __, at 270.

271 *Id.* at 25.
efforts have generally been met with stiff opposition from law enforcement, the momentum this year appears to be on the side of reform proponents, suggesting either Lofgren’s Online Communications Act or the GPS Act may gain traction during the 113th Congress. However, other ECPA reform bills introduced in the House in May of 2013 have followed the Senate’s lead and do not contain provisions relating to geolocation information, raising doubts that geolocation privacy measures would be included in an eventual ECPA reform bill.

Outside of the aforementioned bills, another wrinkle to the legislative milieu is the Fourth Amendment Preservation and Protection Act of 2013, introduced by Senator Rand Paul of Kentucky in May 2013. The three-page bill bypasses ECPA and CSLI issues and instead effectively abandons the third party doctrine altogether. It restricts government access to records held by third parties to situations in which the subject of the investigation has given their consent to the disclosure of those records or the government has obtained a probable cause warrant to access them. While laudable for its simplicity, Paul’s bill would undoubtedly face stiff opposition from law enforcement and other government agencies that use the doctrine to conduct investigations. Still, if Sen. Paul’s bill manages to garner a hearing by the Senate Judiciary Committee, it would prompt some helpful discussions about the scope of the third-party doctrine and ideas about constraining its use.

---


275 Id. at §4.
ii. Potential Obstacles to Legislation

The state of California’s recent experience with attempting to enact legislation related to CSLI demonstrates the difficulties associated with legislative action in this area. Over the summer of 2012, the California legislature approved a bill that would require state law enforcement to obtain a warrant before obtaining CSLI through a service provider.\textsuperscript{276} The bill also required that the permitted period for a search warrant not exceed thirty days, but allowed for law enforcement to seek an extension from a judge or magistrate upon a finding of continuing probable cause and that the extension served the underlying purpose of obtaining the warrant.\textsuperscript{277}

Like the federal bills addressing this issue, the California bill (SB 1434) contained several exceptions to the warrant requirement, including for responding to a call for emergency services, the “informed, affirmative consent of the owner,” as well as an emergency exception in which threat of death or serious physical injury necessitates disclosure of information, and a warrant cannot be obtained in time to prevent the perceived threat.\textsuperscript{278} For instances in which law enforcement would use the emergency involving threat of death or bodily injury, law enforcement would be required to provide the court with a statement within 48 hours after asking for the record, explaining the emergency need and why the information sought was necessary to resolving the emergency.\textsuperscript{279}

The bill passed in the California Assembly with a vote of 63 to 11\textsuperscript{280} and passed in the Senate with a vote of 33 to 3.\textsuperscript{281} Yet a month later, Governor Gerald Brown vetoed the bill.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{276} S.B. 1434(h) (a), 2012 Leg., ___ Sess. (Ca. 2012).
\item \textsuperscript{277} \textit{Id.} at (h) (b).
\item \textsuperscript{278} \textit{Id.} at (h) (c).
\item \textsuperscript{279} \textit{Id.} at (h) (d).
\end{itemize}
\end{footnotesize}
conceding that while action by the legislature may be necessary to ensure that California law keeps pace with technological developments, SB 1434 did not appropriately balance “the operational needs of law enforcement and individual expectations of privacy.” A year earlier. Governor Brown had vetoed another bill that would have restricted the ability of law enforcement to search a suspect’s cellular phone incident to an arrest, and thus this veto may not have surprised many.

In the event that Congress musters the support that California’s legislature had and enacts a legislation to wholly reform the government’s collection of electronic information about Americans, it is quite possible that in the interest of securing the necessary votes geolocation privacy will be removed from a final bill. Even if the GPS Act or Online Communications Act is adopted as the legislation of choice, President Obama may be compelled to veto the bill as Governor Brown did, in the interest of preserving law enforcement’s ability to utilize CSLI in conducting criminal investigations. Still, recent votes by legislatures in both Texas and Maine indicate that other states are willing to take action on this issue. Both states have pending legislation that would require law enforcement to obtain a warrant before gathering CSLI. However, the Texas legislature submitted another bill to the Governor that, like the ECPA Amendments Acts in Congress, does not include CSLI provisions, making it unlikely that the

CSLI bill will advance as well. The Texas and California outcomes portend a similar fate for the federal legislation. Still, there might be a manner by which the Supreme Court can effectuate a limitation on warrantless CSLI searches.

B. A Jurisprudential Limiting Principle – Reviving the Dragnet Search Doctrine

Justice Sotomayor’s concurrence in Jones reflects concerns with the duration and scope of high-technology searches. Justice Sotomayor raised questions about the continuing efficacy of the third party doctrine in the 21st century, writing that the current approach of the 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.” She advised that “whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.” Justice Sotomayor’s exposition stops there, as the Court resolved the issues of the case on a “narrower basis.” Justice Sotomayor’s concerns have a foundation in the Supreme Court’s overlooked dragnet search doctrine.

The concerns over dragnet searches reach back to the founding of the country in the form of “general warrants.” Law professor Christopher Slobogin describes dragnet searches as “programmatic government efforts to investigate, detect, deter, or prevent crime or other

287 Id. at ___.
288 Id.
289 Id.
290 Christopher Slobogin, Government Dragnets, 73 LAW & CONTEMPORARY PROBS. 107 (2010).
significant harm by subjecting a group of people, most of whom are concededly innocent of wrongdoing or of plans to engage in it, to a deprivation of liberty or other significant intrusion.”291 Dragnet searches, which require no individualized suspicion, arose in Supreme Court jurisprudence in the mid-1960’s, and were upheld by the Court “if they involved only minimally intrusive government actions necessary to protect important health or safety interests that an individualized probable cause regime could not sufficiently protect.”292 An additional requirement for these searches was that the government must have in place some mechanism for limiting the discretion of the officials conducting the searches, so as to prevent searches that were “arbitrary, discriminatory, or harassing.”293 These mechanisms could be either a warrant for an “area inspection” or “legislative or regulatory regimes that were effective as warrants in eliminating discretion.”294 Yet new technologies have afforded law enforcement additional means of conducting dragnet searches.295 As the above cases indicate, the collection and utilization of CSLI has proven to be a valuable tool for law enforcement, a tool about which they are reluctant to divulge information.296 The dragnet search doctrine has seen limited application since the 1960’s, but the utilization of CSLI is exactly the type of dragnet search that the Court expressed concern with in the past.297

291 Slobogin, supra note ___, at 110.


293 Id. at 267.

294 Id. (internal citation omitted).

295 Slobogin, supra note ___, at 109.

296 Cyrus Farivar, FBI to ACLU: Nope, we won’t tell you how, when, or why we track you, ARS TECHNICA, Jan. 16, 2013, available at http://arstechnica.com/tech-policy/2013/01/fbi-to-aclu-nope-we-wont-tell-you-how-when-or-why-we-track-you/.

297 Slobogin, supra note ___, at 127.
With respect to high-technology searches, the U.S. Supreme Court suggested additional considerations might be warranted to address so-called dragnet searches:

But the fact is that “reality hardly suggests abuse.” If such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable. Insofar as respondent's complaint appears to be simply that scientific devices such as the beeper enabled the police to be more effective in detecting crime, it simply has no constitutional foundation. We have never equated police efficiency with unconstitutionality, and we decline to do so now.²⁹⁸

Justice Rehnquist shared the same kind of concerns that lower courts have expressed about the government’s ability to conduct widespread, pervasive searches with modern technology.²⁹⁹ Justice Rehnquist, however, did not define what types of activity constitute a dragnet search. Yet his statement does reflect a concern that certain types of policy activity are so egregious that they warrant additional scrutiny even when the third party doctrine is implicated.

Additional color was added to the dragnet search doctrine eight years after Justice Rehnquist’s dissent in Knotts. In Florida v. Bostick, the Court held that police officers had not engaged in an unlawful seizure by routinely boarding buses at scheduled stops and asking passengers for permission to search their luggage.³⁰⁰ Justice Marshall issued a dissent, joined by Justices Blackmun and Stevens, and wrote, “[t]hese sweeps are conducted in ‘dragnet’ style. The police admittedly act without an ‘articulable suspicion’ in deciding which buses to board and

²⁹⁸ Knotts, 460 U.S. at 283-84 (internal citations omitted).

²⁹⁹ See, e.g., CSLI: Brooklyn 2010, supra note __.

which passengers to approach for interviewing. By proceeding systematically in this fashion, the
police are able to engage in a tremendously high volume of searches.”^301

Two principles to the dragnet search doctrine can be derived from Justice Marshall’s
opinion. The first principle is scope. Justice Marshall was disturbed by the fact that police
officers could stop and search any bus that drove through Florida, with little regard for actual
cause. The second is volume. Related to the first principle, Justice Marshall expressed concern
that the unconstrained search method allowed the police to conduct an inordinate number of
searches, seemingly limited only by police resources. These two principles track closely with the
concerns of scope and duration expressed by Justice Sotomayor in her concurrence in Jones. In
making requests for CSLI, law enforcement officers are able to obtain massive amounts of
information about individuals without first obtaining a warrant. Given the relatively inexpensive
nature of the requests (to law enforcement, at least), this provides law enforcement with a cost-
friendly and highly effective tool for investigations. But as Justice Marshall observed in Bostick,
“the effectiveness of a law-enforcement technique is not proof of its constitutionality.”^302 Thus
future judicial examination of CSLI searches should explore the dragnet search doctrine and
consider bringing its precedential strength to the concerns of scope and duration.

i. Academic Proposals To Limit High-Technology Searches Provide
Additional Precision

A note published in the Virginia Law Review two years after the Knotts decision raised
concerns with the scope and duration of dragnet searches: “an exception would prohibit the
warrantless monitoring of public automobile travel when conducted in a dragnet fashion, as, for
example, where a substantial number of people are tracked without individualized suspicion, or

^301 Id. at 441-42 (Marshall, J., dissenting).
^302 Id. at 440.
an individual is tracked for an extended length of time.” As noted above, the Maynard and the Jones concurrences also explained the need to limit searches in terms of scope and duration, but there has been little work done expanding on how to measure scope and duration.

Some scholars have offered potential solutions to this conundrum. Professor Slobogin has a proposal centering on the principles of proportionality – which weighs the necessity of the search against its level of invasiveness - and exigency – that unless there is some emergency need, some form of prior authorization must be given for a search to occur. He explains that duration can be limited by the government’s justification and writes, “[t]he justification for a government search or seizure ought to be roughly proportionate to the invasiveness of the search or seizure.” His reasoning is that “the Court’s search and seizure jurisprudence is consistent with the idea that the more privacy-invading or autonomy-limiting a police action is, the more justification the government must show before it may be carried out.”

From this premise, Professor Slobogin argues that dragnet-style searches (such as CSLI searches) that are not specifically authorized by legislative enactment should be held to a higher standard. In order for the police to perform such searches the government must demonstrate that the likelihood of the search’s success is proportionate to the intrusiveness of the dragnet search or that the search is justified by exigent circumstances. Slobogin offers two examples of how a dragnet search might be analyzed under the proportionality rationale, comparing a search of the

304 Slobogin, supra note __ at 138.
306 Slobogin, supra note __, at 1590.
bags of all persons in a specific location to a “camera-surveillance operation” across a city area. The former, assuming it had a level of intrusiveness akin to “somewhere between a frisk and a house search” would require what he calls “generalized probable cause,” while the latter would require a lesser showing due to the less intrusive nature of the search conducted.  

In this vein, it appears that the government would be more justified in conducting over-inclusive searches when the societal need is particularly great, such as in terrorism related investigations. Of course, if the proportionality principal were to apply so as to require some showing of particularized suspicion, the government could still find exceptions in the “special needs” cases. Even in the “special needs” cases, however, courts will generally require that the government create some procedures to minimize intrusions on innocent individuals.  

Professor Slobogin articulates a reasonable way of thinking about electronic surveillance. His approach, however, presents several practical difficulties. First, how do courts (or law enforcement, for that matter) determine the sorts of reasons that are sufficient to justify electronic surveillance? Second, how should we think about intrusiveness? Professor Slobogin argues that social science data—such as surveys—could assist courts in determining

---

308 *Id.* at 139.

309 Professor Slobogin cites several cases where particularized suspicion is not necessary although some non-suspicious people will be searched: *see, e.g.*, Bd. of Educ. v. Earls, 536 U.S. 822, 829 (2002) (“It is true that we generally determine the reasonableness of a search by balancing the nature of the intrusion on the individual’s privacy against the promotion of legitimate governmental interests [but] in the context of safety and administrative regulations, a search unsupported by probable cause may be reasonable when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable” (internal quotation marks omitted and emphasis added)); Mich. Dep’t of State Police v. Sitz, 496 U.S. 444, 455 (1990) (“the balance of the State’s interest in preventing drunken driving, the extent to which this system can reasonably be said to advance that interest, and the degree of intrusion upon individual motorists who are briefly stopped”).

310 Slobogin, *supra* note __, at 1595; *see, e.g.*, United States v. Martinez-Fuerte, 428 U.S. 543, 562 (1976) (“the reasonableness of the procedures followed in making these checkpoint stops makes the resulting intrusion on the interests of motorists minimal”).

311 Questions abound: will probable cause be needed for CSLI over the course of a week? Will reasonable suspicion justify one day of CSLI? What if the police are nearly certain of the suspect’s culpability, will CSLI be permitted for months?
what kinds of surveillance are most intrusive. However, he acknowledges that the Court’s accuracy in gauging societal views on intrusiveness in the context of public surveillance and data mining has been mixed. Moreover, what amount of CSLI would cross the threshold from reasonably intrusive to unacceptably intrusive? While courts might be able to make that determination in a reasonable manner, disagreement among circuits would be likely to occur over what that critical point of intrusiveness might be, and thus the test would do little to alleviate the disparate treatment CSLI searches receive across the country. Finally, such an inquiry creates room for a great deal of second-guessing. As an investigation ebbs and flows, the amount of justification that law enforcement has may increase and decrease. This could create an awkward scenario in which the warrantless electronic surveillance of the same individual is permissible at one point of an investigation but not at a subsequent point.

An alternative, perhaps more direct, proposal focusing on how best to limit the applicability of the third party doctrine is that offered by law professor Stephen Henderson. In 2007, he offered a 9-factor framework for courts to use in determining when to limit government access to third party information like CSLI. Those factors included “the purpose of the disclosure, the personal nature of the information, the amount of information, the expectations of the disclosing party, the understanding of the third party, positive law guarantees of confidentiality, government need, personal recollections, and changing social norms and technologies.”

---

312 Slobogin, supra note __, at 1595.

Professor Henderson admitted that application of this nine-factor framework might cause a great deal of uncertainty, and a couple years later he offered a revised, shortened framework that would be “more administrable.” The revised framework proposes that courts analyze a person’s expectation of privacy by looking to whether the conveyance in question “is reasonably necessary to participate meaningfully in society or is socially beneficial;” the personal nature of the information and the extent to which, aside from the conveyance, the information is either shared with others or withheld; the extent to which non-governmental entities have access to the information “outside the institution;” and the extent to which existing law permits or forbids access to and sharing of such information.

While Professor Henderson’s four-factor approach offers a means for the courts to place some limitations on the third party doctrine, it is unclear that the application of his test would yield a positive outcome in situations where the information at issue is CSLI. For example, courts could differ on the question of whether the conveyance of location information to a CSP by the use of a cell phone is “reasonably necessary” to participate meaningfully in society. Even if we assume that it is, the prevalence and popularity of mobile apps that share a cell user’s location could present a situation in which a law abiding citizen who loves to check-in on Foursquare might have a lower expectation of privacy than a potential culprit who chooses to use her phone for criminal purposes and does so in a guarded, privacy-conscious manner. Courts would also be required to investigate whether cell phone providers share customer CSLI with

---

314 Id. at 1025-26.
316 Id. at 50-51.
317 Foursquare is a mobile application that lets its 30 million users “check-in” at locations, based on their phone’s geographic location. See, About, https://foursquare.com/about/ (last accessed Jan. 18, 2013).
outside entities, a practice reported to occur quite frequently. Henderson’s last factor, the landscape of existing law, may be another nail in the coffin for a user’s expectation of privacy, but as discussed above, future legislation may alter that.

ii. Problems With A Judicially Limited Approach

A weakness of the dragnet doctrine proposal is that Justice Rehnquist’s language in *Knotts* is dicta, and thus one might argue that it cannot serve as a guiding principle for Fourth Amendment doctrine with respect to CSLI searches. It is certainly true that the dragnet language in *Knotts* is dicta, and CSLI searches are not perfect analogs to the kind of dragnets where police round up dozens of criminal suspects. Nonetheless, as explained above, the language in *Knotts* and the concerns expressed by Justice Marshall in his dissent in *Bostick* are important for the ideas they represent. The fear of dragnets in these cases is substantially similar to the fears expressed by the courts that have already taken up the issue of warrantless CSLI searches.

This point aside, it is unclear that either of the aforementioned judicial proposals could provide members of the public (let alone law enforcement) any more certainty than currently exists now. What one court may find to be an unacceptably intrusive search, when utilizing the proportionality framework advocated by Professor Slobogin, another may find permissible. And courts adopting Professor Henderson’s third party doctrine proposal could reasonably reach differing conclusions in factually similar cases. Even then, it is impossible to predict whether lower courts or the Supreme Court for that matter would adopt one of these jurisprudential tests for addressing warrantless CSLI searches in future cases.

---

A hearing held by the House Judiciary Committee’s Subcommittee on Crime, Terrorism, and Homeland Security on April 25, 2013 explored the contours of this debate and provides some further insights into how such approaches might be received both by Congress as well as law enforcement and other stakeholders who must confront these issues on a regular basis.\(^\text{319}\) One area in which there seemed to be some agreement between both law enforcement apologists and public interest advocates was statutory protections limiting the use of “tower dumps.” Tower dumps occur when law enforcement makes a request for all call records from a cell tower over a particular period of time. Because these searches necessarily collect significant amounts of information on a large number of people, both sides said that restrictions on their use merited Congress’s consideration.\(^\text{320}\)

But as for the general treatment of CSLI searches, the same dividing lines still exist. Witnesses with views amenable to law enforcement interests continue to maintain that the imposition of a probable cause requirement for CSLI searches would impair law enforcement investigations, and render that “building block” of criminal investigations much more difficult and costly to obtain.\(^\text{321}\) On the other hand, the ACLU’s Catherine Crump argued that the nature of the intrusion involved means a probable cause standard should be the general rule, with certain exceptions permitted for emergency situations.\(^\text{322}\) Thus, it seems that a case-by-case approach that both academic proposals appear to represent would attract little interest from these


\(^{320}\) Geolocation Privacy Hearing (written testimony of Mark Eckenwiler, Senior Counsel, Perkins Coie LLP and former Associate Director for Technology, Office of Enforcement Operations, Criminal Division, U.S. Dept. of J., at 8); Geolocation Privacy Hearing (written testimony of Catherine Crump, Staff Attorney, ACLU, at 9-10).

\(^{321}\) Geolocation Privacy Hearing (oral testimony of Mark Eckenwiler).

\(^{322}\) Geolocation Privacy Hearing (oral testimony of Catherine Crump).
two sides. Interestingly though, when asked by Rep. Sensenbrenner whether Congress must act in this area and set some boundaries governing the use of high tech surveillance techniques, Chief of Detectives of the District Attorneys Office in Rockland County, New York Peter Modafferi answered in the affirmative, stating that in many instances law enforcement is “acting in the dark” with new forms of technology that are useful for investigative purposes, and could benefit clarification from Congress that addresses the changes in technology. 323

The courts thus have a number of options for rendering some definitive answers to these questions. The questions that remain are which option they might employ, and whether Congress may act first.

IV. Conclusion

Cell phone users voluntarily convey CSLI information to their CSPs by powering on their phones and sending and receiving information via the device. Thus, the third party doctrine applies and prevents a user from claiming a right to privacy in her location. Lower courts have struggled to find a limiting principle to rein in the application of the third party doctrine. A legislative solution can be created, requiring the police to demonstrate probable cause before acquiring CSLI from a CSP. As Justice Alito wrote in his concurrence in Jones, “[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.” 324 Because of the importance of this issue to the public and the growing use of CSLI for criminal investigations, Congress should act decisively in this area and not laggardly await an uncertain decision by the Court.

323 Geolocation Privacy Hearing (oral testimony of Peter A. Modafferi, Chief of Detectives Rockland County, N.Y. District Attorneys Office).

324 Jones, 132 S. Ct. 964 (Alito, J., concurring).
But, if Congress is unable to come to a consensus, or the legislation is vetoed, a jurisprudential solution can also be created. The judicial reasoning should be steeped in the precedent of the dragnet search doctrine and should seek to limit CSLI searches based on their scope and duration.