National Security Law Journal

Excerpt from Vol. 3, Issue 2 (Spring/Summer 2015)

Cite as:

Lauren Doney, Comment, *NSA Surveillance,* Smith *&* *Section 215: Practical Limitations to the Third-Party Doctrine in the Digital Age*, 3 NAT'L SEC. L.J. 462 (2015).

ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, homeland security, and national defense.

We welcome submissions from all points of view written by practitioners in the legal community and those in academia. We publish articles, essays, and book reviews that represent diverse ideas and make significant, original contributions to the evolving field of national security law.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

COMMENT

NSA SURVEILLANCE, *SMITH* & SECTION 215:

PRACTICAL LIMITATIONS TO THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

Lauren Doney*

In June of 2013, The Guardian reported that the National Security Agency ("NSA") was collecting telephony metadata from U.S. citizens under Section 215 of the USA PATRIOT Act. This quickly prompted questions about the legal basis of the program, including its compliance with the Fourth Amendment. In defense of the program, the Obama Administration pointed out both legislative and judicial approval of the program, and also cited a 1979 case, Smith v. Maryland, as precedent for the collection of telephony metadata. In Smith, the Court applied the third party doctrine and found that no Fourth Amendment search had occurred when the defendant voluntarily shared telephone numbers he dialed with his telephone provider, and therefore maintained no privacy interest in that information. However, rather than assuaging concerns about the Section 215 program, the government's reliance on Smith provoked new concerns about the application of the third party doctrine. Some of this concern is due to incredible advancements in technology that have reshaped society while the law has failed to keep pace. As individuals increasingly provide vast amounts of personal data to third parties in the course of their daily lives, the third party doctrine has become a nearly insurmountable obstacle to asserting Fourth Amendment privacy rights. A more conservative application of the third party doctrine is needed, and two recent decisions suggest the Supreme Court is open to revisiting the

* George Mason University School of Law, J.D. Candidate, May 2015; University of Central Florida, B.A., August 2011; Director of Communications and Engagement, *Just Security*; Notes and Research Editor, *National Security Law Journal*, 2014-2015.

doctrine. Drawing support from these two cases, this Comment proposes a more limited application of the third party doctrine.

INTRODUCTION

In June of 2013, *The Guardian* reported[1] that the National Security Agency ("NSA"), the U.S. government agency responsible

[1] Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald & Ewan McCaskill, *NSA Prism program taps in to user data of Apple, Google and others*, GUARDIAN (June 6,

for the collection and processing of foreign communications for intelligence and counterintelligence purposes,[2] was also collecting the communications of U.S. citizens.[3] *The Guardian* reports described two NSA surveillance programs, only one of which will be examined here.[4] Under the Section 215 program, NSA was collecting the call

2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

[2] "Foreign intelligence information" is:

> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—
>
> (A) the national defense or the security of the United States; or
>
> (B) the conduct of the foreign affairs of the United States.

50 U.S.C. §1801(e) (2012).

[3] NSA is responsible for the collection, processing, and dissemination of signals intelligence ("SIGINT"). Exec. Order No. 12,333, § 1.12(b). "SIGINT is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons." *See Signals Intelligence*, NAT'L SEC. AGENCY, http://www.nsa.gov/sigint/. The term "communications intelligence" ("COMINT") has also been used to describe NSA's responsibilities. COMINT is a division of SIGINT and "is produced by the collection and processing of foreign communications passed by electromagnetic means . . . and by the processing of foreign encrypted communications, however transmitted." U.S. DEP'T OF DEF., DIR. 5100.20, THE NATIONAL SECURITY AGENCY AND THE CENTRAL SECURITY SERVICE, para. III(B) (June 24, 1991).

[4] The second surveillance program reported by *The Guardian* is the Section 702 program, which will not be examined in this Comment. The program reportedly allowed NSA to intercept internet-based communications data (including the content of communications) of non-U.S. persons overseas, which also resulted in the incidental collection of such data from U.S. persons. NSA reportedly collected internet-based communications by "tap[ping] into the servers" of major U.S. internet providers in order to extract customers' personal data, such as e-mails, video chats, documents, and more. *NSA slides explain the PRISM data-collection program*, WASH. POST, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (last updated July 10, 2013). For a thorough discussion of the Section 702 program, see Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015).

detail records (also referred to as "telephony metadata")[5] for millions of domestic and international telephone calls pursuant to a single court order.[6] The *Guardian*'s reports generated considerable public discussion of NSA's activities and prompted questions about the legal basis of the Section 215 program,[7] including how this bulk collection of telephony metadata complied with the Fourth Amendment.[8]

In the weeks following the initial disclosures of NSA's domestic surveillance, President Obama and other executive branch officials defended the agency's actions, noting that both the legislative and judicial branches had approved the Section 215

[5] The terms "call detail records" and "telephony metadata" are used interchangeably by the Foreign Intelligence Surveillance Court ("FISC") in the leaked court order, and will be used similarly throughout this Comment. *See* Greenwald, *supra* note 1. As used in this context, the term "metadata" refers to information about telephone calls—not the content of the calls. Metadata includes information like telephone numbers associated with calls placed and received, as well as date, time, and duration of calls. *See generally* ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2-3 (Aug. 9, 2013) [hereinafter BULK COLLECTION WHITE PAPER], *available at* http://perma.cc/8RJN-EDB7; *see also* MEMORANDUM FROM THE OFFICE OF LEGAL COUNSEL FOR THE ATTORNEY GENERAL, RE: REVIEW OF THE LEGALITY OF THE STELLAR WIND PROGRAM 81 (May 6, 2004).

[6] This Comment refers to this telephony metadata program as the "Section 215 program." The name of the program is derived from its location in its authorizing legislation. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272 (codified as amended at 50 U.S.C. § 1861 (2012). Section 215 of the Act replaced §§ 501-503, the "business records" provisions under Title V of the Foreign Intelligence Surveillance Act of 1978 ("FISA"). Congress added Title V to FISA in 1998 and has since amended it with legislation like the USA PATRIOT Act and the Intelligence Authorization Act for Fiscal Year 2002. Pub L. No. 107-108, § 314(a)(6)-(7), 115 Stat. 1402 (2001).

[7] *See, e.g.*, Thomas Earnest, *Balancing the Public Interest in Disclosures*, JUST SECURITY (Jan. 21, 2014), http://justsecurity.org/6018/public-interest-disclosures-marc-thiessen/; Jennifer Granick & Christopher Sprigman, *The Criminal N.S.A.*, N.Y. TIMES (June 27, 2013), http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html; Julian Sanchez, *Snowden: Year One*, CATO UNBOUND (June 5, 2014), http://www.cato-unbound.org/2014/06/05/julian-sanchez/snowden-year-one.

[8] A complete legal analysis of the Section 215 program is beyond the scope of this Comment.

program.[9] Officials also cited a 1979 case, *Smith v. Maryland*, as an authority for the collection of telephony metadata that occurred under the Section 215 program.[10] The Supreme Court in *Smith* determined that the government's use of a single pen register to monitor the telephone numbers dialed by the defendant did not constitute a "search" for purposes of the Fourth Amendment, and therefore, no warrant was required.[11] Moreover, the defendant had no "reasonable expectation of privacy" regarding the numbers he dialed, because he had voluntarily conveyed such information to a third party, his telephone company.[12] This notion that information shared with third parties has no Fourth Amendment protection is known as the "third-party doctrine."[13] The executive branch and the Foreign Intelligence Surveillance Court ("FISC") have since relied upon *Smith's* precedent to justify the more expansive and technologically sophisticated Section 215 program.

According to the Obama administration, the data collected under the Section 215 program does not include call content, but does include telephony metadata—such as information about phone numbers dialed, calls received, and call duration—that individuals voluntarily share with phone companies.[14] Consequently, collection of such information under the Section 215 program falls within the scope of the third-party doctrine and *Smith*: it is not a Fourth Amendment "search" because "persons making phone calls lack a

[9] *See, e.g.*, BULK COLLECTION WHITE PAPER, *supra* note 5. In 2006, the FISC stated that Section 215 was a valid legal authority for bulk collection of telephony metadata, including the metadata of U.S. persons. In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 06-05 (FISA Ct. May 24, 2006).

[10] Smith v. Maryland, 442 U.S. 735 (1979). For examples of officials invoking the *Smith* precedent, see Defendant's Memorandum of Law in Opposition to Plaintiff's Motion Preliminary Injunction, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (13 Civ. 3994), 2013 WL 5744828. *See also* BULK COLLECTION WHITE PAPER, *supra* note 5.

[11] *Smith*, 442 U.S. at 745-46. *See* BULK COLLECTION WHITE PAPER, *supra* note 5, at 19.

[12] *Smith*, 442 U.S. at 738.

[13] Fourth Amendment scholar Orin Kerr describes the doctrine as the rule that information "loses Fourth Amendment protection when it is knowingly revealed to a third party." Orin S. Kerr, *The Case for Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).

[14] BULK COLLECTION WHITE PAPER, *supra* note 5, at 23.

reasonable expectation of privacy in the numbers they call" and in the information voluntarily provided to a third party.[15] When NSA intercepts this information, the government argues, it is not a "search" and no warrant is required.[16] According to the administration, if no privacy interest is violated when the government obtains telephony metadata of one individual, no privacy interest is violated when the government obtains telephony metadata of millions of individuals.

The Obama administration's efforts to assuage Americans' concerns about the legality of the program instead provoked significant debate about the third-party doctrine and its application to NSA's Section 215 program.[17] Because *Smith* permitted only individualized, short-term surveillance of the phone numbers dialed by an identified suspect,[18] some, including the U.S. District Court for the District of Columbia, have argued that *Smith* cannot possibly justify the bulk surveillance of millions of individuals' call-detail records that occurs under the Section 215 program.[19] In addition,

---

[15] *Id.* at 19-20 ("A Section 215 order for the production of telephony metadata is not a 'search' . . . because, as the Supreme Court has expressly held, participants in telephone calls lack any reasonable expectation of privacy under the Fourth Amendment in the telephone numbers dialed.").

[16] *Id.* at 22.

[17] *E.g.,* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 125 (Jan. 23, 2014) [hereinafter PCLOB Report], *available at* https://www.pclob.gov/Library/215-Report_on_the_Telephone_Records_Program.pdf ("As suggested by the observations of Justices Alito and Sotomayor in *United States v. Jones*, collectively representing the views of five Justices, the Supreme Court might find that the third-party doctrine, regardless of its validity as applied to traditional pen/trap devices and particularized subpoenas, does not apply to the compelled disclosure of data on a scope as broad and persistent as the NSA's telephone records program.").

[18] Smith v. Maryland, 442 U.S. 735, 736-37 (1979).

[19] In an opinion regarding the Section 215 program, the U.S. District Court for the District of Columbia distinguished the Section 215 program from *Smith* and concluded:

> [T]he surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the

societal changes and advancements in technology suggest that *Smith* may no longer represent the best approach to determining permissible invasions of privacy. As individuals increasingly provide vast amounts of personal information to third parties in the course of their everyday lives, some have questioned whether the default application of the third-party doctrine has needlessly narrowed Fourth Amendment privacy rights.[20] Accordingly, this Comment argues that a more restrained application of the third-party doctrine is necessary, drawing support from two recent Supreme Court decisions: *Riley v. California* and *United States v. Jones*. In these landmark Fourth Amendment cases, the Court limited the government's ability to conduct warrantless searches of cell phones and GPS information. Although neither *Jones* nor *Riley* directly involved the Section 215 program, the decisions nonetheless provide valuable insight into the Supreme Court's perception of new surveillance technologies and how they impact Fourth Amendment rights. With several cases challenging the constitutionality of the Section 215 program currently making their way through federal district and appeals courts, the Supreme Court may very well

> contrary . . . I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

Klayman v. Obama, 957 F. Supp. 2d 1, 32 (D.D.C. 2013).

[20] *E.g.*, David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 139 (2013) ("In the age of data aggregation, the stakes for privacy implicated by this third-party doctrine have grown dramatically. Vast reservoirs of our private data are gathered by or otherwise reside in the hands of private entities."); Lauren Elena Smith, *Jonesing for a Test: Fourth Amendment Privacy in the Wake of* United States v. Jones, 28 BERKELEY TECH. L.J. 1003, 1003 (2013) ("The evolution of surveillance technologies over the last few decades has led some observers to wonder if the Fourth Amendment will become irrelevant in the digital age. Privacy protections are eroding, as law enforcement is able to access more information that is voluntarily shared by technology-utilizing citizens."); Jennifer Granick, *Prediction: Fourth Amendment Evolves in 2014*, JUST SECURITY (Dec. 31, 2013, 4:32 PM), http://justsecurity.org/5195/prediction-fourth-amendment-evolves-2014/. *See also* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(b) (2012) (criticizing the third-party doctrine and the application of *Smith* as making a "mockery of the Fourth Amendment").

consider a challenge to some aspect of the program in the near future.[21]

Part I of this Comment provides a brief history of the Fourth Amendment, the third-party doctrine, and *Smith*. Part II distinguishes the Section 215 program from *Smith*, and in doing so, demonstrates why the third-party doctrine may be in need of some restraint. In Part III, this Comment suggests that the Court is likely to reexamine the third-party doctrine and Fourth Amendment privacy rights in the context of new technology, using *Jones* and *Riley* as examples.[22] Part IV offers a proposal for a more nuanced application of the third-party doctrine. First, the Court should determine if an alternative to sharing information with a third party exists. If one does not exist, the third-party doctrine does not apply, and the Court must then consider the context and consequences of the government action to determine whether a search has taken place. The inquiry is designed to fulfill the underlying purpose of the doctrine:[23] Fourth Amendment protection is lost when information is freely made public, but individuals' privacy rights would still be protected under circumstances in which sharing information is required for participation in essential functions of daily life.[24]

I. OVERVIEW OF THE FOURTH AMENDMENT

The Fourth Amendment to the U.S. Constitution protects individuals and their property from warrantless government searches and seizures.[25] Originally, the Supreme Court confined these

[21] *See, e.g.,* Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014); *Klayman*, 957 F. Supp. 2d at 1; ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); First Unitarian Church v. NSA, No. 13-3287 (N.D. Cal. filed July 16, 2013).

[22] Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 132 S. Ct. 945, 957 (2012).

[23] The notion that there is no privacy interest in information voluntarily conveyed to third parties is based on practical considerations. If the Fourth Amendment were to be applied universally, then a warrant would likely be required for everything. This would likely lead to considerable frustration for law enforcement officials.

[24] Smith v. Maryland, 442 U.S. 735, 744 (1979) ("Because the depositor 'assumed the risk' of disclosure, the Court held that it would be unreasonable for him to expect his financial records to remain private.").

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

safeguards solely to the circumstances explicitly articulated in the text. Fourth Amendment protections applied only when physical searches or seizures of property—"persons, houses, papers, and effects"—occurred.[26] But interpretation of the Fourth Amendment, and, therefore, what sort of government action would be considered a search, has been influenced by technological advancements and societal changes. With the introduction of new technology, such as the telephone and wiretap, the Court has since recognized a "constitutionally protected reasonable expectation of privacy" even when no physical intrusion has occurred.[27]

In the 19th Century, the invention of the telegraph and telephone fundamentally transformed communications, connecting individuals scattered across the nation and vastly increasing communications capabilities. As use of the telephone increased, the government capitalized upon this increase in communications, adapting existing surveillance technology to monitor these new forms of communication.[28] In the 1928 case of *Olmstead v. United States*, the Supreme Court upheld the use of warrantless wiretapping of a telephone conversation because no physical trespass onto the defendants' property had occurred.[29] When government officials suspected the defendants of running a bootlegging operation, they installed wiretaps on telephone lines located in the basement of the defendants' office building and streets outside of their homes.[30] But because the government had not physically intruded onto the defendants' property to install the wiretaps, the Court rejected the argument that a search (and therefore, a Fourth Amendment violation) had occurred.[31] The Court foreclosed any possibility that Fourth Amendment privacy rights could be invoked without a physical intrusion into an individual's property, papers, or effects.

---

[26] Olmstead v. United States, 277 U.S. 438, 457, 464-66 (1928).
[27] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).
[28] *See* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 225 (4th ed. 2011).
[29] *Olmstead*, 277 U.S. 438.
[30] *Id.* at 457.
[31] *See id.* at 464 ("The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

In a passionate dissent, Justice Brandeis warned about the practical limitations of the Court's holding. He worried that the strict, property-based approach articulated in *Olmstead* would improperly cabin the Fourth Amendment and fail to protect individuals from non-physical government intrusions that were equally invasive:

> The progress of science in furnishing the government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[32]

Brandeis' prescient dissent forecasted how advancements in technology could alter government surveillance techniques, and in turn, impact individual expectations of privacy. Although he correctly predicted the inadequacy of *Olmstead* in addressing these changes, the Court struggled for decades to fit Fourth Amendment rights into the confines of the precedent it had established.

A. Applying Olmstead in a Changing World

The strict approach of *Olmstead* meant that for decades privacy rights were literally confined to the words of the Fourth Amendment. *Olmstead* faced criticism in the ensuing years, as telephone use (and, correspondingly, the use of wiretaps) increased.[33] Despite growing evidence that the physical trespass threshold was ill-equipped to protect Fourth Amendment rights in the face of new government surveillance capabilities and changes in electronic means of communication, it took nearly forty years for the Court to overturn it.[34] As the examples below demonstrate, the Court

---

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

[33] *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R43586, THE FOURTH AMENDMENT THIRD PARTY DOCTRINE 5 (2014); SOLOVE & SCHWARTZ, *supra* note 28, at 225, 313 ("Wiretapping was used to intercept telegraph communications during the Civil War and became very prevalent after the invention of the telephone. The first police wiretap occurred in the early 1890s. In the first half of the twentieth century, wiretaps proliferated . . . .").

[34] *See* Katz v. United States, 389 U.S. 347, 353 (1967).

struggled to apply *Olmstead* to new methods and increased deployment of government surveillance in this time period.[35] As the dissents in these cases point out, Fourth Amendment determinations involving government surveillance frequently yielded counterintuitive outcomes and seemed to turn on relatively superficial distinctions in facts.

In the 1942 case *Goldman v. United States*, the Court determined that government agents' use of a detectaphone, without a warrant, to overhear conversations in the defendants' office next door did not violate the Fourth Amendment.[36] Government agents gained access to defendants' office and installed a "listening apparatus in a small aperture in the partition wall with a wire to be attached to earphones extending into the adjoining office."[37] But when the agents returned the next day, they realized that the listening device did not work and instead used another device, a detectaphone.[38] A five-justice majority applied *Olmstead* and found that the government's use of the detectaphone did not require a physical invasion of the defendants' property and that no search had taken place—despite the fact that the agents had physically entered the defendants' office in an attempt to install a listening device.[39] According to the Court, the use of the detectaphone from next door was no physical invasion of the defendants' property:[40] "Whatever trespass was committed was connected with the installation of the listening apparatus."[41] No such trespass was associated with the use of the detectaphone next door, so no Fourth Amendment violation had occurred.

---

[35] *See, e.g.*, Silverman v. United States, 365 U.S. 505, 512-13, (1961) (Douglas, J., concurring) ("My trouble with *stare decisis* in this field is that it leads us to a matching of cases on irrelevant facts. An electronic device on the outside wall of a house is a permissible invasion of privacy according to *Goldman* . . . while an electronic device that penetrates the wall, as here, is not. Yet the invasion of privacy is as great in one case as in the other.").
[36] Goldman v. United States, 316 U.S. 129 (1942).
[37] *Id.* at 131.
[38] *Id.* at 131-32.
[39] *Id.* at 134-35.
[40] *Id.* at 134.
[41] *Id.*

In a dissent advocating the overturning of *Olmstead*'s property-based approach, Justice Murphy argued that the strict reading of the Fourth Amendment had and would continue to significantly diminish the privacy rights the country's forefathers had intended to protect.[42] He observed:

> The conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials if men and women are to enjoy the full benefit of that privacy which the Fourth Amendment was intended to provide . . . It is our duty to see that this historic provision receives a construction sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation.[43]

Without flexibility, Murphy warned, the Fourth Amendment was in danger of becoming "obsolete, incapable of providing the people of this land adequate protection."[44] Still, *Olmstead* remained in place, and government surveillance continued to advance.

Ten years later, in *On Lee v. United States*, the Court found that use of a hidden microphone worn by an informant, which relayed conversations without the defendant's knowledge that were taking place on the defendant's property, did not violate his Fourth Amendment rights.[45] Although the undercover informant physically entered the defendant's property for the purpose of recording him, the Court rejected the notion that *Olmstead* protected the defendant's privacy rights.[46] The undercover agent had entered the defendant's property, the Court said, but it was with the consent, "if not by the implied invitation of" the defendant.[47] A frustrated Justice Frankfurter condemned the Court's application of *Olmstead* in his

[42] *Goldman*, 316 U.S. at 138 (Murphy, J., dissenting).
[43] *Id.* The need for the Fourth Amendment to adapt to cover novel intrusions that the Forefathers could not have anticipated is clear. *See also* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 313 (1972) ("Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance.").
[44] *Goldman*, 316 U.S. at 138 (Murphy, J., dissenting).
[45] On Lee v. United States 343 U.S. 747, 749, 751 (1952).
[46] *Id.* at 753-54.
[47] *Id.* at 751-52.

dissent: here a physical trespass *had* occurred, yet the Court refused to recognize this clear intrusion as a Fourth Amendment violation.[48] Frankfurter officially endorsed Murphy's *Goldman* dissent and declared that *Olmstead* must be overturned. Its inflexible approach to the Fourth Amendment undermined protections against government search and seizure. Echoing Justice Brandeis' warning in *Olmstead*, Frankfurter wrote, "The circumstances of the present case show how the rapid advances of science are made available for that police intrusion into our private lives against which the Fourth Amendment of the Constitution was set on guard."[49]

By the early 1960s, the Court was openly struggling to apply *Olmstead* in the wake of new and more frequent instances of government surveillance and seemed to distance itself from a strict property-centric approach to Fourth Amendment rights. In 1961 and then again in 1967, the Court provided early hints that it might be open to reconsidering *Olmstead*. In one case, the Court held that the placement of a recording device in the defendant's office violated the Fourth Amendment, and the Court went so far as to rule unconstitutional a state statute that permitted it.[50] In another case, a unanimous Court held that the government's warrantless use of a "spike mike," a device that allowed police to listen through the defendant's walls, was also violation of the Fourth Amendment.[51] In its holding, the Court declined to overturn *Olmstead* explicitly, but attempted to distance itself from the precedent's confines, saying, "In these circumstances we need not pause to consider whether or not there was a technical trespass under the local property law relating to party walls. Inherent Fourth Amendment rights are not inevitably measurable in terms of ancient niceties of tort or real property law."[52]

---

[48] *Id.* at 761-62 (Frankfurter, J., dissenting).
[49] *Id.* at 759-760 (majority opinion); Olmstead v. United States, 277 U.S. 438, 458 (1928).
[50] Berger v. New York, 388 U.S. 41 (1967).
[51] Silverman v. United States, 365 U.S. 505 (1961). The spike mike only barely intruded on the physical property—it "made contact with a heating duct serving the house" of the defendants. *Id.* at 506-07.
[52] *Id.* at 511.

B. The Modern Fourth Amendment: A Reasonable Expectation of Privacy

Finally, in 1967, the Court adopted a far more expansive view of Fourth Amendment rights in government surveillance cases—one much more in line with the dissents in *Olmstead, Goldman,* and *On Lee* than the majorities. In *Katz v. United States*, the Court announced that the Fourth Amendment "protects people, not places."[53] Despite the lack of physical trespass in the case, the Court found that warrantless government eavesdropping on the defendant's conversations, which took place in a glass-enclosed, public telephone booth, was a violation of the Fourth Amendment.[54] This acknowledgement of a "constitutionally protected reasonable expectation of privacy"[55] without an accompanying physical trespass was a notable departure from the property-centric approach dictated by *Olmstead*.[56] The *Katz* majority rejected the government's argument that the defendant lacked any Fourth Amendment protection simply because he used a public phone booth to place his calls.[57] When a person "occupies [a telephone booth], shuts the door behind him, and pays the toll that permits him to place a call [he] is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," the majority wrote, continuing, "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[58] According to the Court, the government did not need to physically invade the defendant's property for a Fourth Amendment violation to have taken place.

Despite the conviction of the *Katz* majority's rhetoric, however, the opinion failed to articulate a clear test for determining when a search in violation of the Fourth Amendment has occurred.

---

[53] Katz v. United States, 389 U.S. 347, 389 (1967).
[54] *Id.*
[55] *Id.* at 351.
[56] *Id.* at 353 ("[A]lthough a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision has rested.").
[57] *Id.* at 352.
[58] *Id.*

In a concurring opinion, however, Justice Harlan provided guidelines that have since become the standard relied upon by courts today: a violation of Fourth Amendment rights occurs when the government intrudes upon an individual's "reasonable expectation of privacy" without a warrant.[59] A "reasonable expectation of privacy" exists when two elements have been met: (1) the individual has demonstrated "an actual (subjective) expectation of privacy," and (2) that subjective expectation of privacy is one that "society is prepared to recognize as 'reasonable.'"[60] When each of these elements has been satisfied, an individual has a reasonable expectation of privacy from warrantless government searches. When an individual has not demonstrated a legitimate expectation of privacy—for example, by sharing personal information with a third party—the Fourth Amendment does not prohibit the government from accessing that information without a warrant,[61] as the next section will explore.

C. *The Third-Party Doctrine and* Smith

The third-party doctrine says that an individual maintains no reasonable expectation of privacy in information voluntarily conveyed to a third party, thereby failing the *Katz* test for determining when a Fourth Amendment violation has occurred.[62] As a result, the government may access information shared with a third party, without a warrant, without it constituting a search under the Fourth Amendment.[63] One of the most significant cases in developing the doctrine occurred in 1979, when the Court

[59] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in that case, which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy."). However, not all warrantless searches are unconstitutional. *E.g.*, Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.").

[60] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[61] United States v. Miller, 425 U.S. 435, 443 (1976).

[62] *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1989); *see also Miller*, 425 U.S. at 443-44; Kerr, *supra* note 13, at 561.

[63] *Smith*, 442 U.S. at 745-46.

considered *Smith v. Maryland*, the case now relied upon by the Obama administration as one authority for its Section 215 program.[64]

In *Smith*, the Court upheld the government's warrantless use of a pen register to monitor the telephone numbers dialed by the defendant.[65] Police suspected Smith of repeatedly placing threatening telephone calls to a victim, and installed a pen register on Smith's phone line at the telephone company without his knowledge. The pen register recorded the numbers that Smith dialed but did not record the content of his calls, call duration, or incoming calls—in essence, telephony metadata. With the pen register in place, police found that Smith had, in fact, called the victim, and proceeded to arrest him. The defendant argued that his Fourth Amendment rights had been violated, but the Court rejected Smith's argument, explaining that the defendant had no reasonable expectation of privacy in the telephone numbers he dialed because that information was voluntarily shared with a third party—the telephone company.[66]

Applying the *Katz* reasonable expectation of privacy standard, the Court first considered whether the defendant had exhibited a reasonable expectation of privacy and whether it was an expectation that society would recognize as legitimate. In a 5-4 decision, the Court found that Smith had no reasonable expectation of privacy in the numbers he dialed because he knew that information was shared with the phone company—after all, the telephone company required subscribers to dial a number in order to place and connect his calls.[67] Anyone who ever used a telephone knew that. Moreover, telephone companies kept records of their subscribers' phone calls for billing purposes—subscribers like Smith received regular billing for telephone services that contained this information.[68] Even if Smith had intended to keep this information private, the Court continued, Smith's expectation of privacy was not one that society would recognize as legitimate because the Court had previously stated that he had "no legitimate expectation of privacy in

[64] *See* BULK COLLECTION WHITE PAPER, *supra* note 5.
[65] *Smith*, 442 U.S. at 737.
[66] *Id*. at 735.
[67] *Id*. at 742.
[68] *Id*. at 742-43.

information he voluntarily turns over to third parties."[69] When Smith dialed the numbers on his telephone, he knew he was sharing that information with the telephone company, and in turn, "assumed the risk that the company would reveal to police the numbers he dialed."[70] Smith failed the *Katz* test: he had no reasonable expectation of privacy in the numbers he dialed. Even if he did, this expectation was not legitimate. Given he had no reasonable expectation of privacy, the Court concluded, the government's use of the pen register to record the phone numbers Smith dialed did not constitute a search for Fourth Amendment purposes, and therefore did not require a warrant.[71] *Smith* has since been relied on for its third-party doctrine precedent,[72] and more than thirty years later, the government is still using *Smith* to collect telephony metadata—but in an entirely new way.

II. WHY THE THIRD-PARTY DOCTRINE MUST BE CIRCUMSCRIBED: DISTINGUISHING THE SECTION 215 PROGRAM FROM *SMITH*

Thirty-five years ago when *Smith* created the third-party doctrine, no one could have imagined that soon ninety percent of adult Americans would carry a cellular phone, the Internet would be available in nearly every home, and iPhones would sweep the market. The *Smith* era had not even anticipated the commercialization of technology that is now considered functionally obsolete, such as beepers or facsimile machines.[73] The general American public now owns technology that was simply unfathomable in 1979. The

[69] *Id*. at 743-44.
[70] *Id*. at 744.
[71] *Smith*, 442 U.S. at 745-46.
[72] *See, e.g.,* Kerr, *supra* note 13, at 570. See THOMPSON II, *supra* note 33, at 15 for a line of cases invoking the third-party doctrine precedent. *See* Richard A. Epstein, *Privacy and the Third Hand: Lessons from the Common Law of Reasonable Expectations*, 24 BERKELEY TECH. L.J. 1199 (2009) (discussing how the third-party doctrine fits into other legal contexts and Fourth Amendment circumstances).
[73] Pew Research found that ninety percent of adult Americans own a cell phone. The numbers are even higher in the 18-29 age group, in which ninety-eight percent own a cell phone. *Mobile Technology Fact Sheet*, PEW RESEARCH CENTER, http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/ (last visited Apr. 7, 2015).

proliferation of technology was accompanied by a decline in the cost of new surveillance techniques, making surveillance more affordable and easier to conduct on a large scale.[74]

Defenders of NSA's Section 215 program point to the fact that telephony metadata collection does not include collection of the *contents* of the communications, relating the telephony metadata program to the pen register used in *Smith.*[75] However, there is little evidence to suggest that the *Smith* Court envisioned its approval of the limited and specific surveillance of one individual would also sanction something like the long-term GPS tracking in *Jones*, the search of cell phone data, or the broad surveillance of millions of individuals under the Section 215 program. The *Smith* Court, in determining that no Fourth Amendment search had occurred, emphasized the limited nature of the information resulting from the pen register surveillance and the fact that law enforcement officials did not acquire the contents of Smith's calls.[76] But there are significant differences between the government surveillance approved in *Smith* and the Section 215 program: the differences in the methods of surveillance used, and the level of detail of the information derived from the surveillance in the two scenarios.

A. The Nature of Smith *Surveillance: Narrow and Primitive*

Smith involved surveillance conducted through a pen register, a small device installed at the telephone company that made a record of the numbers dialed by that specific telephone line. The pen register in *Smith* was directed at one specific person, an identified criminal suspect who was placing obscene and threatening telephone calls to a woman.[77] Police installed a pen register on the

---

[74] Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. 335, 353 (2014) (demonstrating the difference in costs between new surveillance techniques and older techniques). "For example, the average cost of cell phone tracking across the three major providers is about $1.80 per hour for twenty-eight days of tracking. Using beeper technology for the same period of time is nearly sixty times more expensive, while covert car pursuit is over 150 times more expensive." *Id.*

[75] *Smith*, 442 U.S. at 737.

[76] *Id.* at 737, 741.

[77] *Id.*

suspect's telephone line, capable only of recording the telephone numbers dialed by the defendant via electrical impulses created by the telephone's rotary dial when released.[78] It did not collect the content or length of the call, and, in fact, could not even collect information about the call's completion.[79] Unlike the information collected in the Section 215 program, the information collected from the pen register was not placed into any database, not aggregated with any other information, and did not disclose any aggregate data from any other individuals.[80] The pen register surveillance was in place for only one day before it yielded enough information for police to secure a warrant to search the suspect's home.[81] In short, the method of surveillance conducted in *Smith* was both narrow in scope and primitive in its technological reach.

B. The Nature of Section 215 Surveillance: Broad and Advanced

In contrast, the surveillance undertaken by the government in the Section 215 program is both broad in scope and technologically advanced: NSA collects millions of telephone records from telecommunications providers. These records contain information such as the telephone numbers of calls placed and received, as well as the time and length of calls.[82] The records are requested and received in bulk, and include the call records of individuals not suspected of any wrongdoing.[83] This call detail

[78] *Id*. at 739.
[79] *Id*. at 737.
[80] PCLOB Report, *supra* note 17, at 114.
[81] Smith v. State, 283 Md. 156, 158-59, 389 (1978), *aff'd*, 442 U.S. 735 (1979) ("On March 17, the telephone company, at the request of the police, installed a pen register at its central offices to record the phone numbers of calls made from the telephone at Smith's residence. On March 17, a call was made from Smith's residence to the victim's home. The police thereafter obtained a search warrant to search Smith's automobile and residence. The search of the residence revealed that a page in Smith's telephone book was turned down; it contained the name and number of the victim. On March 19, the victim viewed a six-man line-up at police headquarters and identified the appellant Smith as the man who robbed her.").
[82] *See Amended Memorandum*, In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 13-109, 2 n.2 (FISA Ct. Aug. 29, 2013).
[83] Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB. POL'Y 757, 869 (2013) ("The NSA is engaging in

information is then compiled into one database and retained there for a period of up to five years.[84] According to the government, the aggregation and maintenance of the call detail records is necessary to establish a "historical repository that permits retrospective analysis."[85] NSA analysts may access this database and query the records contained within it without a warrant or court order, in order to obtain foreign intelligence information.[86] This surveillance method has been in place for seven years, and is conducted on a continuous basis.[87]

Although telephony metadata does not disclose the contents of communications, the call detail records currently collected by the government contain rich data that was unavailable for pen register collection at the time of *Smith*.[88] The Court in *Smith* had distinguished the installation of a pen register from the listening device held to have constituted a search in *Katz*, saying, "pen

bulk collection absent any reasonable suspicion that the individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, almost all of the information obtained will bear no relationship whatsoever to criminal activity.").

[84] PCLOB Report, *supra* note 80, at 12.

[85] *See Amended Memorandum,* In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted], No. BR 13-109, 21 (FISA Ct. Aug. 29, 2013).

[86] *See* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

[87] *See generally* PCLOB Report, *supra* note 17, at 16.

[88] According to the PCLOB Report:

> [T]he pen register approved in *Smith v. Maryland* compiled only a list of the numbers dialed from Michael Lee Smith's telephone. It did not show whether any of his attempted calls were actually completed—thus it did not reveal whether he engaged in any telephone conversations at all. Naturally, therefore, the device also did not indicate the duration of any conversations. Furthermore, the pen register provided no information about incoming telephone calls placed to Smith's home, only the outbound calls dialed from his telephone.

Id. at 114. Senator Dick Durbin also posed questions as to whether *Smith v. Maryland* should be revisited in light of advancements in technology and communications. *Report of the President's Review Group on Intelligence and Communications Technologies*: *Hearing Before the S. Judiciary Comm.*, 113th Cong. (2014), *available at* http://www.judiciary.senate.gov/meetings/hearing-on-the-report-of-the-presidents-review-group-on-intelligence-and-communications-technologies.

registers do not acquire the contents of communications."[89] Yet modern call detail records contain substantially more information than in the *Smith* era: they now include the times and dates of telephone calls, along with the length of the conversation and other unique identifying characteristics.[90] The aggregation of call detail records creates a database of personal information that offers substantial details about an individual's life. This information is far more valuable to the government than information yielded from a single instance of pen register surveillance—if it were not, there would be no reason for the government to collect, compile, and retain this metadata on such a substantial scale.[91] Former NSA Director General Michael Hayden has illustrated that fact, boasting that metadata evidence is so complete and reliable that it can justify the use of deadly force against an individual, once claiming: "We kill people based on metadata."[92] Another government official explained at a 2014 Senate hearing that "there is quite a bit of content in metadata."[93] This aggregation of telephony metadata raises privacy concerns for individuals for the same reason that it carries value for

[89] Smith v. Maryland, 442 U.S. 735, 741 (1989) ("Yet a pen register differs significantly from the listening device employed in *Katz* . . . .").
[90] PCLOB Report, *supra* note 17, at 115 ("The NSA's collection program, however, would show not only whether each attempted call connected but also the precise duration and time of each call. It also would reveal whether and when the other telephone number called Smith and the length and time of any such calls.").
[91] *Id*. at 112 ("Because telephone calling records can reveal intimate details about a person's life, particularly when aggregated with other information and subjected to sophisticated computer analysis, the government's collection of a person's entire telephone calling history has a significant and detrimental effect on individual privacy.").
[92] General Michael Hayden, Speech at the Johns Hopkins University Foreign Affairs Symposium (Apr. 7, 2014), *available at* https://www.youtube.com/watch?v=kV2HDM86XgI.
[93] *Report of the President's Review Group on Intelligence and Communications Technologies*: *Hearing Before the Senate Judiciary Committee*, 113th Cong. (2014) (statement of Michael J. Morell, Deputy Director, CIA), *available at* http://www.judiciary.senate.gov/meetings/hearing-on-the-report-of-the-presidents-review-group-on-intelligence-and-communications-technologies ("I'll say one of the things that I learned in this process, that I came to realize in this process, Mr. Chairman, is that there is quite a bit of content in metadata. When you have the records of phone calls that a particular individual made, you can learn an awful lot about that person . . . There is not, in my mind, a sharp distinction between metadata and content.").

the government: it can provide a highly detailed and intimate description of an individual's life.

C. Why a New Approach is Needed

What was once an infrequent and relatively minor restraint on Fourth Amendment rights has become a frequent barrier to nearly any assertion of Fourth Amendment rights. The third-party doctrine in *Smith* prevented one criminal suspect from using the Fourth Amendment to prohibit the police from monitoring the numbers he dialed. The third-party doctrine in the context of modern surveillance, such as the 215 program, prevents millions of individuals who are not criminal suspects from using the Fourth Amendment to protect themselves against government monitoring of the numbers they dial, the length of their phone calls, and the calls they receive.

In the time of *Smith,* voluntarily sharing information with a third party was an active choice, and therefore, so was the relinquishing of Fourth Amendment protections. Now it is nearly impossible to avoid conveying information to some third party on a regular basis. We no longer send letters in the mail; we send text messages and emails through our telephone company, arming the company (and the government) with rich personal data in doing so. We no longer conduct research in a library; we conduct research on the Internet, supplying a variety of websites (and the government) with our personal information as we search. We no longer rent videos at Blockbuster; we order movies through our cable provider, or stream them through a provider like Netflix or Amazon, allowing these services to monitor our preferences and habits as we watch. It is not difficult to imagine a world in which physical mail no longer exists—the U.S. Postal Service has already scaled back mail delivery services.[94] Nor is it difficult to envision a world in which physical libraries and books no longer exist—library usage has declined with the advent of technology, and funding for operating public libraries

[94] *Postal Service renews push to stop Saturday delivery*, FOXNEWS.COM (July 18, 2013), http://www.foxnews.com/politics/2013/07/18/postal-service-renews-push-to-stop-saturday-delivery/.

has also dropped.[95] We do not have to conceive of a world in which Blockbusters no longer exist—the video rental company announced plans to close all retail stores in 2014.[96] Landlines are quickly being replaced by cell phones, which are now used for purposes far beyond simple phone calls.

The only way for an individual to avoid sharing information with a third party is never to use any telephone at all.[97] Because avoidance is practically impossible, *Smith*'s third-party doctrine has become an almost insurmountable obstacle in asserting Fourth Amendment privacy rights in the digital age. Strict application of the third-party doctrine, when applied in an increasingly sophisticated digital context, seems to subvert the Fourth Amendment,[98] rendering extremely sensitive personal information vulnerable to government search, surveillance, collection, and analysis. And as technology advances, it becomes less necessary for the government to conduct physical searches and seizures of property, papers, and effects. If the Fourth Amendment is to provide any safeguards at all from government intrusion, the third-party doctrine cannot continue to serve as a complete bar to asserting these rights.

III. COMING SOON: A CHANGE TO THE THIRD-PARTY DOCTRINE

Fourth Amendment history discussed in Part I of this Comment demonstrated how the Court's original, strict interpretation of the Fourth Amendment failed to adequately safeguard privacy rights as technology and society changed.[99] But

[95] Press Release, American Library Association, State Funding for Many Public Libraries on Decline (Feb. 10, 2009), *available at* http://www.ala.org/news/news/pressreleases2009/february2009/orscosla.

[96] *Blockbuster Closing All of Its Remaining Retail Stores*, HUFFINGTON POST (Nov. 6, 2013), http://www.huffingtonpost.com/2013/11/06/blockbuster-closing_n_4226735.html.

[97] Donohue, *supra* note 83, at 874.

[98] *See* LAFAVE, *supra* note 20, at § 2.7(b) (criticizing the third-party doctrine and the application of *Smith* as making a "mockery of the Fourth Amendment").

[99] The line of cases between *Olmstead* and *Katz* aptly illustrates the futility of a rigid interpretation of the Fourth Amendment. The Supreme Court struggled with the consequences of its strict trespass-based approach to Fourth Amendment searches in the years before adopting a more augmented approach in *Katz*. *See, e.g.,* Berger v. New York, 388 U.S. 41 (1967); Silverman v. United States, 365 U.S. 505 (1961); On

that same history demonstrates the Court's willingness to reexamine precedent and adopt a less harsh standard in order to meet the challenges posed by technological and societal advancements.[100] Although it may take years, or even decades, for the Court to reach the point of revision, eventually, it does.[101] Right now, the Court is standing on the precipice of change. Two recent Supreme Court cases suggest that the Court is open to reexamining the third-party doctrine's application to new, more invasive searches and surveillance techniques, particularly when those techniques can provide a great deal of personal information about an individual.[102]

Lee v. United States, 343 U.S. 747 (1952); Goldman v. United States, 316 U.S. 129 (1942).

[100] Often times, the Court embraced the dissenting opinions they had once dismissed. *See, e.g.*, Katz v. United States, 389 U.S. 347, 353 (1967) ("[A]lthough a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision has rested."); On Lee v. United States 343 U.S. 747 (1952) (Douglas, J., dissenting) ("The nature of the instrument that science or engineering develops is not important. The controlling, the decisive factor, is the invasion of privacy against the command of the Fourth and Fifth Amendment."); Goldman v. United States 316 U.S. 129, 138 (1942) (Murphy, J. dissenting) ("The conditions of modern life have greatly expanded the range and character of those activities which require protection from intrusive action by Government officials if men and women are to enjoy the full benefit of that privacy which the Fourth Amendment was intended to provide."); Olmstead v. United States, 277 U.S. 438 (1928) (Brandeis, J., dissenting) ("When the Fourth and Fifth Amendments were adopted 'the form that evil had theretorfore taken' had been necessarily simple. Force and violence were then the only means known to man by which a government could directly effect self-incrimination . . . . But 'time works changes, brings into existence new conditions and purposes.' Subtler and more far-reaching means of invading privacy have become available to the government . . . . Ways may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrence of the home.").

[101] As Justice Scalia observed in 2001, "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." Kyllo v. United States, 533 U.S. 27, 33-34 (2001).

[102] United States. v. Jones at 954, 957 (Sotomayor, J., concurring), 964 (Alito, J., concurring).

A. United States v. Jones

In *United States v. Jones*, the Court was asked to determine whether a Fourth Amendment search occurred when police, acting without a warrant, attached a GPS tracking device to a car and subsequently monitored the movements of the car over a period of four weeks.[103] The Court determined that the government's actions constituted a search within the meaning of the Fourth Amendment.[104] In doing so, the Court returned to its original Fourth Amendment threshold test from *Olmstead*, concluding that the attachment of the GPS device constituted a trespass.[105] Justice Scalia, citing the plain language of the Fourth Amendment,[106] called the trespass-focused approach an "irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs."[107]

The concurring opinions, which deviate from the property-based approach, are more significant than the plurality because they cast doubt on the precedent of *Smith* and the third-party doctrine. Justice Alito's concurrence, in which Justices Ginsburg, Breyer, and Kagan joined, states that while short-term monitoring of an

[103] *Id.* at 948 (majority opinion).
[104] *Id.* at 949.
[105] As one analyst commented:

> Without rejecting *Katz* and reasonable expectations, the *Jones* majority returned to property rights as a basis for Fourth Amendment protection. The Government physically occupied private property for the purpose of obtaining information when it attached a GPS device to a private vehicle and used it to gather information. This was a search that the government could not conduct without a valid warrant.

Jim Harper, U.S. v. Jones*: A Big Privacy Win*, CATO BLOG (Jan. 23, 2012), http://www.cato.org/blog/us-v-jones-big-privacy-win (internal quotation marks omitted). *See also* Olmstead v. United States, 277 U.S. 438, 465-67 (1928).
[106] *Jones*, 132 S. Ct. at 949-51 ("*Katz* did not erode the principle 'that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.'" (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring))).
[107] *Id.* at 953; *see also id.* at 955 (Sotomayor, J., concurring) ("Katz's reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

individual's movements may be in accordance with reasonable expectations of privacy, the use of longer-term GPS monitoring involved here resulted in a "degree of intrusion that a reasonable person would not have anticipated."[108] Justice Sotomayor's separate concurrence went further, explicitly questioning the third-party doctrine in the digital age, and stating, "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[109] She added that the doctrine was not well tailored for the digital age, where information is frequently shared with third parties.[110]

B. Riley v. California

The *Jones* concurrences also seem to have laid the groundwork for the Court to reconsider the third-party doctrine while taking account of a changing technological landscape. In the summer of 2014, the Supreme Court, in a landmark decision for privacy rights in the twenty-first century, ruled that police could not search cell phones without a warrant.[111] The Court soundly rejected a number of government arguments that would have extended existing Fourth Amendment doctrine that allows for warrantless searches of physical items (like wallets, purses, or briefcases) found on a person when he or she is arrested to permit searches of cell phones.

Writing for a unanimous Supreme Court, Chief Justice Roberts rejected the argument that searches of data contained on cell phones were analogous to physical searches of items like wallets.[112] In fact, cell phone searches could contain even greater amounts of more private information than the information found in a physical search of a car or home. Information that could be ascertained from

[108] *Id*. at 964.
[109] *Id*. at 957.
[110] *Id.*
[111] *See* Riley v. California, 134 S. Ct. 2473, 2495 (2014) ("Our answer to the question of what police must do before searching a cell phone . . . is accordingly simple—get a warrant.").
[112] *Id*. at 2488-89.

a person's wallet or purse is rather limited, while information that could be ascertained from a person's cell phone is nearly limitless.[113] Comparing the two items and the information that could be collected from each "is like saying a ride on a horseback is materially indistinguishable from a flight to the moon."[114] The Court's message was quite clear: digital searches are a whole new frontier.

The scope of *Riley* was limited—cell phone searches incident to arrest in criminal cases—but the sweeping rhetoric of the Court's opinion suggests that it might also apply to digital searches in other legal contexts.[115] In rejecting the government's argument that law enforcement officers should always be permitted to search a cell phone call log, the Court offered an important clue about the future of the third-party doctrine as well:

> The Government relies on [*Smith*], which . . . concluded that the use of a pen register was not a "search" at all under the Fourth Amendment. There is no dispute here that the officers engaged in a search of Wurie's cell phone. *Moreover, call logs typically contain more than just phone numbers* . . . .[116]

---

[113] *Id.*

[114] *Id.*

[115] *See, e.g.,* Amy Davidson, *Four Ways the Riley Ruling Matters for the NSA*, NEW YORKER (June 29, 2014), http://www.newyorker.com/online/blogs/closeread/2014/06/four-ways-the-riley-ruling-matters-for-the-nsa.html ("[*Riley*] will help define the future of the Fourth Amendment, which affirms individuals' right to 'be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures' in the absence of a warrant. [The decision also touches] on questions of language and technology, and the way one shapes the other."); Robert Graham, Riley v. California*: Support Cloud Privacy Too?*, ERRATA SECURITY (June 25, 2014), http://blog.erratasec.com/2014/06/riley-v-california-support-cloud.html (suggesting *Riley* will have a substantial impact on cloud privacy issues, while noting that the case could have been decided on "narrow grounds," rather than in the sweeping language of the opinion); Dennis Holmes, *What the SCOTUS Cell Phone Decision Means Going Forward* (June 26, 2014), PRIVACY TRACKER, https://www.privacyassociation.org/privacy_tracker/post/what_the_scotus_cell_phone_decision_means_going_forward ("This ruling will almost certainly be applied to other electronic devices such as tablets and laptop computers. There may also be the potential for this ruling to extend its privacy protection beyond the digital information stored on electronic devices to digital information generally.").

[116] Riley v. California, 134 S. Ct. 2473, 2495 (2014) (emphasis added).

This last sentence suggests that the Court believes call log information contains information worthy of Fourth Amendment protection. If that is the case, the Court may be willing to reexamine whether or not metadata, such as the call detail records collected under the Section 215 program, merits some Fourth Amendment protection as well.

IV. A MORE CONSERVATIVE APPLICATION OF THE THIRD-PARTY DOCTRINE

The third-party doctrine has utility. However, where used as a default presumption, particularly in an area involving the fundamental constitutional right to be free of unreasonable government interference, the doctrine's credibility begins to falter.[117] Assuming that the Court is willing to reexamine the broad application of the third-party doctrine in the context of new technology, this Comment suggests that a more discriminating application of the third-party doctrine is possible.

Rather than disposing of the third-party doctrine entirely, or continuing with the assumption that any and all information provided to a third party immediately loses all Fourth Amendment protections, the Court ought first to determine whether the third-party doctrine should apply at all. When an individual has no alternative to providing the information at issue to a third party, the Court should not automatically apply the doctrine as a bar to Fourth Amendment protection. The Court should next consider the nature of the government action, focusing on the context and consequences of the surveillance in order to determine whether a Fourth Amendment search has taken place. These inquiries—(a) determining if an alternative to sharing information with a third party exists, and if not, (b) evaluating the context and consequences of the government action to determine whether a search has taken place—address two categories of concern articulated by the Court in *Jones* and *Riley*: (a) consent, and (b) the degree of privacy subject to government intrusion.

[117] LAFAVE, *supra* note 20, at §2.7(b).

A. Addressing Consent: Is There An Alternative?

In this first stage of analysis, the Court would assess whether an individual could reasonably avoid sharing the information in question with the government and/or a third party.[118] As third party technology has become an integral aspect of our daily lives, it is becoming increasingly difficult to avoid it. So, rather than presuming every instance in which an individual has shared information with a third party is evidence that the individual has voluntarily relinquished his or her "legitimate expectation of privacy," the Court should first ask whether the individual *could reasonably avoid* providing this information to a third party.[119] If the answer is "yes," the third-party doctrine applies and no Fourth Amendment concerns may be raised. But if the answer is "no," the Court would consider the context and consequences of the surveillance, which is discussed in section B below.

The loss of privacy rights accompanying the application of the third-party doctrine is premised on the assumption of voluntary consent.[120] However, as Justice Marshall observed in his *Smith* dissent, information has not truly been "voluntarily" provided to the third party if "as a practical matter, individuals have no realistic

[118] This first inquiry is also designed to address the "reasonable expectation of privacy" element from *Katz*. Katz v. United States, 389 U.S. 347, 360 (1967). (Harlan, J., concurring). Rather than assuming that sharing information with a third party defeats any reasonable expectation of privacy, the Court could instead ask, "Could the individual have reasonably avoided providing this information to a third party?" If the answer is yes, that would confirm that the individual voluntarily provided that information to a third party. He or she assumed the risk that the personal information would be shared with the government and consequently had no reasonable expectation of privacy.

[119] Justice Marshall suggested a similar test: "whether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society." Smith v. Maryland, 442 U.S. 735, 750 (1979).

[120] Kerr, *supra* note 13, at 561, 565 ("Although the third-party doctrine has been framed in terms of the 'reasonable expectation of privacy' test, it is better understood as a consent doctrine. Disclosure to third parties eliminates protection because it implies consent.").

alternative."[121] In *Jones*, Justice Sotomayor questioned whether true consent was possible in the digital age where individuals "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection."[122]

If the Court were to consider the Section 215 program, the answer to this first inquiry would likely be "no." Individuals could not reasonably avoid providing this information to third parties, which in turn, share that information with the government. Given the scope of the Section 215 program,[123] the only way for an individual to avoid providing her or his information to the government is never to use any telephone at all. Even if "opting out" is a possibility, doing so would be tantamount to divesting "oneself of a role in the modern world—impacting one's social relationships, employment, and ability to conduct financial and personal affairs."[124] In effect, there is no alternative available to individuals who want to avoid disclosing their telephone communications to the government. The situation becomes even direr when one considers the Section 215 program not within the confines of this Comment, but in the context of other bulk intelligence collection activities, such as the surveillance program conducted under Section 702 authority, which monitors Internet communications.[125] An individual might be able

[121] *Smith*, 442 U.S.at 750 (Marshall, J. dissenting). Justice Sotomayor echoed this point in her *Jones* concurrence, saying, "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

[122] *Id*.

[123] Greenwald, *supra* note 1.

[124] Laura K. Donohue, *supra* note 83, at 874.

[125] This program was enacted in its current form in July 2008. FISA Amendments Act of 2008 (FAA), Pub. L. No. 110-261, 122 Stat. 2436 (codified at 50 U.S.C. § 1881a et seq. (2012)). Congress reauthorized the FAA in 2012. FAA Reauthorization Act of 2012, Pub. L. 112-238, 126 Stat. 1631 (codified at 50 U.S.C. § 1881a et seq. (2012)). Section 702 empowers the Attorney General ("AG") and Director of National Intelligence ("DNI") to authorize surveillance targeting non-U.S. persons "reasonably believed to be located outside the United States" with the assistance of an electronic communication service provider (*e.g.*, Internet service provider,

to avoid using either the Internet or the telephone in some circumstances, but to opt out of using both would surely render the individual a non-participating member of society. As a matter of practicality, it is not reasonable for an individual in modern society to completely abstain from using the telephone. In this case, when third party information-sharing cannot be reasonably avoided, the Court would next consider the context and consequences of the surveillance.

B. Measuring the Degree of Privacy Invaded: Consider the Context and Consequences

After determining that the third-party doctrine does not apply, the Court should next evaluate the nature of the search or surveillance, looking at the context and consequences of the government action in order to determine if a search for Fourth Amendment purposes has taken place. Justice Marshall's *Smith* dissent suggested a similar evaluation of the surveillance: the Court should "evaluate the 'intrinsic character' of investigative practices with reference to the basic values underlying the Fourth Amendment."[126] Unlike the previous inquiry, there is no single

telephone provider, etc.) in order to "acquire foreign intelligence information." §§ 1881a(a), (b), and (g)(2)(A) (targeting of persons); §1801(i) (defining U.S. persons); § 1801a (outside of the U.S.); § 1881(b)(4) (defining electronic communication service providers); § 1881a(g)(2)(A)(vi) (acquisition of foreign intelligence will require assistance from electronic communication service provider). Although § 1881a(a) states that the targeting is intended to "acquire foreign intelligence information," the FAA section pertaining to certification requirements indicates a lower standard, noting that certifications only need to state that a "significant purpose of the acquisition is to obtain foreign intelligence information." § 1881a(a), (g)(2)(A)(v). Under § 702, the government need not seek individual orders approving individual targets for surveillance. Rather than specifying individual targets in individual FISC applications, the AG and DNI prepare annual certifications that authorize the targeting. The certification, along with AG-approved targeting procedures (measures "reasonably designed" to prevent targeting of U.S. persons and limit the acquisition of U.S. persons' communications), and minimizations procedures (guidelines that govern the collection, retention, and sharing of non-publicly available information obtained from non-consenting U.S. persons) are then presented to the FISC for review. § 1881a(d)(2); § 1881a(e)(2); § 1881a(i)(1)(A).

[126] *Smith*, 442 U.S. at 750-51 (Marshall, J., dissenting) (citing his own dissent in *California Bankers Assn. v. Shultz*, 416 U.S. 21, 95 (1974)).

question that will yield a definitive yes or no answer to aid the Court in determining whether a Fourth Amendment search has occurred. Instead, by considering the collection method and information provided (the context of the surveillance), as well as how that information could be used (the consequences of the surveillance), the Court would evaluate the intrinsic character of the surveillance method. A fact-specific inquiry, aimed at the (1) context, and (2) the consequences of permitting the search, would provide a tool that allows the Court to accommodate new technology and methods. Support for this approach can once again be found in *Jones* and *Riley*.

Although these two opinions cited different privacy-implicating factors about the nature of the *Jones* surveillance, there are two unifying and interrelated themes in both concurrences: concerns about (1) context, including the types of information collected, how the surveillance is conducted, and what the surveillance data could reveal about the individual; and (2) consequences, such as what happens to the surveillance data upon collection, how the data could be used, and what effect the surveillance could have on other constitutional rights. In both instances, it was not the mere attachment of a surveillance device, or even the act of monitoring that caused the concurring justices' trepidation. Instead, their anxiety was triggered by the collection and compilation of the data and what that data might reveal about an individual.

Justice Sotomayor focused on the level of detail provided by the GPS data, and the "record[ing] and aggregat[ing]" of the information,[127] which offered the government with a more detailed image of a person's private life. "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," she wrote in *Jones*.[128] In isolation, GPS monitoring may convey only an address or the coordinates of one's location, but when an accumulation of such information is stored and retained by the government for "years into the future" the

[127] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).
[128] *Id*. at 955.

consequence is that the information may be used to deduce far more intimate personal information.[129] In his concurring opinion, Justice Alito focused on the length of time of the GPS surveillance.[130] When he stated that long-term GPS monitoring violates privacy expectations, implicit in that statement was the understanding that short-term GPS monitoring did not necessarily present the same concerns. This consequence, the more comprehensive picture of the individual created by long-term surveillance, was what seemed to raise Justice Alito's Fourth Amendment concerns.

In both opinions, considering the context of the surveillance allowed the justices to evaluate the consequences of the surveillance outside of one specific instance, looking at the totality of the circumstances. The duration of surveillance mattered a great deal to Justice Alito. Two hours' worth of GPS surveillance likely was not enough surveillance to reach the level of a search, but two months certainly was. Similarly, the size and scope of the surveillance mattered a great deal to Justice Sotomayor. A single set of GPS coordinates in isolation was not enough to reveal intimate details of a person's life, but when compiled with dozens of sets of GPS coordinates, that same surveillance took on an entirely more invasive character. Likewise, in *Riley*, the Court was concerned with both the amount of and the type of information that may be provided by a cell phone search.[131]

Considering the consequences of surveillance similarly allowed the Court to evaluate the realistic implications of that surveillance. In *Jones*, the future of the surveillance data was of concern to Justice Sotomayor, particularly when it would be retained for years and available for the government's use.[132] For Justice Alito,

[129] *Id*. at 956.
[130] *Id*. at 964 (2012) (Alito, J., concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").
[131] Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form unless the phone is.").
[132] *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring).

tracking one location, or even a series of movements over the course of one day, does not necessarily establish a fuller picture of the individual (*e.g.*, one visit to the doctor could just be a check-up).[133] However, collecting or monitoring an individual's movements over a longer period of time permits patterns of behavior to emerge (*e.g.*, several visits to the doctor over the course of a week could indicate a more serious medical issue).[134] For him, the consequence of long-term surveillance was that greater information may be gleaned than in the short term.

Considering the context and consequences of the search allows the Court to tackle the Fourth Amendment implications of the activity. Different methods of surveillance can yield a variety of data and can be exploited in different manners. One case of permissible surveillance under the Fourth Amendment—such as the use of a pen register to collect the metadata from a single phone line of a known criminal suspect—may require a less searching analysis than other cases—such as the use of more technologically advanced program that monitors millions of individual phone lines, with the capability to collect, retain, and search the resulting metadata for years into the future.[135]

V. CONCLUSION

Media reports disclosing the existence of the Section 215 telephony metadata program reignited debate over the third-party doctrine's applicability in the digital age. As individuals increasingly provide vast amounts of personal data to third parties in the course of their daily lives, the third-party doctrine has become a nearly insurmountable obstacle to asserting Fourth Amendment privacy rights. A more conservative application of the third-party doctrine is needed, and two recent decisions suggest the Supreme Court is open to revisiting the doctrine.

---

[133] *Id*. at 964 (Alito, J., concurring).
[134] *Id.*
[135] *See* Klayman v. Obama, 957 F. Supp.2d 1, 32-37 (D.D.C. 2013) (contrasting the use of pen register surveillance with the Section 215 program).

If the Court has the opportunity to limit the scope of the third-party doctrine, then existing Fourth Amendment jurisprudence, including *Jones* and *Riley*, provide some guidance for how the Court may proceed. It should first conduct an inquiry as to the appropriateness of applying the doctrine. Rather than viewing the disclosure of information to a third party as evidence that an individual could have no "legitimate expectation of privacy," the Court should ask whether the individual *could reasonably avoid* providing this information to a third party. If disclosure was unavoidable, the Court should next conduct a fact-specific inquiry into the "intrinsic character" of the surveillance, evaluating the context and consequences of the government activity in question.

As society's reliance on technology deepens, the third-party doctrine threatens to engulf the entire Fourth Amendment. In light of this reality, a more restrained application of the third-party doctrine will be necessary to preserve the effect and meaning of the Fourth Amendment. Adopting the approach outlined above would help limit the reach of the third-party doctrine without undermining its original purpose.