Washington Journal of Law, Technology & Arts

Volume 10 | Issue 1 Article 5

7-1-2014

Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?

Elizabeth Atkins

WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 10, ISSUE 1 SUMMER 2014

SPYING ON AMERICANS: AT WHAT POINT DOES THE NSA'S COLLECTION AND SEARCHING OF METADATA VIOLATE THE FOURTH AMENDMENT?

Elizabeth Atkins[*]

Cite as: 10 Wash. J.L. Tech. & Arts 51 (2014)
http://digital.lib.washington.edu/dspace-law/handle/1773.1/1390

ABSTRACT

Edward Snowden became a household name on June 5, 2013, when he leaked highly classified documents revealing that the American Government was spying on its citizens. The information exposed that the National Security Agency (NSA) collected millions of American's metadata through forced cooperation with telephone-service providers. Metadata contains sensitive and private information about a person's life. When collected and searched, metadata can reveal a portrait of a person's intimate activities amounting to a violation of one's reasonable expectation of privacy.

This Article suggests changing the current standard allowing the NSA to collect and search metadata under Section 215 of the USA PATRIOT Act. The threshold needed to obtain and search a person's metadata should be raised from the current standard of reasonable and articulable suspicion to a higher burden of probable cause. Since Mr. Snowden's unauthorized disclosure, there has been public outcry regarding metadata collection. In response, President Obama issued a Public Policy Directive limiting the scope of metadata that the NSA can collect. Additionally, Congress has proposed legislation changing how the NSA collects, stores, and searches

[*] Elizabeth Atkins, Thomas Jefferson School of Law, Class of 2015. Thank you to Professor Cohn for her valuable insight and expertise, and to Randy Abreu for his patience and infinite support.

metadata. The bills, however, keep intact the minimum reasonable and articulable standard necessary to search metadata.

The breadth of information that can be gleaned from metadata makes it intrusive and subjects it to the Fourth Amendment. Yet gathering and searching metadata can be a valuable tool in the fight against terrorism and protecting American citizens from future attacks. Requiring the threshold to be raised to a probable cause determination adequately balances privacy interests against national security interests.

TABLE OF CONTENTS

INTRODUCTION

> "Metadata is what allows an actual enumerated understanding, a precise record of all the private activities in all of our lives. It shows our associations, our political affiliations and our actual activities."[1]

[1] Edward Snowden, Remarks at the Amnesty International USA Annual General Meeting (Apr. 5, 2014); *see* Karl Plume, *Snowden, Greenwald urge caution of wider government monitoring at Amnesty event*, REUTERS (Apr. 5, 2014, 8:29 PM), http://www.reuters.com/article/2014/04/06/us-usa-security-

On June 5, 2013, Edward Snowden shocked the world when he revealed highly classified National Security Agency (NSA) documents to *The Guardian*, a British daily newspaper.[2] These documents exposed the Foreign Intelligence Surveillance Court's (FISC) secret order instructing Verizon to collect metadata from all telephone calls within the United States and abroad.[3] Snowden disclosed that the NSA was spying on American citizens through the mass collection of "telephony metadata," with Congressional and Presidential authorization.[4] Immediately thereafter, President Obama and Senator Diane Feinstein began downplaying the Orwellian nature of the program, notably justifying it by stating: "*it's just metadata*."[5]

However, the mass collection of metadata was troubling to many Americans because the NSA was not only spying on those believed to be associated with Al-Qaida but also on messages between Americans without ties to suspected terrorism.[6] Even

---

snowden-idUSBREA3500320140406.

[2] Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[3] Marjorie Cohn, *NSA Metadata Collection: Fourth Amendment Violation*, JURIST (Jan. 15, 2014), http://jurist.org/forum/2014/01/marjorie-cohn-nsa-metadata.php; Administration White Paper, *Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* 1–2 (Aug. 9, 2013), *available at* http://op.bna.com/der.nsf/id/sbay-9aeu73/.

[4] In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From [REDACTED], No. BR 13–80, 2013 U.S. Dist. LEXIS 147002 (FISA Ct. Apr. 25, 2013) [hereinafter Primary Order]; Greenwald, *supra* note 2.

[5] President Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter President Obama's Remarks]; *Transcript: Diane Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program [hereinafter *Senator Feinstein's Remarks*]; *see, e.g.*, ALDOUS HUXLEY, BRAVE NEW WORLD (1932); GEORGE ORWELL, ANIMAL FARM (1945); GEORGE ORWELL, NINETEEN EIGHTY-FOUR (1949). These books popularized the concept that would come to be known as "Orwellian", which describes manipulation of citizens by a totalitarian government by use of secret surveillance.

[6] *Id.*; James Ball, *NSA Monitored calls of 35 world leaders after US official*

more disturbing was the massive amount of sensitive and personal information that could be gathered from metadata in and of itself.[7] As metadata became defined in the public sphere, it became clear to Americans and human rights organizations alike that it's not *just* metadata.

The NSA's sweeping surveillance was legalized when Congress passed the USA PATRIOT Act, arguably the most expansive piece of legislation in America's history.[8] Post-9/11, the USA PATRIOT Act allowed the government to use surveillance and technology more aggressively than ever before in an attempt to prevent future attacks.[9]

Congress originally authorized metadata collection under Section 215 of the Act.[10] Section 215 was amended in the USA PATRIOT Improvement and Reauthorization Act of 2005, which required the government to provide "a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant . . . against international terrorism . . . ."[11] Section 215 expanded the government's ability to compel the

---

handed over contacts, THE GUARDIAN (Oct. 24, 2013), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls; *see* Josh Levs & Catherine E. Shoichet, *Europe furious, 'shocked' by report of U.S. spying*, CNN.COM, (July 1, 2013), http://www.cnn.com/2013/06/30/world/europe/eu-nsa (explaining that European officials are shocked and outraged by the reports Snowden leaked that the NSA is spying on European Union leaders).

[7] *See infra* Part IV.

[8] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), 107 Pub. L. No. 56, § 215, 115 Stat. 272, 287–88 (2001) (codified in scattered titles of U.S.C.); Drew Fennell, *The USA PATRIOT Act*: *Can we be Both Safe and Free?*, 21 DEL. LAW. 10, 10 (2003) ("On October 25, 2001, a matter of weeks after September 11, the U.S. Congress passed the USA PATRIOT Act, a bill that contains the most sweeping and comprehensive changes in domestic law enforcement in history . . . .").

[9] Richard A. Clarke et al., THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 73 (Dec. 12, 2013) [hereinafter PRESIDENT'S REVIEW GROUP REPORT].

[10] USA PATRIOT Act § 215.

[11] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

production of "any tangible things including books, records, papers, documents, and other items."[12]

Under this expanded program, the government began collecting United States citizens' call records without warrants. This program is unprecedented because it targeted not only phone calls made to suspects living outside of the country but call records *between American citizens* themselves. The government systematically collected and searched sensitive information on its own citizens without meeting the constitutional constraints of the Fourth Amendment. In most cases, the Fourth Amendment imposes a warrant requirement to perform a search.[13] Prior to performing a search on a constitutionally protected area, a person must first have probable cause and then obtain a warrant from a judge.[14] The government's failure to obtain a warrant before searching a person's metadata records violates that person's reasonable expectation of privacy.[15] Even though government officials, including President Obama, have reassured American citizens that they are not listening to the content of their calls, the metadata of these calls can still reveal an illuminating look at the callers' private lives.

For example, consider Person X, an American citizen born in the United States. Person X is a college-educated, 26-year-old program developer who just began law school. He has no association to terrorist activity. Yet every day the NSA collects his phone records and stores all of his metadata in a database waiting to be queried.

Imagine one day the NSA suspects that Person X is associated with a terrorist organization. Every phone number he has contacted within the past five years is collected. The information the government could collect about Person X based solely on his metadata displays detailed information about his life: the abortion clinic he called in college after an accident with his girlfriend, his pastor and religious affiliation, his therapist, his association with the National Rifle Association, the presence of bill collectors, a

---

[12] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 81.
[13] Katz v. United States, 389 U.S. 347 (1967).
[14] *Id.*
[15] *Id.*

clinic that treats sexually transmitted diseases, or the pizza restaurant down the street from his house from which he orders. Suddenly, what seems like an innocent and harmless amount of "metadata," coupled with simple investigation, becomes an intimate look into the personal life of Person X. The government has no right to this level of private information about a person, absent a warrant as required by the Fourth Amendment. Yet the government collects this data on U.S. citizens on a daily basis.

Part I of this Article provides an in-depth background of the development of the right to privacy with respect to modern technology and surveillance. Part II discusses the history that led to the passage of the USA PATRIOT Act, particularly Section 215, which authorizes metadata collection. Part III discusses current challenges to the metadata collection program. Part IV argues that the threshold to search metadata under Section 215 should be raised from a reasonable articulable suspicion of terrorist activity to the higher standard of probable cause.

I. THE HISTORY OF MODERN SURVEILLANCE DEVELOPED UNDER THE FOURTH AMENDMENT

Modern surveillance can be traced to the Cold War era; specifically, to the Vietnam War.[16] Former Presidents Lyndon Johnson and Richard Nixon encouraged expansive surveillance of individuals and organizations opposed to the war.[17] As a result, the CIA began monitoring antiwar activists.[18] In the 1950s, FBI Director J. Edgar Hoover conducted a massive counter-intelligence program, known as COINTELPRO.[19] Under the guise of fighting communism, the government engaged in surveillance, infiltration, dissemination of false information, and abuse of the criminal justice system.[20] In the 1970s, a series of congressional committees

[16] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 54.
[17] *Id.* at 54–55.
[18] *Id.*
[19] Natsu Taylor Saito, *Whose Liberty? Whose Security? The USA PATRIOT Act in the Context of COINTELPRO and the Unlawful Repression of Political Dissent*, 81 OR. L. REV. 1051, 1080–88 (2002).
[20] *Id.*

convened to discuss what led to the abuses that had taken place under COINTELPRO during the previous decades.[21]

The final report, containing 96 policy recommendations, was prepared by the Church Committee, named after Chairman Senator Frank Church.[22] The Church Committee Report concluded that spying endangers both the security of the nation and the rights of Americans.[23] In 1976, President Gerald Ford formally prohibited the CIA from using surveillance measures on American citizens unless explicitly approved by the Attorney General.[24] The use of electronic surveillance for national security purposes became a growing concern, culminating in a series of privacy cases.[25] These cases governed the way courts have viewed electronic data for more than 40 years.[26]

A. The Court's Development of a Right to Privacy in Emerging Technology

Three Supreme Court cases have helped shape the right to privacy in light of emerging technological advancements.[27] The invention of electronic devices led to the discovery of how to eavesdrop on communications that use these devices. The police turned to wiretapping to monitor otherwise private conversations in

---

[21] *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate*, 94th Cong. (1976) [hereinafter *Church Committee Report*].

[22] Nicholas C. Dranias, *The Patriot Act of 2001 versus the 1976 Church Committee Report: An Unavoidable Clash of Fundamental Policy Judgments*, 17 C.B.A. REC. 28, 29 (2003).

[23] *Id.* at 30.

[24] Exec. Order No. 11905, United States Foreign Intelligence Activities, 41 Fed. Reg. 7703 (Feb. 18, 1976).

[25] *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 478 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347 (1967); Miller v. United States, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979); United States v. Jones, 132 S. Ct. 945 (2012).

[26] *See, e.g.*, *Olmstead*, 227 U.S. at 478; *Katz*, 389 U.S. 347; *Miller*, 425 U.S. 435; *Smith*, 442 U.S. 735; *Jones*, 132 S. Ct. 945 (cases cited range from 1928 to 2012).

[27] *See Olmstead*, 277 U.S. 438; *Katz*, 389 U.S. 347; *Jones*, 132 S. Ct. 945.

order to collect evidence against suspected criminals. Those people whose conversations were overheard challenged the collection of such data, and the debate over privacy rights through electronic communications began. *Olmstead v. United States*, *Katz v. United States*, and *United States v. Jones* all involve electronic surveillance and the right to privacy under the Fourth Amendment.[28]

1. *Olmstead v. United States*: Establishing Privacy as a Trespassory Doctrine

In *Olmstead*, federal agents installed wiretaps on phone lines to investigate a conspiracy to distribute alcohol during the Prohibition.[29] The agents tapped phone lines leading into the suspects' houses and offices without actually entering the premises.[30] They gathered evidence for five months and recorded multiple conversations.[31] The Supreme Court held that a wiretap was not a "search" within the meaning of the Fourth Amendment because there was not a physical trespass onto real property.[32] This holding paved the way for the trespassory/non-trespassory distinction regarding invasions into constitutionally protected areas.[33] However, as people increasingly relied on the telephone for conducting their private affairs, *Olmstead's* reasoning became more difficult to maintain.[34]

Indeed, Justice Louis Brandeis' dissent in *Olmstead* has become the flagship of privacy rights arguments in post-*Olmstead* cases.[35] Justice Brandeis disagreed with the majority's distinction

---

[28] *Olmstead*, 277 U.S. 438; *Katz*, 389 U.S. 347; *Jones*, 132 S. Ct. 945.

[29] *Olmstead*, 277 U.S. at 455–58 (describing the factual background of the case).

[30] *Id.*

[31] *Id.* at 471 (Brandeis, J., dissenting).

[32] *Id.* at 466.

[33] Lon A. Berk, *After Jones, The Deluge: The Fourth Amendment's Treatment of Information, Big Data and the Cloud*, 14 J. HIGH TECH. L. 1, 12 (2014).

[34] *Id.* at 13.

[35] Neil M. Richards, *The Puzzle of Brandeis, Privacy, and Speech*, 63 VAND. L. REV. 1295, 1296 (2010).

between trespassory and non-trespassory invasions.[36] He stated that unjustified searches and seizures violate the Fourth Amendment no matter how the information was gathered.[37] The principles set forth in the majority, Brandeis reasoned, go to the very nature of "constitutional liberty and security" and apply to all invasions by the government.[38] What violates a person's personal liberty is not the actual rummaging of drawers, but the "invasion of his indefeasible right of personal security," Brandeis wrote.[39] In comparing wiretapping to mail tampering, Brandeis thought that the invasion of the telephone was far worse.[40] When a telephone line is tapped, confidential conversations are heard and privacy is violated at both ends of the line.[41]

2. *Katz v. United States*: Overruling *Olmstead* and Paving the Way toward Non-Trespassory Privacy Rights

In 1967 the Supreme Court finally adopted a different test for determining whether a search was reasonable, relying principally on the Brandeis dissent in *Olmstead*.[42] In *Katz v. United States*, Katz was a bookmaker who used a telephone booth to transmit wagering information across state lines.[43] Federal agents used an electronic listening device outside of the telephone booth and obtained recordings of the calls.[44] The recordings were used at trial to convict Katz.[45] On appeal, the government based its argument on the trespassory view of the Fourth Amendment, noting that the agents were outside of the phone booth and not within a

[36] *Olmstead*, 277 U.S. at 477–78 (Brandeis, J., dissenting).

[37] *Id.* ("Unjustified search and seizure violates the Fourth Amendment, whatever the character of the paper; whether the paper when taken by the federal officers was in the home, in an office, or elsewhere; whether the taking was effected by force, by fraud, or in the orderly process of a court's procedure.").

[38] *Id.* at 474 (quoting Boyd v. United States, 116 U. S. 616).

[39] *Id.* at 475 (quoting Boyd v. United States, 116 U. S. 616).

[40] *Id.* at 475.

[41] *Id.*

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

[43] *Id.* at 348.

[44] *Id.* at 348–54.

[45] *Id.* at 348.

constitutionally protected area.[46]

The Supreme Court rejected this argument and overruled the literal interpretation of *Olmstead*, recognizing that the Fourth Amendment "protects people not places."[47] Specifically, the Court stated that telephone technology had become "vital" to private communications and rejected the argument that the use of a telephone was analogous to a broadcast of one's voice into public areas.[48] The Justices reasoned that the Fourth Amendment protects people, not simply areas, and a violation of the Fourth Amendment cannot turn on the presence or absence of a physical intrusion.[49]

Justice John Harlan's concurrence built upon the framework set forth in the majority opinion.[50] He formulated the "reasonable expectation" test for determining whether government activity constitutes a violation of the Fourth Amendment.[51] The two-prong test requires that (1) the individual has an actual (subjective) expectation to privacy, and (2) the expectation is one society is prepared to recognize as "reasonable."[52] If both prongs are satisfied, there is a reasonable expectation of privacy.[53] Harlan's test, and not the majority opinion, was adopted in *Smith v. Maryland* and is the test now used to determine whether a search has taken place.[54]

3. *United States v. Jones*: Foreshadowing Modern Non-Trespassory Privacy Concerns

In 2010 the Supreme Court unanimously held that tracking a person's movements for a month via a GPS monitoring device that police had attached to the driver's vehicle without a warrant

---

[46] *Id.* at 352.
[47] *Id.* at 351.
[48] *Id.* at 352.
[49] *Id.* at 353.
[50] *Id.* at 361 (Harlan, J., concurring).
[51] *Id.* at 360–61.
[52] *Id.* at 361.
[53] *Id.*
[54] Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1, 7 (2009).

violates the Fourth Amendment.[55] In *United States v. Jones*, federal agents were investigating Mr. Jones for narcotics distribution and placed a GPS device under his Jeep without a warrant.[56] For the next 28 days, agents used the device to track the Jeep and collected more than 2,000 pages of data.[57]

Jones was convicted after the trial court found that his Fourth Amendment rights were not violated since there was no reasonable expectation of privacy in movements from one place to another.[58] On appeal, the Supreme Court found that a "reasonable person does not expect anyone to monitor and retain a record of every time he drives his car . . . rather, he expects his movements to remain 'disconnected and anonymous.'"[59] The Supreme Court's opinion was not based on the *Katz* reasonable expectation of privacy test, but instead relied on the *Olmstead* analysis regarding common law trespass.[60]

B. Smith v. Maryland*: Developing the Third-Party Doctrine*

The third-party doctrine further confuses a person's privacy rights when electronic devices are involved. In *Smith v. Maryland*, the Supreme Court held that one who gives information to a third-party does not have a reasonable expectation of privacy, and thus falls outside the purview of the Fourth Amendment.[61]

In *Smith*, the defendant Smith was convicted of robbery after the police instructed the telephone company to monitor the phone numbers Smith dialed. [62] After the victim was robbed, she gave

---

[55] United States v. Jones, 132 S. Ct. 945, 949 (2012).
[56] *Id.* at 948.
[57] *Id.*
[58] *Id.*
[59] United States v. Maynard, 615 F.3d 544, 561 (D.C. Cir. 2010) (quoting United States v. Wylie, 569 F.2d 62, 6 (D.C. Cir. 1977)) ("[P]olice-citizen communications which take place under circumstances in which the citizen's 'freedom to walk away' is not limited by anything other than his desire to cooperate do not amount to 'seizures' of the person."), *cert. denied* 131 S. Ct. 671 (2010), *aff'd*, *Jones*, 132 S. Ct. 945.
[60] *Jones*, 132 S. Ct. at 953.
[61] Smith v. Maryland, 442 U.S. 735, 742 (1979).
[62] *Id.* at 737.

police a description of the attacker and of an automobile parked near the scene.[63] She also began receiving threatening phone calls from the same attacker.[64] Eleven days later, a police officer spotted a man matching the description provided by the victim driving the same automobile.[65] The police officer traced the license plate to Michael Smith.[66] The next day the telephone company, at the request of the police department, installed a pen register at its main office to record the numbers dialed from Smith's telephone.[67] The police did not have a warrant before the company installed the pen register.[68] The register revealed Smith had called the victim after the robbery, permitting police to obtain a warrant to search his home.[69] Smith was arrested based on evidence gathered in his home and afterwards he was positively identified by the victim as her attacker.[70]

During pre-trial motions, Smith sought to suppress all evidence derived from the pen register, claiming the pen register violated his Fourth Amendment right to privacy because the police failed to obtain a warrant.[71] The trial court denied the motion and after Smith was convicted, he appealed.[72] The court of appeals affirmed the conviction, holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment [sic] is implicated by the use of a pen register installed at the central offices of the telephone company."[73] Three judges dissented, one stating that individuals do have a legitimate expectation of privacy in the phone numbers they dial and concluding that the pen register was a search.[74]

---

[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.* at 737–38.
[73] *Id.* at 738 (quoting Smith v. State of Maryland, 283 Md. 156, 173 (1978)).
[74] *Id.* at 738.

The Supreme Court first quoted *Katz v. United States* in defining what constitutes a "search" under the Fourth Amendment.[75] The Court noted the difference between *Katz* and the pen register used against Smith.[76] In *Katz* the police used a device to listen to the content of the defendant's conversation. [77] In *Smith*, the police only obtained a telephone number.[78] The Supreme Court held that there is no reasonable expectation of privacy in the numbers dialed from a phone because the user voluntarily dials the numbers and conveys the information to the telephone company.[79] The justification for this holding was twofold. First, the Court doubted that "people in general entertain any actual expectation of privacy in the numbers they dial."[80] Second, the Court wrote that even if Smith did have an expectation of privacy in the numbers he dialed, it was not one that society was willing to recognize as reasonable.[81] This was based on the Court's previous holdings that there is no legitimate expectation of privacy in information disclosed to a third party.[82]

Three of the Justices dissented, believing that Smith had a right to privacy in the phone numbers he dialed, and that the pen register did constitute a search under the Fourth Amendment.[83] Justice Thurgood Marshall wrote, "Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes."[84] There was no way for the Supreme Court to know its ruling would become the justification for the metadata

---

[75] *Id.* at 739–40.
[76] *Id.* at 740.
[77] *Id.*
[78] *Id.*
[79] *Id.* at 745.
[80] *Id.* at 742.
[81] *Id.* at 743–44.
[82] *Id.* at 744 (citing United States v. Miller, 425 U.S. 435, 442–444; Couch v. United States, 409 U.S. 322, 335–36; United States v. White, 401 U.S. 745, 752 (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963)).
[83] *Smith*, 442 U.S. at 746–52 (Stewart, Brennan, Marshall, JJ., dissenting).
[84] *Id.* at 740.

collection program. Yet the three dissenting Justices foreshadowed the exact issue that is currently the subject of public debate: whether society is ready to recognize a right to privacy in metadata collected under Section 215 of the USA PATRIOT Act.

II. ENACTMENT OF THE USA PATRIOT ACT

Two pieces of legislation led to the metadata program under Section 215. The first is the Foreign Intelligence Surveillance Act of 1979, and the second is the USA PATRIOT Act, which has been amended several times since its inception in 2001.[85] The last amendment expanded Section 215, which allowed the collection of metadata as revealed by the Snowden disclosures in 2013.[86]

A. The Foreign Intelligence Surveillance Act of 1978: Wiretapping and Foreign Intelligence Surveillance

In order to implement the recommendations of the Church Committee Report, Congress enacted the Foreign Intelligence Surveillance Act ("FISA") of 1978.[87] One of FISA's goals was to reconcile the Church Committee's concerns for protecting people against the abuse of power documented in the 1970's with the preservation of the government's ability to protect itself from foreign threat.[88] Although *Katz* held that the Fourth Amendment prohibited the government from wiretapping without a warrant if the interception would produce *evidence of criminal conduct*, it remained unclear whether the same was true when the government investigated "activities of foreign power."[89]

FISA was designed to address these questions, and its creation involved strict rules and structured oversight by all three branches

---

[85] Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1801 et seq. (1978); USA PATRIOT Act of 2001, 107 Pub. L. No. 56, § 215, 115 Stat. 272, 287–88 (2001) (codified in scattered titles of U.S.C.).

[86] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[87] FISA § 1801.

[88] *Id.* at 64.

[89] United States v. United States District Court for the Eastern District of Michigan, 407 U.S. 297, 308 (1972).

of government.[90] FISA also created the Foreign Intelligence Surveillance Court ("FISC") to provide judicial oversight of the government's authority and to handle the classified information encompassed by foreign intelligence.[91] Under the original FISA, any governmental agency seeking to use electronic surveillance for *foreign intelligence* purposes must obtain a warrant by showing probable cause that the target is an agent of a foreign power.[92] Between its enactment in 1978 and September 11, 2001, FISA only slightly widened its scope to include methods of investigation beyond electronic surveillance.[93]

B. September 11, 2001, and the USA PATRIOT Act

The events that took place on September 11, 2001, caused the greatest number of casualties from a terrorist act on United States soil.[94] In response to the 9/11 attacks, Former President George W. Bush declared a "war on terrorism."[95] On October 4, 2001, the Senate proposed legislation designed to enhance law enforcement's ability to investigate potential and actual acts of terrorism.[96] The Senate passed the bill with a vote of 96-to-1 after ten days.[97] The House of Representatives proposed and approved its own version of an anti-terrorism bill the following day by a vote of 337 to 79.[98] These measures led to the USA PATRIOT Act of 2001, passed by Congress on October 25, 2001, and signed into law by President Bush the next day.[99] The USA PATRIOT Act

---

[90] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 65.

[91] *Id.* at 66.

[92] 50 U.S.C. §§ 1801–11.

[93] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 68.

[94] Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOY. U. CHI. L.J. 933, 959 (2002) [hereinafter *Hijacking Civil Liberties*].

[95] George W. Bush, Statement by the President in His Address to the Nation (Sept. 11, 2001), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010911-16.html.

[96] Evans, *supra* note 94, at 966.

[97] *Id.* at 966.

[98] *Id.* at 967.

[99] *Id.*

was designed to strengthen domestic security and broaden the powers of law enforcement agencies to identify and stop terrorism.[100] Split into ten parts, Title II: Enhanced Surveillance Procedures authorizes metadata collection under Section 215.[101]

C. The Metadata Collection Program is Created under Section 215 in Two FISC Orders

When FISA was originally enacted in 1978, the government did not have authority to compel documents.[102] Congress amended FISA in 1998 after the Oklahoma bombings to allow FISC to compel a narrow set of documents.[103] The USA PATRIOT Act significantly expanded FISC's authority to compel documents, but was narrowed in the USA PATRIOT Act Improvement and Reauthorization Act of 2005.[104] As codified, Section 215 authorizes FISC to issue an order for the "production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism."[105] Through two FISC orders, however, the systematic metadata collection program was created. First, FISC authorized mass collection of metadata in the "Primary Order."[106] Second, Verizon was ordered to submit metadata to FISC and the NSA on an ongoing basis through the "Secondary Order."[107]

---

[100] *Id.* at 965.

[101] USA PATRIOT ACT OF 2001, 107 PUB. L. NO. 56, § 215, 115 STAT. 272, 287–88 (2001) (CODIFIED IN SCATTERED TITLES OF U.S.C.).

[102] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9, at 80.

[103] *Id.*

[104] *Id.* at 81; USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[105] USA PATRIOT ACT § 215.

[106] Primary Order, *supra* note 4.

[107] In re Application of the FBI for an Order Requiring the Prod. of Tangible Things From Verizon Bus. Network Servs., Inc. ex. rel. MCI Commc'n Servs. Inc. d/b/a Verizon Bus. Servs., No. BR 13–80, 2013 U.S. Dist. LEXIS 147002, (FISA Ct. Apr. 25, 2013) [hereinafter Secondary Order].

1. The Primary Order to Collect Metadata

The NSA, under Section 215, issued a Primary Order in 2006 that set out the framework and requirements for the mass collection of metadata.[108] The Primary Order required a high-ranking NSA official to determine if there is a reasonable articulable suspicion that the number being queried is associated with an international terrorist organization.[109] Currently, there are 22 designated agents who can authorize a query.[110] These agents may access the information without approval from a FISC court order.[111] The Government must seek authorization for Section 215 periodically from FISC, which it does typically every 90 days.[112]

Since 2006, different FISC judges have authorized the use of Section 215 35 times.[113] However, during the authorization process, FISC found on one occasion that the Government failed to comply with the minimization procedures.[114] In January 2009, the government reported that it used an "alert list" to search metadata that was not approved under the requisite reasonable articulable suspicion standard.[115] The FISC judge concluded that the government engaged in systematic noncompliance and ordered the NSA to seek FISC approval before conducting any inquiry for a probationary six-month period.[116]

Once an agent authorizes a query of a suspect, the agent enters the phone number with which the suspect is associated.[117] The phone number is the original identifier and is called a "seed."[118]

---

[108] *Id.* at 3–4.
[109] *Id.* at 5–7.
[110] *Id.*
[111] *Id.* at 9.
[112] *Id.*
[113] In Re Production of Tangible Things from [Undisclosed Service Provider], Docket Number BR 08–13 (Mar. 2, 2009) (authorizing Section 215 35 times from 2006 through October 2013).
[114] *Id.*
[115] *Id.*
[116] *Id.*; Klayman v. Obama, 957 F. Supp. 2d 1, 18 (stating the probationary period lasted only six months).
[117] *Klayman*, 957 F. Supp. 2d at 16.
[118] *Id.*

When a seed is queried, it is referred to as a "hop."[119] When the phone number is initially queried during the first hop, the NSA captures all metadata directly associated with that seed.[120] The NSA can then make a second hop, in which the NSA captures all metadata associated with each number identified from the first hop.[121] The NSA had authorization, until February 5, 2014, to make one additional hop, for a total of three hops.[122] Once the NSA has collected metadata from the three hops, it can conduct an unlimited number of searches with the breadth of data collected without oversight from FISC and without making additional reasonable articulable suspicion determinations.[123]

2. The Secondary Order Directing Verizon to Submit Metadata

The Secondary Order directed Verizon to provide to the NSA all metadata "on an ongoing daily basis."[124] It directed Verizon to produce "all call detail records" or "telephony metadata" created both between the United States and abroad, and "wholly within the United States, including local telephone calls."[125] The metadata included session-identifying information, trunk identifier, telephone calling card numbers, and call durations.[126] The last part of the order prohibited Verizon from disclosing any information given to the NSA or FBI.[127] Because of the gag order, Verizon and other phone companies could not discuss or reveal that their customers' metadata was being systematically transmitted to the NSA until the Snowden disclosures leaked the information.[128]

---

[119] ACLU v. Clapper, 959 F. Supp. 2d 724, 734 (S.D.N.Y. Dec. 27, 2013).
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] Klayman v. Obama, 957 F. Supp. 2d 1, 17.
[124] Secondary Order, *supra* note 107.
[125] *Id.* at 3.
[126] *Id.*
[127] *Id.* at 2–3.
[128] *Id.*

III. CURRENT CHALLENGES TO THE METADATA COLLECTION PROGRAM AUTHORIZED BY SECTION 215 OF THE USA PATRIOT ACT

Since Snowden revealed classified documents uncovering the metadata collection program, there have been several challenges regarding the constitutionality of Section 215. First, two U.S. District Courts have issued conflicting holdings regarding Section 215.[129] Second, the Presidential Review Group's massive review on the USA PATRIOT Act found Section 215 to be unconstitutional.[130] Third, none of President Obama's proposed changes to Section 215 have been passed into law.[131] Fourth, Congress proposed several pieces of legislation reforming Section 215 that are currently sitting in House Committees.[132]

A. Klayman v. Obama*: Section 215 is Likely to be Unconstitutional*

In *Klayman v. Obama*, the court found the NSA program "almost certainly" violates the Fourth Amendment.[133] The court distinguished the current NSA program from the pen register in *Smith*, claiming an "Orwellian" intelligence gathering system between telecommunication companies and the Government.[134] The court in *Klayman* found that the problem with this system is that people have entirely different relationships with phones today

---

[129] ACLU v. Clapper, 959 F. Supp. 2d 724, 757; Klayman v. Obama, 957 F. Supp. 2d 1, 43.

[130] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9.

[131] The White House, *FACT SHEET: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program*, THE WHITE HOUSE (Mar. 27, 2014), http://www.whitehouse.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m [hereinafter *Obama's Proposal for Ending Section 215*].

[132] LIBERT-E Act, H.R. 2399, 113th Cong. (1st Sess. 2013); USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013); Telephone Metadata Reform Act, H.R. 3875, 113th Cong. (2nd Sess. 2014).

[133] *Klayman*, 957 F. Supp. 2d at 32 ("I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.").

[134] *Id.* at 33; *see supra* note 5 (defining "Orwellian").

than they did when the third-party doctrine was created in *Smith*.[135] Call records, which then would have given the police only scattered information about one's life, now "reveal an entire mosaic—a vibrant and constantly updating picture of the person's life."[136] The court further reasoned that modern society is better prepared and more willing to accept a reasonable expectation of privacy in a phone's metadata, making the metadata program unconstitutional under the Fourth Amendment.[137]

B. ACLU v. Clapper*: Section 215 is Constitutional under the Third-Party Doctrine*

In *ACLU v. Clapper*, the ACLU and other non-profit organizations filed a lawsuit less than a week after the disclosure of the Secondary Order.[138] The NSA collected metadata of the ACLU, a Verizon customer, as required by the Secondary Order.[139] The ACLU's phone records could be used to identify confidential clients such as journalists, legislators, and members of the public.[140] This, they argued, violated their First and Fourth Amendment rights.[141]

The court followed a strict reading of *Smith*.[142] It held that, because Verizon users—ACLU included—voluntarily transmitted numbers they dialed, there was no reasonable expectation of privacy in those numbers.[143] The court stated that the sheer volume of information the NSA can collect and store does not make it a Fourth Amendment violation.[144] Ultimately, the court dismissed the case for lack of standing. [145] The ACLU filed an appeal on

---

[135] *Klayman*, 957 F. Supp. 2d at 36.
[136] *Id.*
[137] *Id.*
[138] ACLU v. Clapper, 959 F. Supp. 2d 724, 735 (S.D.N.Y. 2013).
[139] *Id.* at 735.
[140] *Id.*
[141] *Id.*
[142] *Id.* at 751–52.
[143] *Id.* at 752.
[144] *Id.*
[145] *Id.* at 754.

March 6, 2014.[146] The Government's reply brief was filed on April 10, 2014.[147] The ACLU filed an additional reply brief on April 24, 2014, and the case is pending hearing as of the writing of this Article.[148]

C. The President's Review Group Report Recommends Terminating Metadata Collection due to Privacy Concerns

In response to the general concerns of the American public after the Snowden disclosures, President Obama created the Review Group on Intelligence and Communications Technologies ("President's Review Group").[149] The President's Review Group published a document ("The Report") consisting of 46 policy recommendations to the President that cover a variety of NSA programs, including Section 215 of The USA PATRIOT Act.[150] The recommendations consider both the public's civil liberties and the necessity of homeland security.[151] With respect to Section 215, The Report recommends the NSA end bulk storage of metadata.[152] It suggests a third-party hold the data instead.[153] The President's Review Group cites privacy concerns, similar to those discussed in this Article, as its justification for terminating the metadata program as currently administered by the NSA.[154]

---

[146] Brief for Plaintiffs-Appellants, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013) (No. 14-42), https://www.aclu.org/sites/default/files/assets/corrected_brief_of_plaintiffs-appellants_-_final_stamped_03_07_2014.pdf.

[147] Brief for Defendants-Appellees, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. Dec 27, 2013) (No. 14-42), https://www.aclu.org/sites/default/files/assets/2014-04-10_clapper_govt-opposition-brief.pdf.

[148] Reply Brief for Plaintiffs-Appellants, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. Dec. 27, 2013) (No. 14-42) https://www.aclu.org/sites/default/files/assets/aclu_v._clapper_ca2_reply_brief_final_stamped.pdf.

[149] PRESIDENT'S REVIEW GROUP REPORT, *supra* note 9.

[150] *Id.*

[151] *Id.* at 1.

[152] *Id.* at 17.

[153] *Id.*

[154] *Id.* at 86–88 (citing In Re Production of Tangible Things from Undisclosed Service Provider, Docket Number BR: 08-13 (Mar. 2, 2009)).

D. President Obama's Proposed Changes and Pending Congressional Legislation

In a speech regarding the NSA's programs, President Obama told the American people that the metadata collection program would continue, although not as broadly.[155] However, through a Presidential Directive, President Obama eliminated the third hop.[156] Further, President Obama instructed the Attorney General to develop a new method to match the capabilities of Section 215 without the NSA actually holding the metadata.[157]

While several bills have been proposed to reform Section 215 in the House of Representatives, the USA FREEDOM Act has the most support with 142 co-sponsors.[158] The USA FREEDOM Act was introduced in the House of Representatives on October 29, 2013.[159] USA FREEDOM stands for "Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection, and Online Monitoring" Act.[160] This Act would amend the PATRIOT Act similarly to the LIBERT-E Act.[161] Both bills propose the FBI must include a statement of facts indicating that there are "reasonable grounds to believe that the tangible things sought are relevant and material to an authorized investigation" in order to request metadata records from a phone provider.[162]

On January 9, 2014, this bill was also referred to the subcommittee on Crime, Terrorism, Homeland Security, and

---

[155] President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) (transcript available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence) [hereinafter President Obama's Remarks].

[156] *Id.*

[157] *Obama's Proposal for Ending Section 215*, *supra* note 131.

[158] USA FREEDOM Act, H.R. 3361, 113th Cong. (1st Sess. 2013); Congress, *Summary: H.R. 3361 – USA FREEDOM Act*, CONGRESS.GOV (Oct. 29, 2013), http://beta.congress.gov/bill/113th-congress/house-bill/3361; *see also* LIBERT-E Act, H.R. 2399, 113th Cong. (1st Sess. 2013); Telephone Metadata Reform Act, H.R. 3875, 113th Cong. (2nd Sess. 2014).

[159] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

[160] *Id.*

[161] *Id.* at § 101(a)(1)(B).

[162] *Id.*

Investigations.[163] On May 22, 2014, this bill passed the House of Representatives as amended.[164]

IV. THE STANDARD TO SEARCH METADATA SHOULD BE RAISED TO A PROBABLE CAUSE STANDARD BECAUSE OF VAST PRIVACY CONCERNS

Benjamin Franklin once said, "Those who would give up essential Liberty, to purchase a little temporary safety, deserve neither Liberty nor Safety."[165] However, in the modern world, government surveillance of people at home and abroad is necessary to protect against threats that Mr. Franklin could never have imagined.[166] When does the government cross the line between safety and liberty? The Snowden leaks startled many Americans because of the seeming impossibility that a democratic state could become a surveillance state.[167] Civil liberties groups have called for the elimination of metadata collection—citing egregious civil rights violations—by bringing lawsuits against the NSA and President Obama.[168]

---

[163] *Id.*

[164] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

[165] Benjamin Franklin, *Pennsylvania Assembly: Reply to the Governor, Nov. 11, 1755*, NATIONAL ARCHIVE FOUNDERS ONLINE, http://franklinpapers.org/franklin/framedVolumes.jsp?vol=6&page=238a (last visited July 31, 2014).

[166] In re FBI, No. 13-109, 2013 WL 5307991, at *30–31 (FISA Ct. Aug. 29, 2013) (stating that "telephony metadata" includes comprehensive communications routing information, such as including originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, trunk identifier, telephone calling card numbers, and time and duration of call).

[167] *See supra* note 5 (defining "Orwellian").

[168] *E.g.*, ACLU, *Time to Rein in the Surveillance State*, ACLU.ORG, https://www.aclu.org/time-rein-surveillance-state-0 (last visited Apr. 25, 2014) ("The ACLU has been at the forefront of the struggle to rein in the surveillance superstructure, which strikes at the core of our rights to privacy, free speech, and association."); Electronic Frontier Foundation, *NSA Spying on Americans*, EFF.ORG, https://www.eff.org/nsa-spying ("EFF has been at the forefront of the effort to stop [surveillance of communications] and bring government surveillance programs back within the law and the Constitution.") (last visited Apr. 25, 2014).

Following public backlash regarding metadata collection, all three branches of the Government are taking action. After President Obama spoke to the American people specifically about Section 215 of the USA PATRIOT Act,[169] he issued a Presidential Policy Directive reigning in aspects of the metadata collection program. Additionally, there are roughly 30 different legislative bills before Congress altering the metadata collection program.[170] Two circuit courts have ruled on the opposite sides of the constitutionality of Section 215.[171] Political activist Larry Klayman appealed his case, *Klayman v. Obama*, directly to the Supreme Court on February 3, 2014, citing its "imperative public importance."[172] However, the Supreme Court denied his petition, leaving the constitutionality of Section 215 unresolved.[173] While the exact fate of the metadata collection program remains unknown, the Government's proposed actions merely provide a façade of change.

President Obama's Policy Directive and Congress' attempt at legislation with the USA FREEDOM Act are both superficial attempts at rectifying privacy concerns because the Government does not concede to the necessity of a warrant to search metadata, as required for searches under the Fourth Amendment. Instead, the current reasonable articulable suspicion standard is kept intact in the proposed legislation from both the House of Representatives and President Obama.[174] The Government, through FISC court documents, continually relies on the third-party doctrine in

---

[169] President Obama's Remarks, *supra* note 155.

[170] David Kravets, *Supreme Court passes on NSA bulk phone surveillance case*, ARS TECHNICA (Apr. 7, 2014, 6:46 AM), http://arstechnica.com/tech-policy/2014/04/supreme-court-passes-on-nsa-bulk-phone-surveillance-case/.

[171] Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

[172] 134 S. Ct. 1795 (Apr. 7, 2014).

[173] *Id.*

[174] *H.R. 3361 – USA FREEDOM Act*, *supra* note 158; President Obama's Remarks, *supra* note 155; Presidential Policy Directive/PPD-28, *Signals Intelligence Activities*, THE WHITE HOUSE (Jan. 17, 2014), www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

denying a reasonable expectation of privacy in metadata.[175] However, the third-party doctrine fails to take into account the vast privacy concerns associated with modern technology.

Because so much information about a person's private life can be gleaned from the collection of metadata, the Government should be required to obtain a warrant before searching metadata. As required by the Fourth Amendment, the standard for a warrant is probable cause.[176] Thus, the NSA should be required to make a probable cause determination to perform a "hop" on an American citizen's metadata. This requirement will protect citizens' privacy rights regardless of whether the NSA or the phone companies hold the metadata.

A. The Reasonable Articulable Suspicion Standard should be Updated because It Fails to Take Into Account the Reasonable Expectation of Privacy that should be Associated with Metadata

Although The President's Review Group found Section 215 to be unconstitutional, the metadata program may be a useful tool in the fight against terrorism, as President Obama has argued.[177] For this reason, instead of suggesting an end to the metadata program, the standard for searching metadata during a hop should be changed to require a higher burden of proof showing that the seed being queried is associated with terrorist activity. When FISA was originally enacted, the Government had to show probable cause to believe the target of the electronic surveillance was an agent of a foreign power.[178] This required FISC to obtain a warrant from a neutral and detached magistrate before accessing sensitive data.[179]

However, in the wake of 9/11, the threshold was lowered to require only "specific and articulable facts giving reason to believe

---

[175] *See, e.g.*, In re Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573 at *2–6 (Foreign Intel. Surv. Ct. Aug. 29, 2013).

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

[177] President Obama's Remarks, *supra* note 155.

[178] 50 U.S.C. § 1805.

[179] President's Review Group Report, *supra* note 9, at 88–89.

that the person to whom the records pertain is a foreign power or an agent of a foreign power."[180] This standard was too open-ended and Congress again changed the standard required to search metadata under Section 215 to "a statement of facts showing that there are reasonable grounds to believe that the tangible objects sought are relevant."[181] The standards used in both thresholds (the lowered one of 2001, and the slightly higher one of 2005) rely on the out-of-date third-party doctrine and privacy justifications.

Additionally, the Report points out the ease with which the NSA has abused the metadata program.[182] It cited that "[a]lmost 90 percent of the numbers on the alert list did *not* meet the 'reasonable, articulable suspicion' standard."[183] The NSA should be required to obtain a warrant from FISC before performing any queries because metadata reveals detailed information about a person.

1. Metadata Reveals Highly Personal and Sensitive Information Subject to Fourth Amendment Protection

Since the Snowden revelations, those in charge of intelligence have downplayed the significance of metadata.[184] President Obama assured the American people the content of calls was not being collected.[185] The Chairwoman of the Senate's Committee on Intelligence, Dianne Feinstein, remarked that "this is just

---

[180] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1)).

[181] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[182] President's Review Group Report, *supra* note 9, at 105.

[183] *Id.*

[184] *See, e.g.*, *Transcript: Diane Feinstein, Saxby Chambliss, Explain, Defend NSA Phone Records Program*, WASH. POST (Jun. 6, 2013), http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/06/transcript-dianne-feinstein-saxby-chambliss-explain-defend-nsa-phone-records-program [hereinafter *Senator Feinstein's Remarks*]; President Obama's Remarks, *supra* note 155.

[185] President Obama's Remarks, *supra* note 155.

metadata."[186] Although voice content can be hard to process and difficult to collect on a mass scale, metadata is perfectly suited to computer analysis.[187] Metadata can show the context of a person's life and give an intimate look into one's interests, values, and societal roles.[188] Metadata can also be a rich source for obtaining sensitive information about one's identity, location, and social network.[189] When cross-checked against easily accessed public records, metadata can reveal a person's name, address, credit history, and more.[190] Although the metadata collection program offers powerful tools in the fight against terrorism, it severely implicates personal expectations of privacy.[191]

In an Amici Curiae Brief written in support of a reversal of *ACLU v. Clapper* by the Electronic Frontier Foundation, a small but compelling example is given demonstrating the sensitivities associated with the collection of metadata. If a single telephone call to a bookie is made, it suggests that a person likely made a bet.[192] But an analysis of metadata over time could reveal that the same person has a gambling problem.[193] While aggregating metadata is troubling for an individual, it is even more troubling when connections are made between individuals and larger social trends.[194] Analysis of metadata over time can "map the associations of individuals, revealing friendships, business

---

[186] Senator Feinstein's Remarks, *supra* note 184.

[187] Brian Lam, *Phew, NSA Is Just Collecting Metadata. (You Should Still Worry)*, WIRED.COM (June 19, 2013), http://www.wired.com/2013/06/phew-it-was-just-metadata-not-think-again/.

[188] *Id.*

[189] David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 64 (2013).

[190] Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelations*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/obama-administration-nsa-verizon-records.

[191] Grey, *supra* note 189, at 67.

[192] Brief for ACLU, et al. as Amici Curiae Brief of Experts in Computer and Data Science in Support of Appellants and Reversal, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 14-42) [hereinafter ACLU Amici Curiae Brief].

[193] *Id.* at 11–12.

[194] *Id.* at 12.

relationships, and social and political connections."[195] While this language focuses on the individual, collecting and searching metadata affects the lives of millions of Americans.

Each time the NSA performs a hop, the number of people Section 215 affects expands exponentially. For example, Person X is a suspect, and he made 100 phone calls. The NSA would have access to all 100 of those phone numbers Person X was in contact with. The NSA then has authorization to make a second hop; that is, to take the 100 phone numbers associated with Person X and look at the metadata associated with *each* of those numbers.[196] Further, if the 100 people Person X contacted each also contacted 100 people, the pool of metadata would now include 10,000 total phone numbers (100 people times 100 phone numbers).

A third hop would take the 10,000 phone numbers that were pooled during the second hop, and look at every number that was contacted. If each of those 10,000 people called 100 people, the metadata pool would now consist of 100 phone numbers (first hop) times 100 phone numbers (second hop) times 100 phone numbers (third hop), totaling a pool of one million phone numbers to query. Until President Obama's speech on January 17, 2014, the NSA had authorization to make the *third hop*.[197] FISC formally approved removing the third hop on February 5, 2014, stating its deletion adequately balances privacy and national security interests set forth in President Obama's Presidential Policy Directive.[198]

To illustrate this point with real people, an online blog, Webpolicy.org, performed a short-term study to learn if sensitive and personal inferences could be drawn from metadata.[199]

---

[195] *Id.*

[196] *Id.*

[197] *Id.*; President Obama's Remarks, *supra* note 155 ("Effective immediately, we will only pursue phone calls that are two steps removed from a number associated with a terrorist organization instead of the current three.").

[198] In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01 (FISA Ct. Feb. 5, 2014); Presidential Policy Directive/PPD-28, *supra* note 174.

[199] Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata*, WEBPOLICY.ORG (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ (last visited Apr. 28, 2014).

Beginning in November 2013, WebPolicy.org had participants install the "MetaPhone" application on their Android phones.[200] MetaPhone runs in the background of the user's device and submits device logs and social media information for analysis.[201] While this study is on a relatively small scale (546 participants), WebPolicy.org found that "phone metadata is unambiguously sensitive, even in a small population and over a short time window."[202] In total, the 546 participants contacted 33,688 unique phone numbers.[203] 18 percent of those numbers were identifiable by matching phone numbers against public records, such as Yelp and Google Places directories.[204] Participants had contacted Alcoholics Anonymous, labor unions, divorce lawyers, strip clubs, and sexually transmitted disease clinics.[205]

Additionally, the study indicated a pattern of calls that revealed more sensitive information than individual call records.[206] For example, a participant made phone calls to local neurology groups, a specialty pharmacy, a rare condition management service, and a hotline for a drug used solely to treat multiple sclerosis.[207] An inference can be made, based on this participant's metadata alone, that this participant has a serious medical condition. WebPolicy.org was able to corroborate this participant's medical condition proving that metadata does reveal personal and sensitive content.[208] Another participant had a long telephone call with her sister, then two days later placed a series of calls to Planned Parenthood.[209] She placed another series of calls two weeks later, and a final call a month after.[210] As this study shows, the NSA can gather and use power data with the tools it currently has at its disposal.

---

[200] *Id.*
[201] *Id.*
[202] *Id.*
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *Id.*
[207] *Id.*
[208] *Id.*
[209] *Id.*
[210] *Id.*

To collect and search a person's metadata, the government should have to show probable cause that the person whose records are being searched is associated with international terrorism or clandestine intelligence activities.[211] Gathering the metadata on Person X and everyone whom each of those 100 people contacted is an egregious violation of privacy. Because of the privacy implications and the breadth of information that can be quickly amassed, the NSA should not be allowed to collect metadata without individualized suspicion that Person X is associated with terrorism.

2. The Third-Party Doctrine should be Updated in Light of Modern Technology

The third-party doctrine should be updated to reflect the modern relationship between a person and his cell phone. In *United States v. Jones*, Justice Sotomayor foreshadowed concerns over gathering information through surveillance, noting it could lead to "a too permeating police surveillance."[212] She suggested that it might be "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[213] Much like Justice Brandeis' dissent in *Olmstead v. United States*, Justice Sotomayor's concurrence is at the forefront of the privacy argument in the new age.[214]

The third-party doctrine, as established in *Smith v. Maryland*, states that there is no reasonable expectation of privacy in information voluntarily handed over to a third-party.[215] FISC relies

---

[211] 50 U.S.C. § 1861(a)(1) (using the same language as the statute that the "tangible things sought are relevant . . . against international terrorism or clandestine intelligence activities").

[212] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayer, J., concurring) (internal quotation marks omitted).

[213] *Id.* at 957.

[214] ACLU Amici Curiae Brief, *supra* note 192, at 11 (using Justice Sotomayor's concurrence to make the argument that aggregated metadata generated a comprehensive record of people's habits).

[215] Smith v. Maryland, 442 U.S. 735, 745 (holding there is no reasonable expectation of privacy when a person voluntarily gives their number to a third

on the holding in *Smith* to defend the production of metadata by telephone service providers to the NSA.[216] A person who gets a cell phone voluntarily discloses metadata to his or her cell carrier, a third-party, and his or her expectation of privacy is defeated. However, the facts of *Smith* are vastly different from what the NSA is doing under Section 215.[217] Today's circumstances have become so unlike those of the 1970s that the precedent set in *Smith* becomes completely frustrated. These circumstances include the Government's surveillance capabilities, the modern day relationship users have with their cell phones, and the relationship between the phone companies and the NSA.[218]

In *Klayman*, the Court found four main reasons that the third-party doctrine cannot justify the modern surveillance program under Section 215.[219] First, the pen register installed on Smith's phone was to last a mere 13 days, and it collected data regarding that case only.[220] Thus the information collected was short-term and highly limited.[221] In contrast, the information that the NSA collects is vast and on-going over the course of half a decade.[222] Second, in *Smith*, the police requested the phone company install the pen register on its own equipment to record the numbers dialed.[223] Under the current Secondary Order, telephone companies are required to provide the NSA records "*on a daily basis*."[224] The Government forces the third-parties (the telephone companies) to "create a formalized policy under which the service provider collects information for law enforcement purposes,"

---

party).

[216] In re FBI, No. 13-109, 2013 WL 5307991, at *9 (FISA Ct. Aug. 29, 2013).

[217] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 32.

[218] *Id.*

[219] *Id.* at 32–34.

[220] *Id.*

[221] *Id.*

[222] *Id.* (noting the metadata program could last indefinitely so long as the war on terror persists, which could be forever versus the collection of information in *Smith* was specifically to convict Smith of one crime, to be used in one trial, and then discarded).

[223] *Id.* at 17.

[224] *Id.* at 19 (emphases added) (quoting Secondary Order, *supra* note 107)

circumventing the Fourth Amendment.[225]

Third, the *Smith* Court in the 1970s could not have conceived of the collection of metadata on such an expansive scale.[226] Finally, the scale on which people use their phones is inherently different than it was in the 1970s.[227] Not only is there a significant increase in phone usage (71,958,000 homes with phones in 1979 versus 326,475,248 mobile subscribers in 2012),[228] but the relationship between phone and user is also more personal than ever before.[229] Because of modern and intimate use of phones, information that is gleaned from metadata has changed not only in quantity but also in quality.[230]

Creating a trail of metadata is an unavoidable byproduct of modern life and metadata should not be considered in a vacuum.[231] The ACLU Amici Curiae Brief argued that metadata is generated through the "innumerable and near-continuous digital transactions and interactions" presented by modern life.[232] Financial transactions, medical records, travel records, communications, legal proceedings, biological information, education, health care, and entertainment are personal "digital tracks" every person leaves by simply participating in modern life.[233] Acts such as applying for a loan, renting a DVD, sending or receiving a package, files, or receiving medications through the mail generate metadata.[234] It would be practically impossible for an individual to avoid creating metadata in today's world.[235] A person can no longer assume the risk that their information may be handed over to a third-party because this transaction has now become a daily, if not hourly, occurrence.

Information that was once scattered now reveals a mosaic of a

---

[225] *Id.* at 19.
[226] *Id.*
[227] *See id.* at 20–21.
[228] *Id.* at 20.
[229] *See id.* at 20–21.
[230] *Id.*
[231] ACLU Amici Curiae Brief, *supra* note 192, at 15.
[232] *Id.* at 16.
[233] *Id.*
[234] *Id.* at 16–17.
[235] *Id.* at 18.

person's life.[236] The modern changes in technology render the third-party doctrine outdated and in need of a new jurisprudence that considers an updated look at the expectation of privacy in metadata information.

B. The Actions Proposed by the Government are Ineffective because They Maintain the Lower "Reasonable and Articulable Suspicion" Standard

The Government's proposed legislation is ineffective because it fails to raise the needed threshold to probable cause and continues to diminish citizens' privacy concerns. Representative James Sensenbrenner, Jr., the original author of the USA PATRIOT ACT and lead author on the proposed USA FREEDOM Act, acknowledged that "the NSA was doing some things that were far beyond what the intent of the law should have been . . . ."[237] He criticized Senator Feinstein's proposed legislation, specifically noting that her bill "is a joke" and her view is essentially that "if you like your NSA, you can keep it."[238] What Congress and the President fail to mention, however, is that the problem lies not only with mass collection of metadata, but also in the *way the Government is able to access and search* the metadata. This troubling standard remains unchanged and leaves the door open to a multitude of privacy violations.

President Obama's Policy Directive is superficial because it fails to provide any substantial changes that protect privacy rights. In President Obama's speech to the American people, he proudly claimed to end Section 215 metadata collection "as it currently exists."[239] However, bulk collection is not the biggest problem. The problem is not *where* the metadata is being stored, but *how* the

---

[236] Klayman v. Obama, 957 F. Supp. 2d 1, 36 (referencing the mosaic theory from Maynard, 615 F.3d at 562–63).

[237] Brendan Sasso & Bob Cusack, *Patriot Act author: Feinstein's bill 'a joke'*, THE HILL (Dec. 10, 2013, 6:00 AM), http://thehill.com/homenews/house/192561-feinsteins-nsa-bill-is-a-joke-says-rep-james-sensenbrenner.

[238] *Id.*

[239] President Obama's Remarks, *supra* note 155.

metadata is accessed.

First, President Obama limited the NSA to searching metadata within only two hops of the selection term being used instead of three.[240] Second, the metadata would no longer be collected in bulk by the NSA but would remain with the phone companies.[241] Third, the NSA would obtain the records pursuant to individual orders from FISC.[242] Although these recommendations appear to solve the problem of "dragnet surveillance," they fail to provide any real safety from abuse by the NSA.[243]

The problem with President Obama's Presidential Policy Directive is that it is not binding.[244] Presidential Directives can be amended or withdrawn at any time by the current President.[245] Even if Americans trust President Obama to follow through on the policy directives he proposed, the president in 2016 could reverse those changes with the swipe of a pen.[246] Unless codified in a statute by Congress, any future president, at any time and for any reason, could re-instate the third hop and bring metadata collection back under the purview of the NSA.

Additionally, none of the bills Congress has offered produce any substantial change to Section 215. None of the thirty-plus bills mention raising the standard from reasonable, articulable suspicion to probable cause. Most of the bills proposed, including the flagship USA FREEDOM Act, herald an ending to bulk metadata collection.[247] However, the USA FREEDOM Act barely amends

---

[240] *Obama's Proposal for Ending Section 215*, *supra* note 131.

[241] *Id.*

[242] *Id.*

[243] Electronic Frontier Foundation, *NSA Spying on Americans*, EFF.ORG, https://www.eff.org/nsa-spying (last visited Apr. 14, 2014) ("The US government, with assistance from major telecommunications carriers including AT&T, has engaged in a massive illegal dragnet surveillance of domestic communications and communications records of millions of ordinary Americans since at least 2001.").

[244] Todd F. Gaziano, *The Use and Abuse of Executive Orders and Other Presidential Directives*, THE HERITAGE FOUNDATION (Feb. 21, 2001), http://www.heritage.org/research/reports/2001/02/the-use-and-abuse-of-executive-orders-and-other-presidential-directives.

[245] *Id.*

[246] *Id.*

[247] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

the current standard. Current law requires the government to submit a statement of facts showing reasonable grounds to believe that the tangible things or records sought are relevant to an authorized investigation.[248]

Yet Section 101 of the USA FREEDOM Act would require the Government to show that the tangible things sought are relevant and material to an authorized investigation and that they pertain to (a) a foreign power or an agent of a foreign power, (b) the activities of a suspected agent of a foreign power who is the subject of such an authorized investigation, or (c) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation.[249] This proposed change only narrows what can be considered an "authorized investigation." The NSA would still be able to collect and search metadata based on the lowered standard of reasonable and articulable suspicion.

Unless the standard necessary to collect and search metadata is raised to probable cause and requires the NSA to obtain a search warrant from a neutral and detached magistrate, the same concerns that are currently present could be reinstated even if the proposed actions are implemented. FISC could reinstate dragnet bulk metadata collection under the NSA's direction. FISC previously concluded in 2009 that for two-and-a-half years the NSA had "frequently and systematically violated" the minimization procedures put in place to prevent abuse.[250] FISC Judge Walton also found additional noncompliance issues involving trained analysts querying the metadata without being aware that they were doing so.[251] The FBI could once again issue National Security Letters forcing Verizon and other telecommunication companies to comply with ongoing metadata disclosure. Verizon would have no way to disclose such an order to the public because every National Security Letter contains a gag order forbidding the receiver from

---

[248] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)).

[249] *Summary: H.R. 3361 – USA FREEDOM Act*, *supra* note 158.

[250] President's Review Group Report, *supra* note 9, at 105.

[251] *Id.* at 106.

revealing the Letter's existence.[252] The actions the Government, including President Obama and Congress, are proposing are simply not enough to protect American citizens' privacy rights.

It is unlikely that searching metadata in the fight against terrorism will ever cease.[253] By requiring the standard to be raised to probable cause instead of reasonable and articulable suspicion, Americans will know their privacy is protected under the Fourth Amendment no matter what agency or company is holding their metadata.

CONCLUSION

The metadata information the Government is able to collect, store, and search on a massive scale makes Section 215 a violation of the Fourth Amendment. The Fourth Amendment is clear: to search a constitutionally protected area, one must have probable cause and obtain a warrant from a detached and neutral judge.[254] That is not being done under the metadata program.[255] Although the Government has proposed legislation to modify parts of Section 215, it has failed to change the standard under which the NSA can *search* metadata. Because enormous amounts of information can be gleaned from metadata revealing the intimacies of a person's life, it is time to recognize a right to privacy in metadata. By giving metadata *Katz*-level protection, metadata should be protected under the Fourth Amendment. This would require the NSA to seek a warrant from FISC showing probable cause that the suspect is linked to terrorist activity. Requiring a higher standard for the Government to perform any search of metadata adequately balances the need for privacy in this

---

[252] Electronic Frontier Foundation, *National Security Letters*, EFF.ORG, https://www.eff.org/issues/national-security-letters (last visited Apr. 28, 2014).

[253] David Kravets, *supra* note 170.

[254] *See* Katz v. United States, 389 U.S. 347, 357 (recognizing that the Fourth Amendment imposes a warrant requirement for searches and seizures because warrantless searches are unreasonable per se).

[255] USA PATRIOT Improvement and Reauthorization Act of 2005, 120 Stat. 196 § 106 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)) (Section 215 does not show a requirement for a probable cause determination to be made and a warrant to be issued before searching the metadata).

enormous amount of sensitive information with the need to protect Americans from future terrorist threats.