Fordham Law Review

Volume 82 | Issue 5 Article 15

2014

The Relevance of Relevance: Section 215 of the USA PATRIOT Act and the NSA Metadata Collection Program

Casey J. McGowan
Fordham University School of Law

THE RELEVANCE OF RELEVANCE: SECTION 215 OF THE USA PATRIOT ACT AND THE NSA METADATA COLLECTION PROGRAM

*Casey J. McGowan**

In June 2013, a National Security Agency (NSA) contractor, Edward Snowden, leaked classified documents exposing a number of secret government programs. Among these programs was the "telephony metadata" collection program under which the government collects records from phone companies containing call record data for nearly every American. News of this program created considerable controversy and led to a wave of litigation contesting the validity of the program.

The legality of the metadata collection program has been challenged on both constitutional and statutory grounds. The program derives its authority from Section 215 of the USA PATRIOT Act, codified as 50 U.S.C. § 1861. The statute requires that there be reasonable grounds to believe the data collected is "relevant to an authorized investigation." The government deems all these records "relevant" based on the fact that they are used to find patterns and connections in preventing terrorist activity. Critics of the program, however, assert that billions of records cannot possibly be relevant when a negligible portion of those records are actually linked to terrorist activity. This Note examines the conflicting interpretations of "relevant," and concludes that while the current state of the law permits bulk data collection, the power of the NSA to collect records on such a large scale must be reined in.

TABLE OF CONTENTS

* J.D. Candidate, 2015, Fordham University School of Law; B.A., 2012, Marist College. Special thanks to Professor Ian Weinstein for his enthusiasm and insight throughout this process and to Larry Abraham for suggesting this topic. I am also grateful to my family for their never-ending support and encouragement.

INTRODUCTION

In June 2013, Edward Snowden, a National Security Agency (NSA) contractor, leaked information to the press concerning several secret government programs.[1] Snowden's files revealed that the U.S. government had ordered Verizon to release phone record data for millions of customers.[2] This order was part of a larger "telephony metadata"[3]

1. Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *2 (D.D.C. Dec. 16, 2013).
2. *See id.*
3. Metadata refers to the business records information acquired through programs such as the NSA surveillance programs that Snowden's leaked documents refer to. Metadata

collection program[4] for all domestic phone calls on the network.[5] Snowden has since been charged with espionage and theft of government property.[6] He currently resides in Russia, where he was granted temporary political asylum, although he could seek permanent asylum in another country.[7] Snowden's status has caused significant tension between the United States and Russia, and he has become an extremely divisive figure.[8] Some view him as a champion of individual rights, while others believe his actions were unjustified and have labeled him a traitor.[9]

The leaks have put the U.S. government in the tenuous position of facing both public and legal scrutiny for this and similar programs. The government has acknowledged the existence of the programs and confirmed the validity of the leaked information.[10] The metadata collection program is authorized by the Foreign Intelligence Surveillance Court (FISC) under the Foreign Intelligence Surveillance Act (FISA), which was enacted as section 215 of the USA PATRIOT Act (Patriot Act).[11] The metadata collection program began in 2006, and as of October 2013, has been renewed thirty-five times.[12] In response to the public and media outcry, the White House issued an administration white paper outlining the legal basis

includes time, date, and routing information of telephone calls. Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Steven's Fourth Amendment?*, 74 FORDHAM L. REV. 1731, 1734 n.18 (2006).

4. The program has been referred to by a number of names including the "bulk data collection program," the "bulk telephony metadata collection program," the "telephony records program," and the "metadata records program." This Note refers to it as the metadata collection program.

5. Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari at 3, *In re* Elec. Privacy Info. Ctr., 134 S. Ct. 638 (2013) (No. 13-58), 2013 WL 3484365, at *3 [hereinafter EPIC Petition]. The order required Verizon to produce call detail records "(i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." *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., No. BR 13-80, slip op. at 1–2 (FISA Ct. Apr. 25, 2013), *available at* http://epic.org/privacy/nsa/Section-215-Order-to-Verizon.pdf [hereinafter FISC Order].

6. Pete Williams & Becky Bratu, *US Charges NSA Leaker Snowden with Espionage*, NBC NEWS (June 21, 2013, 5:52 PM), http://usnews.nbcnews.com/_news/2013/06/21/19079389-us-charges-nsa-leaker-snowden-with-espionage?lite.

7. Steven Lee Myers & Andrew E. Kramer, *Defiant Russia Grants Snowden Year's Asylum*, N.Y. TIMES, Aug. 2, 2013, at A1.

8. Stephen Moore, Note, *Cyber Attacks and the Beginnings of an International Cyber Treaty*, 39 N.C. J. INT'L L. & COM. REG. 223, 252 (2013).

9. *See* Alexander E. Blanchard, *A False Choice: Prior Restraint and Subsequent Punishment in a Wikileaks World*, 24 U. FLA. J.L. & PUB. POL'Y 5, 45 (2013).

10. *See* Complaint for Declaratory and Injunctive Relief at 1, ACLU v. Clapper, 959 F. Supp. 2d 724 (2013) (13 Civ. 3994(WHP)), 2013 WL 2492595.

11. U.S. DEP'T OF JUSTICE, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 1 (2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf.

12. Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *8 (D.D.C. Dec. 16, 2013).

for the program,[13] which has been rebuked by both privacy interest groups and scholars.[14]

In addition to public scrutiny, the government faces legal action from a number of groups. One of the predominant pending cases involves the ACLU suing a group of high-ranking government officials involved in matters of national security.[15] Private individuals brought a similar suit in the D.C. District Court.[16] Additionally, the Electronic Privacy Information Center (EPIC) petitioned the U.S. Supreme Court for a writ of mandamus to vacate the Verizon order.[17] One main contention, voiced by the public at large, as well as scholars and privacy interest groups, is that common sense dictates that collecting billions of records precludes the possibility that all—or even most—of those records are "relevant" to an investigation, as required by section 215.[18] This Note addresses the various arguments concerning relevance and determines whether the metadata program comports with the language of its statutory authorization.

The records collection program is extremely expansive, as evidenced by the leaked documentation supporting the allegations, impacting millions of Americans whose records are being tracked. Given the far-reaching effects of the metadata collection program, the current litigation is more pertinent to everyday privacy rights and civil liberties than similar attempts in the past. The direction that the courts deciding this issue take in the current litigation will likely impact Fourth Amendment rights and basic privacy rights in the United States for years to come.

Part I of this Note provides background information about the origins of the metadata collection program and its purported legal basis. This includes the First and Fourth Amendments of the U.S. Constitution and prior judicial interpretations of these amendments, as well as the enactment of the Patriot Act and its later amendments. Part II explains the conflict between the federal government and various privacy interest groups in determining how the term "relevant" should be understood and whether the program is legal.

---

13. *See id.*

14. *See, e.g.*, Orin Kerr, *The Problem with the Administration "White Paper" on the Telephony Metadata Program*, VOLOKH CONSPIRACY (Aug. 12, 2013, 2:34 PM), http://www.volokh.com/2013/08/12/problem-withthe-administration-white-paper-on-the-telephony-metadata-program/. In addition to the academic debate surrounding the program, it has become a highly litigated issue with a number of interested parties submitting amicus briefs opposing metadata collection. *See, e.g.*, Brief of *Amicus Curiae* Cato Institute in Support of Petitioner, *In re* Elec. Privacy Info. Ctr., 134 S. Ct. 638 (2013) (No. 13-58), *available at* http://epic.org/privacy/nsa/in-re-epic/Cato-Amicus.pdf [hereinafter Cato Brief]; Brief of *Amicus Curiae* Professors of Information Privacy and Surveillance Law in Support of Petitioner, *In re Elec. Privacy Info. Ctr.*, 134 S. Ct. 638 (No. 13-58), *available at* http://www.law.indiana.edu/front/etc/section-215-amicus-8.pdf [hereinafter Privacy Professors' Brief]; *see also infra* Parts I.E, II.B.

15. *See* Complaint for Declaratory and Injunctive Relief, *supra* note 10.

16. *See infra* Part I.E.2.

17. Timothy B. Lee, *Could the Supreme Court Stop the NSA?*, WASH. POST (July 9, 2013, 9:15 AM), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/09/nsa-litigation-could-go-straight-to-the-supreme-court/.

18. *See infra* Part II.B.

Finally, Part III argues that while the current state of the law weighs in favor of the metadata collection program, the court should rein in the NSA's power to collect private information without probable cause in light of technological developments and privacy concerns.

I. CONSTITUTIONAL RIGHTS, WARRANTLESS SEARCHES, AND STATUTORY AUTHORIZATIONS: HOW MASS DATA COLLECTION BECAME AN INVESTIGATIVE NORM

Part I discusses the evolution of Fourth Amendment protections in regard to technological advances, as well as the history of section 215 of the Patriot Act.[19] Part I.A explores constitutional issues surrounding the metadata collection program. Part I.B discusses the statutory authorization for the program—section 215 of the Patriot Act—and the history of that Act. Part I.C surveys the metadata collection program, including how the NSA claims to use the information and what procedural safeguards exist. Part I.D introduces past cases challenging similar NSA surveillance programs and their relation to the current telephony data collection program. Part I.E provides the framework for the current litigation, and Part I.F addresses the issue of standing in those cases.

A. The Constitutional Framework for Mass Data Collection

The metadata collection program implicates both First and Fourth Amendment concerns. Although this type of surveillance has not been squarely addressed by the Supreme Court, past search and seizure jurisprudence is especially relevant to understanding the legality of the program and is discussed in Part I.A.1. Part I.A.2 briefly sets forth the relevant First Amendment issues.

1. Defining a "Search": Constitutional Limits on Warrants and the Scope of the Fourth Amendment

The metadata collection program involves the collection of data without a warrant, raising significant Fourth Amendment concerns. The Fourth Amendment states, in relevant part, that people have the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[20] In drafting the Amendment, the Constitution's Framers sought to have the boundaries of a search narrowly defined before it occurs.[21] The use of warrants as a check on the system helps eliminate the potential for abuse of the power to search, even when the investigating officer has good intentions.[22]

---

19. The Patriot Act is the common name for 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, 115 Stat. 272.

20. U.S. CONST. amend. IV.

21. Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 532 (2006).

22. *Id.*

The Fourth Amendment has been understood to mean that searches for evidence of a crime, and seizures of such evidence, are presumptively unreasonable when no warrant is obtained, unless the search falls into one of the few recognized exceptions to the warrant requirement.[23] What is considered a "search" for the purposes of the Fourth Amendment has been a source of debate and controversy, leading to the Supreme Court's repeated consideration of the issue. *Katz v. United States*[24] set forth the test for when government activity amounts to a search. The Court applied that standard in *Smith v. Maryland*[25] and determined that the Fourth Amendment no longer protects information provided to a third party. More recently, in *United States v. Jones*,[26] Justices Sotomayor and Alito recognized, in concurring opinions, that it may be time to reevaluate the third-party doctrine laid out in *Smith*.

a. Katz *and the Reasonable Expectation Test*

In *Katz v. United States*, the Court held that a "search" can occur even without physical intrusion into a "constitutionally protected area."[27] In *Katz*, FBI agents wiretapped a public phone booth where a suspected gambler, Charles Katz, had conversations about his wagers.[28] Katz argued that his privacy was violated by such a "search" in contravention of the Fourth Amendment.[29] The Court agreed, holding that Katz had an expectation of privacy in his telephone conversations and that the application of the Fourth Amendment depends on whether the person claiming its protection has a legitimate expectation of privacy that has been invaded by the government.[30] In his concurrence, Justice Harlan delineated a two-question inquiry for determining whether a search has occurred: (1) whether the individual "exhibited an actual (subjective) expectation of privacy"[31] and (2) whether the subjective expectation of privacy is "one that

23. STEPHEN A. SALTZBURG & DANIEL J. CAPRA, AMERICAN CRIMINAL PROCEDURE: INVESTIGATIVE 32 (9th ed. 2010). Courts have recognized a number of exceptions to the warrant requirement over time. Searches pursuant to one of these categories are exempt from the warrant requirement and evidence found during that search is admissible. For example, the Court has recognized an exigent circumstances exception, which permits officers to conduct a search without a warrant where immediate action is necessary to prevent the loss of evidence or to protect the safety of the public or police officers. *Id.* at 361. Additionally, in *Coolidge v. New Hampshire*, the Court stated that officers who have a right to be in a particular place may seize evidence in plain view if they have probable cause to believe it is subject to seizure. *See* Coolidge v. New Hampshire, 403 U.S. 443, 466 (1971). This is by no means an exhaustive discussion, as there are a number of other recognized exceptions by which a search may be found lawful, even without a valid warrant.

24. 389 U.S. 347 (1967).

25. 442 U.S. 735 (1979).

26. 132 S. Ct. 945 (2012).

27. *Katz*, 389 U.S. at 350.

28. *Id.* at 348.

29. *Id.* at 349.

30. *See id.* at 353, 359.

31. *Id.* at 361.

society is prepared to recognize as 'reasonable.'"[32] This analysis was then applied in subsequent cases involving privacy rights in technology.[33]

The Court noted that, historically, searches only occurred upon physical penetration,[34] and that without an actual trespass, the Fourth Amendment was not violated.[35] However, *Katz* and subsequent cases moved away from this interpretation and took a more expansive view of what constitutes a search.[36]

b. Eroding Fourth Amendment Protections: Applications of the Katz *Principle*

Since *Katz*, the reasonable expectation test has been applied to modern investigative techniques. In recent cases, courts have frequently held that an individual lacked an expectation of privacy, and thus the investigation was not a "search" subject to Fourth Amendment protections.[37]

i. *Smith v. Maryland*: The Third-Party Doctrine

In *Smith v. Maryland*, the Court addressed the issue of whether a pen register[38] is a "search" within the meaning of the Fourth Amendment, thus requiring a warrant.[39] Petitioner Michael Lee Smith was convicted of robbing Patricia McDonough's home and making threatening phone calls to the residence afterwards.[40] Smith was suspected as the robber after police traced the license plate number of a suspicious vehicle seen outside the home back to him.[41] The day after obtaining the registration information, police directed Smith's telephone company to install a pen register on his number without obtaining a warrant.[42] The register revealed that Smith's

32. *Id.*
33. *See infra* note 37; *see also infra* Part I.A.1.b.
34. *Katz*, 389 U.S. at 352.
35. *See* Olmstead v. United States, 277 U.S. 438, 466 (1928) (stating that without a physical invasion into a defendant's house or "curtilage," there is no search or seizure within the protection of the Fourth Amendment); *see also* Goldman v. United States, 316 U.S. 129, 134–36 (1942) (holding that because the trespass did not materially aid in the collection of evidence, the Fourth Amendment was not violated).
36. For a full discussion of the *Katz* principle, cases encouraging a more flexible understanding of the Fourth Amendment, and the application of *Katz* to evolving technologies, see Kevin Emas & Tamara Pallas, United States v. Jones*: Does* Katz *Still Have Nine Lives?*, 24 ST. THOMAS L. REV. 116, 125–39 (2012).
37. *See, e.g.*, California v. Ciraolo, 476 U.S. 207 (1986) (stating that despite an individual's attempts to restrict some views of his activities (i.e., from ground level), there is no expectation of privacy against aerial surveillance from 1,000 feet because it is public airspace); Oliver v. United States, 466 U.S. 170 (1984) (affirming that individuals do not have a reasonable expectation of privacy in open fields); United States v. White, 890 F.2d 1012 (8th Cir. 1989) (finding that there is no reasonable expectation of privacy in a public restroom stall).
38. A pen register is a device that records the numbers called by the telephone to which it is attached. SALTZBURG & CAPRA, *supra* note 23, at 50.
39. Smith v. Maryland, 442 U.S. 735, 737–38 (1979).
40. *Id.* at 737.
41. *Id.*
42. *Id.*

number had called the McDonough residence, which the police then used to obtain a search warrant for his home.[43] During the search, a phonebook was found open to the page listing the McDonough's number, and Mrs. McDonough later identified Smith in a six-man lineup.[44] Smith sought to suppress all evidence derived from the pen register since the police had failed to obtain a warrant prior to its installation.[45]

Applying *Katz*, the Court acknowledged that a search can occur even without a physical invasion into a "constitutionally protected area."[46] Citing Justice Harlan's concurrence in *Katz*, the Court divided the issue into two discrete questions: (1) whether the individual had a subjective expectation of privacy and (2) whether that expectation is one that society views as reasonable.[47] Smith had no claim that his property was invaded, because the register was installed at the telephone company's office. He argued instead that despite the lack of a trespass, his expectation of privacy was infringed upon.[48] The Court, however, distinguished the communications in *Katz* from those in *Smith* based on the fact that a pen register does not collect the contents of the call itself, only information about the call.[49]

The Court stated, first, that people cannot have an expectation of privacy in this type of data since they must realize this information is conveyed to telephone companies and retained for billing purposes, among other reasons.[50] The Court further noted that even if Smith had a subjective expectation of privacy, it was not objectively reasonable, as "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities, even if the information is revealed on the assumption that . . . the confidence placed in the third party will not be betrayed."[51] Because Smith voluntarily conveyed the information to a third party, he assumed the risk that the company would reveal the information to police,[52] and therefore the search did not require a warrant.[53] This approach, known as the third-party doctrine, holds that information conveyed to a third party is susceptible to exposure to law enforcement without the speaker's consent.[54]

Justice Stewart, in dissent, argued that numbers dialed from a private phone fall under the same constitutional protection as private conversations,

43. *Id.*
44. *Id.*
45. *Id.*
46. *Id.* at 739.
47. *Id.* at 740.
48. *Id.* at 741.
49. *Id.*
50. *Id.* at 742–43.
51. *Id.* at 744 (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).
52. *Id.*
53. *Id.* at 745–46.
54. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

and that Smith had a reasonable expectation of privacy.[55] In a separate dissent, Justice Marshall argued that implicit in the notion of assumption of risk is a sense of choice, and that in older consensual surveillance cases, the defendant had some discretion in determining who could access his communications.[56] Justice Marshall argued that with the advent of technology and its role in everyday life, the majority promoted the rule that "unless a person is willing to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[57]

ii. *United States v. Jones*: Modernizing the Fourth Amendment

In a more recent test of Fourth Amendment limits, the Court applied the *Katz* test in *United States v. Jones*.[58] There, the Court addressed the issue of whether attaching a GPS tracking device to a vehicle and using it to monitor the vehicle's movements constitutes a search under the Fourth Amendment.[59] Law enforcement applied for a warrant authorizing the use of a GPS tracking device on the car of a suspected drug trafficker's wife.[60] The warrant was issued with the requirement that the device be installed within ten days.[61] Agents waited until the eleventh day to install the GPS device and then proceeded to track the car's movements over the course of the next twenty-eight days.[62] The drug trafficker moved to suppress the GPS evidence, but the district court only partially granted the motion, ruling that the data obtained while the vehicle was in the private parking garage where they first installed the device was inadmissible.[63] The trafficker was convicted of drug-related offenses, but on appeal, the D.C. Circuit reversed, holding that the evidence was obtained by warrantless use of the GPS, thus violating the Fourth Amendment.[64]

The Supreme Court held that a "search" had occurred and that the trafficker's Fourth Amendment rights were therefore violated.[65] Justice Scalia reasoned that *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.'"[66] The Court stated that *Katz* did not

55. *Smith*, 442 U.S. at 747.
56. *Id.* at 750.
57. *Id.*; *see also* Schulhofer, *supra* note 21, at 546 (discussing how, in modern life, it is not truly "voluntary" to turn over personal information, as such exposure is inevitable by individuals availing themselves of technological conveniences and societal norms).
58. 132 S. Ct. 945 (2012).
59. *Id.* at 948.
60. *Id.*
61. *Id.*
62. *Id.*
63. *Id.* The data tracking his movements on public roadways, however, was admissible as there is no expectation of privacy in that information. *Id.*
64. *Id.* at 949.
65. *Id.*
66. *Id.* at 951 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983)).

narrow the Fourth Amendment's scope, and that the reasonable expectation of privacy test was an addition to the common law trespass understanding of a search.[67]

The Court, in *Jones*, acknowledged the existence of related issues and addressed the difficulty inherent in deciding those issues. Questions of whether the crime involved affects the scope of a search or whether visual surveillance through electronic means, without any trespass, constitutes a search remain unanswered.[68] Justice Sotomayor, in a concurring opinion, expressed concern over the fact that technology now makes physical intrusion unnecessary in most cases.[69] She stated, "More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," because in the growing age of digital technology, people are routinely required to provide information about themselves in the course of carrying out their daily activities.[70] She urged that the Fourth Amendment protections may only be applied if the Court's jurisprudence "ceases to treat secrecy as a prerequisite for privacy," but acknowledged that those questions need not be resolved in *Jones* because of the physical intrusion into his car.[71]

Justice Alito stressed that technology can change the expectations of a reasonable person:

> Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. . . .
>
> On the other hand, concern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions.[72]

Although there is no simple solution for what test to use in determining whether Fourth Amendment protections apply, the Court has begun to acknowledge that there are many unresolved issues in this body of law. This decision may very well be the beginning of a paradigm shift in Fourth Amendment jurisprudence.[73]

---

67. *Id.* at 951–52.
68. *Id.* at 953–54.
69. *Id.* at 955; *see also* Jeremy H. Rothstein, Note, *Track Me Maybe: The Fourth Amendment and the Use of Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 502 (2012).
70. *Jones*, 132 S. Ct. at 957.
71. *Id.*
72. *Id.* at 962.
73. Emas & Pallas, *supra* note 36, at 165, 167.

2. Free Speech and the First Amendment

The metadata collection program also raises First Amendment concerns. The First Amendment protects the right to free speech,[74] and critics of the program have asserted that it infringes on protected speech.[75] This particular aspect of the metadata collection program is currently being litigated by the Electronic Frontier Foundation in *First Unitarian Church of Los Angeles v. NSA*.[76]

B. Statutory Authorization for the Program: Patriot Act Section 215

The business records provision of FISA, enacted as section 215 of the Patriot Act, authorizes the metadata collection program.[77] Although FISA is over thirty years old, its application and powers expanded greatly after the September 11, 2001, terrorist attacks.[78]

1. History of the Foreign Intelligence Surveillance Act

FISA was first enacted in 1978 and governs electronic surveillance for foreign intelligence purposes.[79] Although the Federal Rules of Criminal Procedure also govern searches and electronic surveillance, "the secret and less protective rules and procedures of FISA may be employed"[80] when matters of national security are involved and the aim is to collect foreign intelligence. The underlying rationale holds that threats of terrorism are particularly serious, and therefore "privacy intrusions are limited to the collection of information for foreign intelligence purposes."[81]

---

74. U.S. CONST. amend. I.

75. While this Note focuses on the search aspect of the metadata collection program, the concerns about First Amendment free speech protections are an important aspect of the debate. For a discussion of First Amendment rights in cyberlaw, see Anupam Chander & Uyên Lê, *The Free Speech Foundations of Cyberlaw* (U.C. Davis Legal Studies, Working Paper No. 351, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2320124.

76. The First Amendment issues raised by this litigation are beyond the scope of this Note. However, for an overview of this case and the First Amendment concerns raised by the metadata collection program, see *First Unitarian Church of Los Angeles v. NSA*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/cases/first-unitarian-church-los-angeles-v-nsa (last visited Mar. 25, 2014). Critics contend that even though the actual content of the calls is not obtained, the NSA is able to piece together enough information that the program violates First Amendment protections. For example, in 2006, then Senator Joe Biden told CBS that the content of calls is not necessary to know about that person's life, and that based solely on what calls an individual makes, it is possible to get a pattern of that person's life that is "very, very intrusive." *The Early Show* (CBS television broadcast May 12, 2006), *available at* https://www.aclu.org/blog/national-security/flashback-biden-agrees-access-metadata-very-very-intrusive-video.

77. U.S. DEP'T OF JUSTICE, *supra* note 11, at 1.

78. *See infra* notes 110–12 and accompanying text.

79. William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, 1148 (2003).

80. *Id.*

81. *Id.* at 1148–49.

FISA imposes less judicial control over the scope of surveillance than other statutory regimes and does not always require meeting the high standard of probable cause before surveillance can commence.[82] FISA has been construed to satisfy the reasonableness requirement of the Fourth Amendment, and therefore compliance with these procedures and criteria has been held as an adequate substitute for a warrant.[83] The surveillance authorized by FISA, however, is not intended for law enforcement purposes, as there is a distinction between foreign intelligence and law enforcement.[84] There is often a suspicion of criminal activity when surveillance of U.S. citizens is involved, but law enforcement was never the main purpose of FISA.[85]

2. Establishing the Foreign Intelligence Surveillance Court

The FISC was established by 50 U.S.C. § 1803 and consists of eleven district court judges from at least seven of the federal circuits, all of whom must reside within twenty miles of the District of Columbia.[86] FISC judges are publicly designated by the chief justice of the United States.[87] They have the power to "hear applications for and grant orders approving electronic surveillance anywhere within the United States," but may not hear an application that was previously denied by another FISC judge.[88]

In addition to the FISC, the Foreign Intelligence Surveillance Court of Review (FISCR) has been described as "the nation's most secret appellate court."[89] This court meets on extremely rare occasions, convening for the first time in its then twenty-four year history in 2002.[90] The FISCR consists of a three-judge panel and considers appeals from FISC decisions.[91] These three judges are also designated by the chief justice of the United States and must be federal district court or appellate court judges.[92] This panel may review any denial of an application made to the FISC.[93] Judges on both the FISC and the FISCR serve a maximum of seven years and are not eligible for redesignation once that period has expired.[94]

---

82. Schulhofer, *supra* note 21, at 533.

83. Banks, *supra* note 79, at 1158; *see, e.g.*, United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987); United States v. Duggan, 743 F.2d 59, 73–74 (2d Cir. 1984). The requirements of FISA have been relaxed since these decisions, and obtaining foreign intelligence still satisfies the Fourth Amendment requirements, even where it is a significant purpose of surveillance, rather than the primary purpose. *See* United States v. Duka, 671 F.3d 329, 337, 341–45 (3d Cir. 2011).

84. *See* Banks, *supra* note 79, at 1160.

85. *Id.*

86. 50 U.S.C. § 1803(a) (2006).

87. *Id.*

88. *Id.*

89. *See* Banks, *supra* note 79, at 1171.

90. *Id.*

91. *Id.*

92. 50 U.S.C. § 1803(b).

93. *Id.*

94. *Id.* § 1803(d).

3. FISC Orders and the Requirement of Relevance

Under FISA, the government can submit applications to the FISC requesting that they order the production of certain records. Recipients of a FISC subpoena for records may challenge that order.[95] The subpoena may be quashed if the challenging party can show that the information sought is privileged or is "not relevant to a legitimate inquiry."[96] The challenging party must petition the FISC, at which time a FISC judge is assigned to review the petition for frivolity.[97] If the petition is not frivolous, it is considered, and may be granted only if "the judge finds that [the] order does not meet the requirements" of 50 U.S.C. § 1861[98] or that it is "otherwise unlawful."[99] The problem with this system, however, is that only the recipient of the order—no other individual—has a right of judicial review before the FISC.[100] The party who receives a subpoena is generally not the party whose privacy interests are at stake, thus providing them with little incentive to challenge the order.[101]

Prior to September 11, FISA was a fairly unknown statute, particularly among the general public.[102] From 1979 through 2000, the FISC received an average of approximately 600 warrant applications per year, but never rejected an application.[103] From 2001 through 2012, however, that number increased drastically, as the FISC received an average of over 1,700 applications, rejecting only eleven.[104] This was due, in large part, to the amendment of sections 215 and 505 of the Patriot Act, which reduced the threshold requirements for intelligence and records gathering.[105]

In 2012, the most recent year for which statistics are available, the government made 1,856 applications to the FISC.[106] Of those, 1,789 were requests to conduct electronic surveillance.[107] All of the applications were approved by the FISC with the exception of one, which was later withdrawn

95. Schulhofer, *supra* note 21, at 545.
96. *Id.*
97. 50 U.S.C § 1861(f)(2)(A)(i)–(ii).
98. For a full discussion of 50 U.S.C § 1861 and the requirements set forth in the business records provision of FISA, see *infra* Part I.B.4.
99. 50 U.S.C. § 1861(f)(2)(B).
100. *See id.* § 1861(f)(2)(A)(i).
101. Schulhofer, *supra* note 21, at 545. Schulhofer suggests that investigators should be required to obtain warrants based on probable cause in order to align more closely with the protections afforded by the Fourth Amendment. *Id.* at 545–46.
102. *Id.* at 534–35.
103. *Foreign Intelligence Surveillance Act Court Orders 1979–2012*, EPIC.ORG, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Mar. 25, 2014).
104. *Id.*
105. Schulhofer, *supra* note 21, at 549. The reduced requirements and the extension of FISA to a broader range of information provides investigators with "quick, relatively unsupervised access to highly personal and politically sensitive records." *Id.* at 548–50.
106. Letter from Peter J. Kadzik, Principal Deputy Attorney General, to Harry Reid, Senate Majority Leader 1 (Apr. 30, 2013), *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf.
107. *Id.*

by the government.[108] Two hundred and twelve of those applications were for business records under 50 U.S.C. § 1861, all of which were approved in their entirety.[109]

4. FISA After 9/11: 50 U.S.C. § 1861, Statutory Authority for the Metadata Collection Program

The metadata collection program derives its legal authority from section 215 of the Patriot Act,[110] which amended parts of FISA.[111] The Patriot Act was passed within a few weeks of 9/11, after limited debates, in an effort to give the White House administration greater authority and power in their efforts to counteract terrorism.[112] The statute allows the director of the FBI or his designee to "make an application for an order requiring the production of any tangible things" in order to collect information concerning foreign intelligence.[113] It also stipulates that any investigation concerning U.S. persons must not be conducted solely on the basis of activities that are protected under the First Amendment.[114] Investigations must be conducted in accordance with Executive Order 12,333, which provides guidance for U.S. Intelligence Activities.[115]

The application must contain a statement of facts showing that there are "reasonable grounds" to suspect that the items sought are "relevant to an authorized investigation."[116] It goes on to provide three examples of things that are presumptively relevant to the investigation:

> [T]hey pertain to—(i) a foreign power or an agent of a foreign power; (ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or (iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation . . . .[117]

While this is not an exhaustive list of what may be considered relevant, it does provide a sense of what the legislature had in mind in enacting the statute.

The statute further provides for the procedures to be followed upon judicial approval, and describes what the order must contain.[118] It also limits whom recipients of an order may disclose information to[119] and provides that anyone who turns over the tangible things designated by the

---

108. *Id.*
109. *Id.* at 2.
110. *See supra* note 11 and accompanying text.
111. Banks, *supra* note 79, at 1166.
112. *Id.*
113. 50 U.S.C. § 1861(a)(1) (2006).
114. *Id.* § 1861(a)(2)(B).
115. Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *amended by* Exec. Order No. 13,470, 3 C.F.R. 218, 227 (2008), *reprinted as amended in* 50 U.S.C. § 401 app. at 934–43 (Supp. V 2011).
116. 50 U.S.C. § 1861(b)(2)(A).
117. *Id.*
118. *Id.* § 1861(c).
119. *Id.* § 1861(d).

order in good faith will not be liable for such production.[120] Subsection f permits recipients of an order to file for judicial review of that order in accordance with 50 U.S.C. § 1803(e)(1).[121] It also permits a recipient to challenge the nondisclosure order one year after the issuance of the original order and outlines the procedures for how such a review is to be conducted.[122] Finally, the statute requires the attorney general to adopt minimization procedures[123] to govern the retention of information received pursuant to orders authorized by this title.[124] Any "tangible things" collected must be used in accordance with these minimization procedures.[125]

Although the title (50 U.S.C. § 1861) is lengthy and involved, there are three essential legal elements concerning the metadata collection program: (1) the collection is part of an authorized investigation, (2) the records obtained are "tangible things," and (3) the data collected is relevant to that investigation.[126] This Note addresses whether the metadata collection program meets these requirements, focusing on the relevancy standard as applied to mass data collection.

C. The Telephony Metadata Collection Program

The metadata collection program is a complicated and secretive endeavor, but since the initial Snowden leaks, information has slowly become available, resulting in a rapidly developing understanding of the program. Part I.C.1 discusses the purpose of the program. Part I.C.2 provides an overview of how the collected data is used, and Part I.C.3 considers past compliance problems where program guidelines were not followed properly.

1. Purpose of the Program

Beginning in 2006, the federal government implemented a metadata collection program for the purpose of "combating international terrorism and preventing potentially catastrophic terrorist attacks on [the United States]" by "identifying terrorist operatives and networks" through the examination of terrorist communications.[127] The metadata collection program is designed to give the NSA the ability to identify terrorist threats

120. *Id.* § 1861(e).
121. *Id.* § 1861(f)(2)(A)(i); *see also supra* Part I.B.3.
122. *See* 50 U.S.C. § 1861(f)(2)(A)(i)–(D).
123. Minimization procedures refers to the specific guidelines that minimize the retention, and prevent the dissemination, of nonpublic information. They do, however, allow information to be disclosed in specific law enforcement and foreign intelligence scenarios. *See id.* § 1861(g)(2).
124. *Id.* § 1861(g)(1).
125. *Id.* § 1861(h).
126. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 6–16. The white paper also discusses the fact that although the orders are prospective in nature, they still comply with § 1861. *Id.* at 16. This however, has not been a highly contested issue and, therefore, is not relevant to this Note.
127. *Id.* at 1–2.

within the country.[128] The term "metadata" is used to refer to call data that does not include the contents of the calls.[129] By following connections and patterns in phone records, NSA analysts seek to find links in the structure of terrorist organizations.[130]

2. How the Data Is Analyzed

The program involves collecting phone records directly from service providers,[131] pursuant to orders from the FISC.[132] The records include both calls made entirely within the United States, as well as those between a U.S. number and a number abroad.[133] Initially, there was much speculation about what "call detail records" referred to,[134] but in August 2013, the White House acknowledged that the data includes "the numbers dialed, the length and time of the calls and other similar dialing, routing, addressing, or signaling information."[135]

Once the data is collected, it is stored in secure databases by the NSA.[136] The records are only supposed to be accessed for counterterrorism purposes,[137] and the data may only be queried upon a finding of reasonable articulable suspicion (RAS)[138] that the information is associated with one or more specified foreign terrorist organizations, the determination of which must be made by one of twenty-two authorized persons at the NSA.[139] This number is known as the "seed" identifier.[140] After an analyst is approved to conduct the query, the inquiry is limited to records within three "hops" of the identifier, meaning that the results of the search show the records for the number that is suspected to be in contact with a terrorist organization (first hop), the numbers in contact with that first hop (second hop), and the numbers in contact with the second hop (third hop).[141] This is designed to

128. *Id.* at 2.
129. *Id.* at 2.
130. *Id.* at 2–3.
131. Verizon, Sprint, and AT&T have all been confirmed as recipients of the FISC orders. Verizon has 98.9 million wireless customers and 22.2 million landline customers, Sprint has a total of 55 million customers, and AT&T has 107.3 million wireless customers, in addition to its 31.2 million landline customers. Siobhan Gorman, Evan Perez & Janet Hook, *U.S. Collects Vast Data Trove*, WALL ST. J., June 7, 2013, at A1.
132. U.S. DEP'T OF JUSTICE, *supra* note 11, at 3.
133. FISC Order, *supra* note 5, at 2.
134. *See* EPIC Petition, *supra* note 5, at 9.
135. U.S. DEP'T OF JUSTICE, *supra* note 11, at 20.
136. David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RES. PAPER SERIES 10 (Sept. 29, 2013), http://www.lawfareblog.com/wp-content/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf.
137. U.S. DEP'T OF JUSTICE, *supra* note 11, at 3.
138. Reasonable, articulable suspicion is defined as the ability "to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant [the] intrusion." Terry v. Ohio, 392 U.S. 1, 21 (1968).
139. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 3–5.
140. *Id.* at 3.
141. *Id.* at 3–4. For an example of how this works in practice and an explanation of how expansive this system has the potential to be, see Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *7 n.21 (D.D.C. Dec. 16, 2013).

give analysts the flexibility to find patterns of communication and connections among numbers.[142]

Any data that has not been reviewed is retained for five years and then automatically purged.[143] Additionally, any data that is found to have been improperly collected is also purged.[144]

3. Past Compliance Problems

Although there are standards and procedures in place, numerous problems have arisen regarding the use of the collected data. In a March 2009 order, FISC Judge Walton expressed concern over a number of past indiscretions involving NSA use of metadata.[145] For example, an alert list was set up to help prioritize the review of metadata, with all matches subject to the RAS standard before review.[146] However, most of the metadata that was queried was not RAS approved. In fact, the government reported that as of January 15, 2009, only 1,935 of the 17,835 identifiers on the alert list were granted RAS status by an authorized NSA official.[147]

Additionally, misrepresentations were made to the FISC concerning the alert-list process and the metadata collection program.[148] The NSA reported that this was due, in part, to the fact that "from a technical standpoint, there was no single person who had a complete technical understanding of [the collection program]."[149]

D. Past NSA Surveillance and Jewel v. NSA

Since the September 11 terrorist attacks, the NSA has been scrutinized for a number of surveillance programs.[150] Notably, in the aftermath of 9/11, President Bush expanded a surveillance program to include domestic communications with suspected terrorists, where previously, NSA warrantless surveillance was limited to parties outside the United States.[151] As early as 2006, reports indicated that mass data collection from American telephone companies was occurring, but that surveillance occurred without approval from the FISC.[152]

The history of NSA surveillance is extensive and ultimately beyond the scope of this Note, yet one ongoing case is particularly relevant in the

142. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 4.
143. Kris, *supra* note 136, at 15.
144. *Id.*
145. *See generally In re* Prod. of Tangible Things from [Redacted], No. BR 08-13, 2009 WL 9150913 (FISA Ct. Mar. 2, 2009).
146. *Id.* at *2.
147. *Id.* at *2 n.2.
148. *Id.* at *3–4. For example, Judge Walton points to repeated misrepresentations about the alert list process. *Id.*
149. *Id.* at *4.
150. *See How the NSA's Domestic Spying Program Works*, ELEC. FRONTIER FOUND., https://www.eff.org/nsa-spying/how-it-works (last visited Mar. 25, 2014).
151. Kathleen Clark, *The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program*, 2010 BYU L. REV. 357, 391.
152. *See id.* at 391–92.

current context. In *Jewel v. NSA*, the Electronic Frontier Foundation sued the government agencies involved in dragnet surveillance.[153] Originally filed in 2008, the suit is ongoing, but essentially seeks to prevent the same type of dragnet surveillance that has been at issue since the Snowden disclosures.[154] The complaint alleges that the government was operating a dragnet surveillance program by soliciting AT&T for the disclosure of all information in their telephone and internet records databases.[155]

In 2009, the Obama Administration moved to dismiss, asserting that it would require the government to divulge "state secrets."[156] The suit was instead dismissed on standing grounds, but was renewed in 2011 when the Ninth Circuit found the allegations were sufficient and the suit could continue in the district court.[157] The Ninth Circuit found that the plaintiffs alleged a concrete and particularized injury, the challenged action was fairly traceable to the harm suffered, and the issue was redressable.[158] Because there was standing, the suit was remanded to the district court to consider defenses, particularly whether the state secrets privilege prevented this action.[159]

In 2013, the Northern District of California found that the state secrets privilege was preempted by the procedural mechanisms of FISA under 50 U.S.C. § 1806(f).[160] The plaintiffs brought their claims under a number of FISA provisions, but notably *not* under 50 U.S.C. § 1861.[161] The court dismissed some of the statutory claims alleged by the plaintiffs, and noted that although there was standing, "the potential risk to national security may still be too great to pursue confirmation of the existence or facts relating to the scope of the alleged governmental Program."[162]

E. Current Litigation

This Note attempts to examine the relevancy standard and its application to the metadata collection program. That issue has been one of the main points of contention in a number of current lawsuits, and courts are now faced with the task of determining just how broad "relevant" is in relation to authorized national security surveillance programs. The Supreme Court declined to hear this issue, but in two lower court decisions, the judges

153. *See Jewel v. NSA*, ELEC. FRONTIER FOUND., https://www.eff.org/cases/jewel (last visited Mar. 25, 2014).

154. *See id.* (stating that the evidence in the case was "confirmed by the government in June, 2013").

155. Jewel v. Nat'l Sec. Agency, 673 F.3d 902, 906 (9th Cir. 2011).

156. *Id.* The state secrets privilege allows the government to "bar the disclosure of information if 'there is a reasonable danger' that disclosure will 'expose military matters which, in the interest of national security, should not be divulged.'" Jewel v. Nat'l Sec. Agency, No. C08-04373 JSW, No. C07-00693 JSW, 2013 WL 3829405, at *4 (N.D. Cal. July 23, 2013) (quoting United States v. Reynolds, 345 U.S. 1, 10 (1953)).

157. *Jewel v. NSA*, *supra* note 153.

158. *Jewel*, 673 F.3d at 908–12.

159. *Id.* at 913–14.

160. *Jewel*, 2013 WL 3829405, at *7.

161. *See id.* at *3.

162. *Id.* at *15.

deciding the case took very different views of the metadata collection program's legality. *Klayman v. Obama*[163] and *ACLU v. Clapper*[164] represent the first time a non-FISC judge has weighed in on the merits of the program.[165] Judge Leon, of the D.C. district court, reached the conclusion that the metadata collection program is not legal, while Judge Pauley, of the Southern District of New York, came to the opposite conclusion. In Part II, the arguments made in these three suits are examined collectively, as the points made are very similar and will inform the decisions on appeal.

1. *In re Electronic Privacy Information Center*

In *In re Electronic Privacy Information Center*,[166] EPIC petitioned the Supreme Court for a writ of mandamus, or, alternatively, a writ of certiorari to review the FISC's decision.[167] EPIC broadly argued that the metadata collection program does not comply with its statutory authority and, by granting the orders, the FISC exceeded its lawful jurisdiction.[168] EPIC further argued that because of the structure of the FISC, the Supreme Court is the only court that can grant relief,[169] and as a Verizon customer for the entire duration of the program,[170] EPIC has suffered an injury and is entitled to the writ. To grant a writ, the court must find that three requirements are met: (1) the party seeking the writ has no other adequate means of relief, (2) they have shown that the right to the writ is clear and indisputable, and (3) the issuing court believes the writ is appropriate given the circumstances.[171] On November 18, 2013, the Court denied the writ without explanation.[172]

2. *Klayman v. Obama*

In the first of two district court cases considering the issue, private individuals brought suit against a number of executive branch officials. This case was the first time a non-FISC federal judge addressed the legality of the metadata collection program.[173]

On December 16, 2013, Judge Leon granted a preliminary injunction preventing the federal government from collecting the records of two individuals, Larry Klayman and Charles Strange, and ordered the

163. No. 13-0851(RJL), 2013 WL 6571596 (D.D.C. Dec. 16, 2013).
164. No. 13 Civ. 3994 (WHP), 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013).
165. *See infra* Part I.E.2–3.
166. 134 S. Ct. 638 (2013).
167. EPIC Petition, *supra* note 5, at 1.
168. *See id.* at 12–13.
169. *Id.* at 13.
170. *Id.* at 10.
171. Cheney v. U.S. Dist. Court, 542 U.S. 367, 380–81 (2004).
172. *See In re* Elec. Privacy Info. Ctr., 134 S. Ct. 638, 638 (2013).
173. *See infra* note 348 and accompanying text.

destruction of any existing records pertaining to these individuals.[174] Larry Klayman has become well known for his litigation against the government over the past two decades and declared this the "biggest ruling in the history of government litigation."[175] Judge Leon accepted the plaintiffs' position that this type of data collection is not controlled by *Smith v. Maryland*.[176] He did, however, grant a stay of the order pending appeal due to the "significant national security interests at stake."[177] Judge Leon also cautioned that, should his ruling be upheld, the government should be prepared to immediately comply with the order, as the appeal process would likely take six months.[178]

3. *ACLU v. Clapper*

Finally, the ACLU filed suit in the Southern District of New York, naming James Clapper, Keith Alexander, Charles Hagel, Eric Holder, and James Comey as defendants.[179] The complaint alleges that the program exceeds it statutory authority and violates the First and Fourth Amendments.[180] The plaintiffs seek a permanent injunction discontinuing the use of FISC orders for metadata collection, as well as an order requiring the NSA to purge all of the data they have about the plaintiffs.[181]

On December 27, 2013, Judge Pauley granted the government's motion to dismiss, finding the metadata collection program legal.[182] Like Judge Leon, Judge Pauley dismissed the plaintiff's statutory claims, but, nonetheless, discussed the merits of the claims and reached the conclusion that they would ultimately fail.[183] Judge Pauley emphasized that all of the data is relevant because the government cannot otherwise make use of the information to find connections.[184] He ultimately based his dismissal on

174. Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *25 (D.D.C. Dec. 16, 2013).

175. Michael D. Shear, *Score One for Thorn in Government's Side Behind N.S.A. Ruling*, N.Y. TIMES, Dec. 18, 2013, at A19.

176. *See Klayman*, 2013 WL 6571596, at *18–19. See *infra* Part II.B for a full discussion of *Smith*'s application to the metadata collection program.

177. *Klayman*, 2013 WL 6571596, at *26.

178. *Id.*

179. Complaint for Declaratory and Injunctive Relief, *supra* note 10. All five defendants are high-ranking national security officers. Clapper is the director of National Intelligence, Alexander is the director of the NSA and the chief of the Central Security Service, Hagel is the Secretary of Defense, Holder is the U.S. Attorney General, and Comey is the director of the FBI. Robert Mueller III was the director of the FBI at the time of the initial complaint, but has since been replaced by Comey. *See Directors, Then and Now*, FBI, http://www.fbi.gov/about-us/history/directors (last visited Mar. 25, 2014).

180. Complaint for Declaratory and Injunctive Relief, *supra* note 10, at 10.

181. *Id.*

182. ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *1 (S.D.N.Y. Dec. 27, 2013).

183. *Id.* at *13.

184. *See id.* at *17.

constitutional grounds, holding that the metadata collection program does not violate either the Fourth or First Amendment.[185]

F. Standing and Jurisdiction

One concern with the issues surrounding the metadata collection program is whether courts will be willing to decide the merits of the case. Comparisons between the current issue and past cases involving NSA surveillance programs, like *Clapper v. Amnesty International USA*,[186] are inapposite. In *Clapper*, Amnesty International challenged the constitutionality of section 702 of FISA,[187] but the claim failed for lack of standing since Amnesty International could not establish an injury in fact.[188] There was no evidence that Amnesty International was a target of surveillance under the statute, and any speculation about a future injury failed to sustain the Article III standing requirement.[189]

Under the present surveillance program, however, evidence of an injury in fact exists, as there is documentation that Verizon, among other providers, turned over phone records for the vast majority of their customers.[190] Those customers can arguably assert an invasion of privacy and a violation of their Fourth Amendment rights, in addition to statutory claims, which is exactly what some parties have done in the current litigation.[191]

Regarding *In re Electronic Privacy Information Center*, the Supreme Court denied the petition for certiorari but did not state why.[192] The Court arguably could have exercised jurisdiction over the case, but ultimately chose not to. *Marbury v. Madison*[193] established that Congress lacks the ability to expand the Supreme Court's original jurisdiction.[194] However, when a particular suit is filed in the Supreme Court, the Constitution's original jurisdiction only applies where the petitioner does not seek to overturn a lower court decision.[195] Essentially, *Marbury* is not a bar to an original action that "attack[s] a lower-court decision that is not itself directly appealable."[196] Justice Souter described such suits as "commonly understood to be 'original' in the sense of being filed in the first instance in

185. *Id.* at *22, *24. See *infra* Part II.C.1.b for a full explanation of Judge Pauley's Fourth Amendment analysis.
186. 133 S. Ct. 1138 (2013).
187. 50 U.S.C. § 1881(a) (2006).
188. *Clapper*, 133 S. Ct. at 1143.
189. *Id.* at 1148–49.
190. *See supra* notes 2–5, 131 and accompanying text.
191. *See infra* Part II.
192. *See supra* note 172 and accompanying text.
193. 5 U.S. (1 Cranch) 137 (1803).
194. *See id.* at 178.
195. Steve Vladeck, *The Supreme Court's Power To Hear* In re EPIC, LAWFARE BLOG (July 10, 2013, 9:05 AM), http://www.lawfareblog.com/2013/07/the-supreme-courts-power-to-hear-in-re-epic/.
196. *Id.*

this Court, but nonetheless for constitutional purposes an exercise of [the] Court's appellate (rather than original) jurisdiction."[197]

Furthermore, there may have been statutory jurisdiction for the Court to hear the petition. EPIC asserts that the Court has jurisdiction under 28 U.S.C. § 1651 (the All Writs Act) and 50 U.S.C. §§ 1803 and 1861(f).[198] 50 U.S.C. §§ 1803(b) and 1861(f)(3) give the Supreme Court the authority to review decisions by the FISC, as appealed to the FISCR.[199] The All Writs Act allows appellate courts to exercise appellate review beyond what is provided for by statute as long as the review is "'in aid of' the appellate court's supervisory jurisdiction over the lower court."[200] Since the Court conceivably could have reviewed the metadata orders, the prerequisites of the All Writs Act are satisfied.[201]

Another interpretation of § 1803 is that the Supreme Court can only hear the petition if the FISCR denies a government application.[202] That, however, cannot happen here because the FISCR has not denied any government application.[203] A similar issue occurred in 2003 when the ACLU petitioned for a writ of certiorari regarding a Department of Justice surveillance program.[204] The ACLU acknowledged that FISA only allows for Supreme Court review following petition by the government, but interpreted Congressional silence on the issue of approved applications to mean that the Court could correct the FISCR's mistakes.[205] The ACLU further asserted that the All Writs Act is designed for situations such as the one they faced in 2003 and the current issue.[206]

Overall it appears that, at least in their ability to bring these suits, the parties involved have the right to challenge the metadata collection program.[207] In the case of EPIC's petition, the Supreme Court was always likely to dismiss the petition since an extraordinary writ "is not a matter of

197. Felker v. Turpin, 518 U.S. 651, 667 n.1 (1996) (Souter, J., concurring).

198. EPIC Petition, *supra* note 5. 50 U.S.C. § 1803(b) states in relevant part "the record shall be transmitted under seal to the Supreme Court, which shall have jurisdiction to review [a decision by the FISCR]." 50 U.S.C. § 1803(b) (2006). The All Writs Act permits the Supreme Court (and other courts established by Congress) to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." 28 U.S.C. § 1651(a).

199. Vladeck, *supra* note 195.

200. *Id.*

201. *Id.*

202. *See* Banks, *supra* note 79, at 1184.

203. *See supra* notes 106–09 and accompanying text.

204. *See* Banks, *supra* note 79, at 1185.

205. *Id.* at 1184–85.

206. *See id.* at 1185.

207. This, however, is contested by the defendants in *ACLU v. Clapper*. They argue that the plaintiffs lack standing to bring this suit. *See* Defendants' Memorandum of Law in Support of Motion to Dismiss the Complaint at 9–14, ACLU v. Clapper, No. 13 Civ. 3994 (WHP) (S.D.N.Y. Aug 26, 2013), 2013 WL 5221584. Similarly, in *In re Electronic Privacy Information Center*, the government largely rests their argument on standing and jurisdictional grounds, rather than emphasizing the merits of the case. *See generally* Brief for the United States in Opposition, *In re* Elec. Privacy Info. Ctr., 134 S. Ct. 638 (2013) (No. 13-58), 2013 WL 5702390.

right," is issued sparingly, and is entirely up to the Court's discretion.[208] It was thought that a dismissal would probably hinge on the merits rather than on jurisdictional grounds, as the Court is likely to allow lower courts to address the issue first when those suits have already been filed, as is the case here. The Court's reasoning behind the denial, however, remains to be determined.[209]

II. DEBATING THE MERITS: IS THE METADATA COLLECTION PROGRAM LEGAL? CONSTITUTIONAL CONCERNS AND INTERPRETING THE MEANING OF "RELEVANCE"

Central to the current litigation is the issue of what relevance means within the context of section 215. This Part discusses the arguments in each current suit collectively, rather than separately. Part II.A provides an overview of where the statutory authorization for the metadata collection program fits within the framework of the Fourth Amendment. Part II.B focuses on defining the word "relevant" within section 215 and debates the breadth of the term in regards to the metadata collection program. Part II.C briefly addresses the Fourth Amendment arguments on each side and discusses whether *Smith* controls.

A. Overview of the Applicable Legal Framework

If the metadata collection program is found to comply with all of the statutory requirements, it would constitute a presumptively reasonable search.[210] That, however, would not completely insulate the program from legal scrutiny, as it could still be found unconstitutional under either the First or Fourth Amendment.[211] It is important to understand the issue of relevancy within the context of the Fourth Amendment framework and the warrant requirements implemented by the courts because, although the searches conducted by the NSA are warrantless, they still have to meet the standards set forth in section 215 to be considered valid. The requirements for a valid search and the requirements set forth by section 215 are strongly intertwined, and neither can be understood without considering the other. Should the courts find that the program complies with the statute, the presumption of a valid search is rebuttable and the program could still be invalidated on Fourth Amendment grounds.

This Note seeks to determine whether the metadata collection program is legal as it is currently utilized. There are a number of debated points pertinent to that overall conflict, but this Note will focus on two main issues that have taken priority in the current litigation: (1) whether the data

208. SUP. CT. R. 20.1.

209. Vladeck, *supra* note 195.

210. *See supra* notes 82–83 and accompanying text.

211. *See infra* Part II.C. Neither of the two lower court decisions regarding this issue have been based on statutory grounds. *See* ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013); Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596 (D.D.C. Dec. 16, 2013).

collected can be considered "relevant" (as that is the central issue in assessing the validity of the metadata collection program under section 215), and (2) whether *Smith v. Maryland* governs a Fourth Amendment analysis of the metadata collection program. The constitutional concerns, however, are of lesser importance to this Note, as many scholars believe that, under current precedent, the program stands on solid constitutional footing.[212]

B. Is the Data "Relevant"?

The initial question in determining whether the metadata collection program complies with 50 U.S.C. § 1861 is whether there are reasonable grounds to believe that the data is relevant to the investigation.[213] Understanding the meaning of the term "relevant" within section 215 has proven challenging, and a number of arguments have been advanced in an attempt to define the term in the manner most advantageous to each side. The government argues that "relevant" is to be applied broadly—making the records collection process legal.[214] On the other hand, privacy advocates feel that it must be defined narrowly, and that by collecting billions of records, the NSA cannot reasonably be simply collecting only "relevant" records.[215] Ultimately, the question turns on whether investigations into specific terrorist groups can create reasonable grounds to believe that metadata of virtually the entire U.S. population is "relevant."[216]

As of the writing of this Note, no non-FISC judge has decided whether the metadata collection program is legal under section 215. In both *Klayman v. Obama* and *ACLU v. Clapper*, the only non-FISC cases to decide the issue to date, the judges declined to base their decisions on statutory grounds, stating that Congress did not intend to permit judicial review under an Administrative Procedure Act (APA) claim.[217] Instead, their decisions centered on the constitutional questions raised.[218] Defining relevance in the context of FISA, however, will likely be an essential part of these cases on appeal.[219]

The remainder of this Part addresses the various arguments and support on each side of the debate. Part II.B.1 looks to FISC opinions, while Part

212. *See infra* notes 349–50 and accompanying text.

213. Kris, *supra* note 136, at 18.

214. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 10–11.

215. EPIC asserted that "the FISC exceeded its statutory jurisdiction when it ordered production of millions of domestic telephone records that cannot plausibly be relevant to an authorized investigation." EPIC Petition, *supra* note 5, at *3.

216. *See* Kris, *supra* note 136, at 20.

217. Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *9–12 (D.D.C. Dec. 16, 2013). One of the main reasons why Congress did not intend for judicial review of this nature is that third parties were never to know about the existence of § 1861 orders, much less have the ability to litigate them. *Id.* at *10. Judge Pauley shared a similar sentiment. ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *13 (S.D.N.Y. Dec. 27, 2013) ("Congress did not intend that targets of section 215 orders would ever learn of them.").

218. *See infra* Part II.C.

219. *See infra* notes 349–50 and accompanying text.

II.B.2 turns to the text of 50 U.S.C. § 1861 itself. Part II.B.3 compares the statute to other sources of law that define "relevance," and Part II.B.4 considers the legislative history of the statute.

1. Differing FISC Interpretations

The FISC continually grants orders for the metadata collection program. The FISC first authorized the metadata collection program in 2006, and since that authorization, the program has been renewed thirty-five times (generally in three-month periods) by fifteen different judges.[220] FISC judges have, however, expressed mixed feelings about the program. While all have ultimately approved it, some are much more supportive of the program than others. Two of the FISC orders that have been made public are representative of the conflicting views on the program. Judge Eagan strongly supports the program, while Judge Walton had some reservations in his approval. These opinions are discussed in turn in Parts II.B.1.a and II.B.1.b.

a. Judge Eagan: The Metadata Collection Program Is Legal

In her August 2013 opinion regarding the issuance of an order in July 2013, Judge Eagan concluded that the standard for relevance is met by the metadata collection program because "international terrorist operatives are using telephone communications," and the bulk records help "to determine those connections between known and unknown international terrorist operatives."[221] Judge Eagan notes that the records do not actually need to be relevant, but that the government must show that there are "reasonable grounds to believe" that the records sought are relevant.[222] Because Congress left the term undefined, Judge Eagan adheres to a broad reading that "amounts to a relatively low standard."[223]

Judge Eagan adopted the reasoning of a 2010 FISC opinion that noted that a finding of relevance rests on whether the bulk collection is necessary for the NSA to utilize tools to generate investigative leads.[224] She stated that the government had done just that by "posit[ing] that bulk telephonic metadata is necessary to its investigations because it is impossible to know where in the data the connections to international terrorist organizations will be found."[225] The NSA uses the historical data once a specific terrorist identifier is found, and maintaining the bulk data allows them to keep that information until it is needed.[226] Without the totality of the data, the

220. *See Klayman*, 2013 WL 6571596, at *8; *see also* U.S. DEP'T OF JUSTICE, *supra* note 11, at 1.

221. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *6 (FISA Ct. Aug. 29, 2013).

222. *Id.*

223. *Id.*

224. *Id.*

225. *Id.* at *7.

226. *See id.*

information gathering process is stunted, thereby rendering the records "relevant."

b. Judge Walton Upbraids the NSA in 2009 for Failure To Conduct the Program in an Appropriate Manner

Judge Walton also signed the order and ultimately approved of the metadata collection program, but remained skeptical about it. His decision was based largely on the fact that the program had been consistently reauthorized, but he expressed concern about the privacy of U.S. citizens and the fact that "the FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses [telephony] metadata."[227] He pointed out a number of oversight problems with the program,[228] and went on to discuss his doubts about the structure and use of the metadata collection.[229] Judge Walton pointed out that "nearly all" of the call records obtained did not concern people who were targets of an FBI investigation, and that ordinarily, the data could not legally be obtained in bulk (i.e., would not be deemed relevant to the investigation).[230] He concluded that this alone would usually be enough for the FISC to deny the application for an order to a phone company.[231]

Despite this lack of relevance, Judge Walton granted the order based on the government's need for the data and the specific oversight procedures intended to monitor the use of the records.[232] Yet he strongly stated that the FISC no longer has confidence that the government is "doing its utmost to ensure" that the court's instructions are fully complied with.[233] As a result, he signed the order based on the FISC's prior determinations that the metadata collection program complies with 50 U.S.C. § 1861, but stated that "more is needed to protect the privacy of U.S. person information."[234]

2. Textual Analysis of 50 U.S.C. § 1861

The scope of relevance has been debated in the current litigation. As Judge Eagan and other supporters of the metadata collection program see it, "relevant" should be read broadly. Opponents of the program, on the other hand, feel that the term should be given its plain meaning, which they define as "actually related" to the investigation.

227. *In re* Prod. of Tangible Things from [Redacted], No. BR 08-13, 2009 WL 9150913, at *5, *8 (FISA Ct. Mar. 2, 2009).
228. *See supra* Part I.C.3.
229. *See In re Prod. of Tangible Things*, 2009 WL 9150913, at *16–20.
230. *Id.* at *6.
231. *Id.*
232. *See id.*
233. *Id.*
234. *Id.* at *8.

a. The Government's Argument: The Purpose Indicates That the Statute Should Be Understood Broadly

The NSA reads "relevant" broadly to encompass situations such as this. The NSA refers to general definitions to support this conclusion, such as "anything '[b]earing upon, connected with, [or] pertinent to' a specified subject matter."[235] In enacting the statute, Congress understood that relevance has special meaning within the law, and the government states that a document is "relevant" not just when it directly bears on the matter, but also where "it is reasonable to believe that it could lead to other information that directly bears on that subject matter."[236]

Where the language of a statute is ambiguous, as is arguably the case here given the debate surrounding the term, courts next look to its purpose.[237] The government contends that the data is relevant because there is reason to believe that conducting a broad search will produce counterterrorism information that fulfills the goal of the program in the first place.[238] As the government states, "Unless the data is aggregated, it may not be feasible to identify chains of communications," and the objectives advanced by the metadata collection program would not be successful if the NSA was limited in the amount of records it could obtain.[239]

b. The Opposition's Argument: The Plain Meaning of the Statute Invalidates the Program

Critics of the program point to the presumptively relevant definition[240] from section 215.[241] This includes records relating to an agent of a foreign power and individuals in contact with a suspected agent of a foreign power.[242] It is common sense that nearly all of the records obtained from Verizon and other phone service providers will not meet these criteria. They therefore believe that the FBI bears the burden of showing why those records are in fact relevant and should be included in the orders.[243]

Opponents further argue that "'everything' nullifies the relevance limitation in the statute."[244] Essentially, they contend that if law enforcement always has access to all records, they can inevitably identify a subset of records as "relevant"—yet that renders the term "relevant" essentially meaningless.[245] In construing a statute, courts are supposed to

235. U.S. DEP'T OF JUSTICE, *supra* note 11, at 9 (quoting 13 OXFORD ENGLISH DICTIONARY 561 (J.A. Simpson & E.S.C. Weiner eds., 2d ed. 1989)) (alterations in original).
236. *Id.* at 9.
237. *See* Bd. of Educ. v. Mergens, 496 U.S. 226, 271 (1990) (Stevens, J., dissenting).
238. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 8–9.
239. *Id.* at 13.
240. *See supra* note 117 and accompanying text.
241. *See, e.g.*, EPIC Petition, *supra* note 5, at *21–22.
242. 50 U.S.C. § 1861(b)(2)(A) (2006).
243. EPIC Petition, *supra* note 5, at *22.
244. *Id.*
245. *Id.*

give meaning to every word that Congress used,[246] but by defining bulk collection as relevant, they would in effect be ignoring that term.

Furthermore, the government has acknowledged that the vast majority of the data collected under the orders is not relevant to any investigation.[247] Allowing the NSA to determine what is relevant once the data is in their possession violates the plain meaning of the statute.[248] In essence, critics contend that the NSA is applying the prerequisite for collecting records retroactively. The statute requires that there be grounds to believe the data is relevant prior to collection, but that determination cannot be made until the records are actually in the NSA's possession and undergoing analysis.[249] It is not logical, according to EPIC's supporters, to believe that there are reasonable grounds that all, or even most, of the records collected will be relevant, which is in direct conflict with the statute's requirement that there be reason to believe the collected items are relevant.[250]

Even if the purpose of the statute is analyzed, critics point out that the program must comply with the guidelines set forth in Executive Order 12,333.[251] One such guideline is that the "[a]gencies within the Intelligence Community shall use the least intrusive collection techniques feasible."[252] Thus regardless of the NSA's stated purpose, the program is not the least intrusive means, as it affects all Americans.[253]

3. Comparing the Business Records Provision to Other Sources of Law

It is worth discussing other sources that define relevance, because the term is left undefined in section 215. No one source is directly on point, but taken collectively, the Federal Rules of Evidence, the rules of civil discovery, similar cases, and other statutes may help courts determine the best reading of "relevant."

a. Federal Rules of Evidence and Civil Discovery

Comparisons have been drawn to the Federal Rules of Evidence's standard for relevance.[254] Rule 401 states that evidence is relevant if "it has any tendency to make a fact more or less probable than it would be without

246. Reiter v. Sonotone Corp., 442 U.S. 330, 339 (1979).

247. Robert Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Newseum Special Program: NSA Surveillance Leaks: Facts and Fiction 8 (June 26, 2013), *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/887-transcript-newseum-special-program-nsa-surveillance-leaks-facts-and-fiction ("[T]he vast majority of the data is never going to be responsive to one of the terrorism-related queries.").

248. Privacy Professors' Brief, *supra* note 15, at 9.

249. *See id.* at 16.

250. *See id.* at 10–11.

251. *See* EPIC Petition, *supra* note 5 at 6–7.

252. Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

253. *See* EPIC Petition, *supra* note 5, at *23.

254. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *6 n.20 (FISA Ct. Aug. 29, 2013).

the evidence."[255] Under this analogy, information would be relevant if it has some bearing on investigations into terrorist organizations.

The Federal Rules of Evidence require that evidence must be material and have probative value to be considered relevant.[256] Materiality considers the fit between the evidence and the case, while probative value refers to the tendency of the evidence to establish the proposition that it is offered to prove.[257] Importantly, one item of evidence does not need to prove the proposition on its own; the evidence is taken en masse.[258] Regarding the metadata collection program, it is not entirely clear how the records fit this standard because the majority of the records individually fail to meet the standard of probative value, but might meet it when considered collectively.

The government also compares "relevant" to its use in civil discovery.[259] The Supreme Court has construed it to "broadly. . . encompass any matter that bears on, or that reasonably could lead to other matter that could bear on, any issue that is or may be in the case."[260] Thus they argue that courts have permitted bulk collection to satisfy a relevance standard.

b. Other Cases

Cases from other contexts may also prove helpful in defining relevance within section 215, but again, there are conflicting interpretations and applications.

i. Government Support

The government points to a number of cases where courts have found a relevance standard satisfied when a large volume of information is collected in order to identify a few pieces of pertinent information that directly impacted the investigation.[261] For example, in *In re Subpoena Duces Tecum*,[262] the Fourth Circuit held that all of a doctor's files could be relevant in an investigation of federal healthcare offenses, despite the fact that not all of them were evidence of the offenses with which he was charged.[263] Additionally, in *Carrillo Huettel, LLP v. SEC*,[264] the Southern District of California held that although not all of the records requested were relevant, they would likely contain enough relevant information for the subpoena to be considered valid.[265]

---

255. FED. R. EVID. 401(a).
256. MCCORMICK ON EVIDENCE 306 (Kenneth S. Broun ed., 6th ed. 2006).
257. *Id.*
258. *Id.* at 308.
259. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 9; *see also infra* note 285 and accompanying text.
260. Oppenheimer Fund, Inc. v. Sanders, 437 U.S. 340, 351 (1978).
261. U.S. DEP'T OF JUSTICE, *supra* note 11, at 10 nn.7–9.
262. 228 F.3d 341 (4th Cir. 2000).
263. *See id.* at 350.
264. Civ. No. 11cv65–WQH(CAB), 2011 WL 601369 (S.D. Cal. Feb. 11, 2011).
265. *Id.* at *2–3.

David Kris, former Assistant Attorney General for National Security, points to *In re Grand Jury Proceedings: Subpoena Duces Tecum*[266] as the most analogous case.[267] There, the government sought records about drug dealers in Kansas City, and in order to locate them, subpoenaed substantially all of Western Union's records, including those of "hundreds of innocent people."[268] The Eighth Circuit, however, approved the subpoena but left open the possibility that on remand the subpoena could be narrowed.[269]

ii. Privacy Advocates' Support

On the other side of the debate, critics point to cases where courts have found that bulk data collection does not amount to relevance in searches for a few key pieces of information.[270] For example, in *In re Grand Jury Subpoena* Duces Tecum *Dated Nov. 15, 1993*,[271] the Southern District of New York held that a subpoena failed the relevancy standard because the data sought contained too much irrelevant information along with the pertinent data.[272] The court explained that because the subpoena demanded irrelevant documents, it was unreasonably broad.[273]

Additionally, in the civil discovery context, the Supreme Court has stated that a subpoena for "all documents" was "anything but appropriate" because it was too broad in what it sought.[274] Again, none of the cases cited in the context of the metadata collection program squarely address the issue presented here and most are tangentially related at best. The courts will therefore be tasked with defining relevance with little guidance from prior decisions.

c. The Stored Communications Act Provides a Point of Statutory Comparison

Section 2703(d) of the Stored Communications Act establishes procedures for the government to obtain information from electronic communications service providers.[275] While not directly related to FISA because it is not related to preventing international terrorism, the language of the statute is very similar to that of section 215. In order to obtain noncontent records (i.e., records pertaining to the subscriber or customer that do not include the content of the communication), the government must offer "specific and articulable facts" demonstrating that there are

266. 827 F.2d 301 (8th Cir. 1987).
267. Kris, *supra* note 136, at 25.
268. *In re Grand Jury Proceedings*, 827 F.2d at 305.
269. *Id.* at 305–06.
270. *See, e.g.*, Kerr, *supra* note 14.
271. 846 F. Supp. 11 (S.D.N.Y. 1994).
272. *Id.* at 13–14.
273. *Id.*
274. Cheney v. U.S. Dist. Ct., 542 U.S. 367, 387–88 (2004). *But see supra* notes 259–60 and accompanying text.
275. *See* 18 U.S.C. § 2703 (2012).

"reasonable grounds to believe that [the records sought] are relevant and material to an ongoing criminal investigation."[276] This is slightly different from section 215, as section 2703(d) requires specific and articulable facts, while section 215 only requires "reasonable grounds."[277] Arguably, section 215 amounts to a lower standard, especially since the specific and articulable facts language existed prior to September 11.[278] Section 2703(d) also refers to criminal investigations, whereas section 215 is for foreign intelligence purposes. As such, it seems, according to the government, that Congress provided "more latitude at the production stage," but balanced it with "post-production checks" that are not present in the Stored Communications Act.[279]

4. Legislative History from the Reauthorizations of Section 215

Over time, FISA has been amended to broaden the scope of the type of things the government can access—as a tradeoff, however, it has become arguably more restrictive in how those things might be accessed.[280] Previously, FISA required the FBI to present "specific and articulable facts," rather than just a showing of relevance.[281] The word "relevancy" was added to section 215 during the 2005 and 2006 reauthorizations.[282]

Critics of the program point to legislative history accompanying the amended statute in 2006, which indicates that the relevancy requirement was added in order to limit the information available under section 215. For example, Senator Wyden discussed his fears that the statute would be used to fight terrorism at the expense of civil liberties, but that ultimately the power to go on "fishing expeditions" was not included in the version to be passed.[283] Senator Feinstein noted that section 215 was changed to "tighten[] the requirement to make it clear that investigators must not only show relevance but also that the request pertains to a known or suspected agent of a foreign power or their associates."[284] Putting the standard in context, Senator Kyl indicated that "[r]elevance is a simple and well established standard of law," and that its use in section 215 was meant to be

276. *Id.* § 2703(d).

277. *Compare* 50 U.S.C. § 1861(b)(2)(A) (2006), *with* 18 U.S.C. § 2703(d) (2012).

278. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *5 (FISA Ct. Aug. 29, 2013).

279. *Id.*

280. Privacy Professors' Brief, *supra* note 14, at 18.

281. Complaint for Declatory and Injunctive Relief, *supra* note 10, at 5.

282. *Compare* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 412, 115 Stat. 272 (codified at 8 U.S.C. § 1226a (2012)) (permitting a request for an order, so long as the investigation concerns "international terrorism or clandestine intelligence activities"), *with* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (requiring reasonable grounds to believe that the items sought are relevant).

283. 151 CONG. REC. 19,306 (2005) (statement of Sen. Ron Wyden).

284. *Id.* at 19,309 (statement of Sen. Dianne Feinstein).

understood in the same manner as other areas of law like subpoenas and civil discovery.[285]

The government points to the fact that the legislature has repeatedly reenacted the statute without change.[286] The problem with this is that the majority of the information needed to make an informed decision about the metadata collection program was, and in many cases remains, classified. However, information was provided to members of both houses through their respective Intelligence Committees prior to both the 2009 and 2011 reauthorizations. For example, prior to the May 2011 reenactment, the Office of the Assistant Attorney General provided notice to the chairmen of the Intelligence Committee of each house to share certain information with their members.[287] The report highlighted the key points of the program, including the fact that it "collect[s] a large amount of information," and that the orders require the production of "substantially all of the telephone calls" handled by a service provider.[288] It also mentions that there is a system of checks and balances in place, but that there have been compliance issues despite those safeguards.[289]

According to certain members of Congress, though, they did not intend for unbounded freedom in determining what is relevant.[290] They assert that under their understanding of the statute, the metadata collection program goes beyond their definition of relevant and that relevant was meant to be a limitation, not a broad standard.[291] Moreover, they required that it be relevant to *an* authorized investigation, rather than general efforts to combat terrorism.[292] Congressman Sensenbrenner, writing for at least some of his colleagues, argues that they understood "relevant" to be a limiting factor, and that they did not intend for it to allow the kind of dragnet collection that the NSA is currently conducting.[293]

285. *See* 152 CONG. REC. 2426 (2006) (statement of Sen. Jon Kyl); *see also supra* notes 259–60, 274 and accompanying text.

286. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 17.

287. Letter from Ronald Welch, Assistant Attorney General, to the Chairmen of the Congressional Intelligence Committees (Feb. 2, 2011), *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf.

288. U.S. DEP'T OF JUSTICE, REPORT ON THE NATIONAL SECURITY AGENCY'S BULK COLLECTION PROGRAMS FOR USA PATRIOT ACT REAUTHORIZATION 1, 3 (2011), *available at* http://www.dni.gov/files/documents/2011_CoverLetters_Report_Collection.pdf.

289. *Id.* at 3–4. For a discussion of some of the compliance issues, see *supra* Part I.C.3.

290. *See* Brief *Amicus Curiae* of Congressman F. James Sensenbrenner, Jr. in Support of Plaintiffs, ACLU v. Clapper, No. 13 Civ. 3994(WHP) (S.D.N.Y. Sept. 4, 2013), *available at* https://www.aclu.org/sites/default/files/assets/2013.09.04_amicus_brief_-_rep_sensenbrenner.pdf [hereinafter Sensenbrenner Brief].

291. *Id.* at 2.

292. *Id.* at 3.

293. *See id.* at 4. For more on Congressman Sensenbrenner's opinions, see *infra* notes 297–99 and accompanying text.

5. Executive and Legislative Responses: Embrace the Program or Rein It In?

The metadata collection program has proven to be extremely divisive, and the recent attention given to NSA surveillance has caused politicians to weigh in on the debate. The remainder of this section provides an overview of public officials' statements concerning the program, competing bills in Congress addressing mass data collection, and the recommendations of a presidential task force assembled to deal with the issue.

a. Conflicting Public Statements

The Obama Administration generally still supports the program, as evidenced by statements made by Robert Litt, General Counsel at the Office of the Director of National Intelligence, over the summer of 2013.[294] In his address, he characterized Snowden's leaks as "reckless" and emphasized the legality of the program.[295] He outlined the rationale behind the conclusion that the program is legal, taking care to note that it is not just "the Intelligence Community alone" that believes bulk collection is authorized under section 215, but also FISC judges and Congress.[296]

On the other side of the debate, Congressman Sensenbrenner, author of the Patriot Act and a member of Congress during all of the Patriot Act's reauthorizations, offered an intriguing opinion. He noted that the metadata collection program is not being used in the manner that section 215 was intended.[297] In his view, mass data collection exceeds the scope of the statute's design.[298] By necessity, bulk collection brings in millions of unrelated records, but that goes "beyond any reasonable understanding of [relevant]."[299]

As discussed, Sensenbrenner indicated that he was unaware of how the metadata collection program operated at the time that he reauthorized it, but members of Congress were provided with information outlining the basics of the program.[300] Senate Majority Leader Reid indicated that it is illogical for Senators (and presumably Congressmen) to say that they were unaware of what was occurring.[301] As he points out, there were "many" classified

294. Robert S. Litt, Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Privacy, Technology and National Security: An Overview of Intelligence Collection (July 19, 2013), *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

295. *Id.*

296. *Id.*

297. *See generally* Sensenbrenner Brief, *supra* note 290 (arguing that Congress did not authorize the type of data collection the NSA is currently undertaking).

298. *See generally id.*

299. *See id.* at 5–6.

300. *See supra* notes 286–89 and accompanying text.

301. Michael McAuliff & Sabrina Siddiqui, *Harry Reid: If Lawmakers Didn't Know About NSA Surveillance, It's Their Own Fault*, HUFFINGTON POST (June 11, 2013, 4:04 PM), http://www.huffingtonpost.com/2013/06/11/harry-reid-nsa_n_3423393.html.

and unclassified meetings, and if an individual did not avail himself of the opportunity to attend, he should not be able to complain that he was ill informed after the fact.[302]

b. Congressional Response: Competing Bills To Define the Scope of Governmental Authority Under § 1861

Over the summer of 2013, a one-sentence bill was introduced and narrowly failed to pass the House of Representatives.[303] The bill would have required all 50 U.S.C. § 1861 orders funded by FISA provisions to include the sentence, "This Order limits the collection of any tangible things . . . to those tangible things that pertain to a person who is the subject of an investigation described in section 501 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1861)."[304] This blanket prohibition ultimately failed, but indicates the growing concern over the metadata collection program.

More recently, there was a renewed attempt to revise FISA. Some members of Congress have indicated a willingness to curb the power of the NSA regarding domestic surveillance through the introduction of the USA FREEDOM Act (Freedom Act).[305] The bill is being co-authored by Congressman Sensenbrenner, and would end "dragnet collection of phone records under Section 215" by requiring that the records obtained are "relevant and material to an investigation," a more exacting standard than the one currently enforced by FISA.[306] Additionally, the bill seeks to add a more exacting judicial review process and enhanced accountability and transparency.[307] The main goal of the bill is to tighten the rules surrounding the collection of metadata by requiring that the items collected pertain to "a foreign power or agent of one; the activities of a target who is a suspected agent of a foreign power; a person in contact with a known or suspected agent of a foreign power," which, in effect, eliminates the viability of the metadata collection program.[308]

While some of Congress is looking to rein in the power of FISA, others are criticizing those efforts. Patrick Kelley, acting general counsel of the FBI, stated that the logic behind the Freedom Act is flawed because it presumes that the NSA knows exactly who they are after, which is not true.[309] He posits that bulk collection is necessary. In that same vein,

---

302. *Id.*
303. Kris, *supra* note 136, at 56–57.
304. 159 CONG. REC. H5023 (daily ed. July 24, 2013).
305. *Id*. at S7618 (daily ed. Oct. 29, 2013).
306. *Id*. at S7619.
307. *See id.*
308. Raffaela Wakeman, *An Overview of FISA Reform Options on Capitol Hill*, LAWFARE BLOG (Nov. 3, 2013 10:08 AM), http://www.lawfareblog.com/2013/11/an-overview-of-fisa-reform-options-on-capitol-hill/.
309. *See* Jared A. Favole, *Intelligence Lawyers Cool to Bill To Revamp NSA*, WALL ST. J. (Nov. 4, 2013, 4:40 PM), http://online.wsj.com/news/articles/SB10001424052702304391204579178132698285314.

Senator Feinstein, chairperson of the Senate Select Committee on Intelligence, along with Ranking Member Chambliss have introduced their own bill in opposition to the view that the Freedom Act authors take.[310] The FISA Improvements Act would affirm the legality of the metadata collection program, but would codify restrictions on when and how the data can be accessed and used.[311] It would impose a strict retention period of five years for any data collected under section 215, and would require approval by the attorney general for querying any data older than three years.[312] The bill would also codify certain issues that were previously addressed in FISC orders, including the limit on hops and the number of people who can access the collected metadata.[313] Finally, the bill would require the NSA to submit its findings of RAS for U.S. persons to the FISC for judicial review, and denial of the request would result in destruction of that collection.[314] The bill largely keeps the metadata collection program intact, while providing for some additional oversight and explicitly codifying the practices that are already ongoing.

c. The Executive Branch Response

While members of Congress immediately began a dialogue about the program, the executive branch was slower to take action. President Obama assembled a task force in August 2013 to brainstorm potential changes to mass data collection, and then in January 2014, gave a public address outlining his decision based on the recommendations of that task force.

i. The Presidential Task Force Recommends Changes

In August 2013, President Obama established a task force, the Review Group on Intelligence and Communications Technology, to assess the NSA metadata collection program and propose changes.[315] The group ultimately proposed more than forty changes to the NSA's current surveillance tactics.[316] In their final report, the panel recommended that the data be maintained by the service providers, rather than collected by the NSA, and that the government only have access to a specific individual's data pursuant to a court order.[317] The report also recommended changes to the FISC appointment process, suggesting that the power be distributed among all nine Supreme Court justices, rather than remaining solely in the hands of the chief justice.[318] The report ultimately does not call for a complete shutdown of the program, but did state that the current system "creates

310. Wakeman, *supra* note 308.
311. *Id.*
312. *Id.*
313. *Id.*
314. *Id.*
315. Siobhan Gorman, *Panel Pushes Revamp of NSA*, WALL ST. J., Dec. 13, 2013, at A1.
316. *See* David E. Sanger & Charlie Savage, *Obama Is Urged To Sharply Curb N.S.A. Data Mining*, N.Y. TIMES, Dec. 19, 2013, at A1.
317. *Id.*
318. *Id.*

potential risks to public trust, personal privacy, and civil liberty."[319] The group's recommendations are not binding, but President Obama has indicated that he is open to the suggestions provided.[320]

ii. President Obama Begins the Process of Change

In a January 2014 speech, President Obama outlined a number of changes to be implemented to the metadata collection program, among other NSA surveillance programs.[321] The address called for FISC approval before data can be examined by analysts, except in cases of emergency.[322] Additionally, the President limited any analysis to two hops, rather than the current three.[323] As far as where and how the records will be stored and whether the FISC will be restructured, the President left those decisions in the hands of Congress.[324]

C. Fourth Amendment: Are These Unreasonable Searches?

While the Fourth Amendment concerns raised by the metadata collection program are important, this Note only discusses them briefly. If the courts decide that the metadata collection program comports with FISA, they will then be tasked with deciding the question of whether the orders are constitutional. The essential inquiry in that analysis is whether *Smith v. Maryland* and the third-party doctrine control the type of data collection that the NSA is currently conducting. It is important to note, however, that even if the activity amounts to a search under the Fourth Amendment, it may still be "reasonable" based on the strong governmental interests at stake.[325] Part II.C.1 examines the government's argument and Judge Pauley's decision that *Smith* controls. Part II.C.2 discusses the various arguments advanced by privacy groups, and the opinion from *Klayman v. Obama* in which Judge Leon found that *Smith* does not control this particular issue.

1. *Smith v. Maryland* Directly Controls This Issue

The NSA contends that *Smith* controls a Fourth Amendment analysis of the metadata collection program. Judge Pauley supported this conclusion in *ACLU v. Clapper*.

---

319. THE PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 17 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

320. *See* Sanger & Savage, *supra* note 316.

321. *See* Mark Landler & Charlie Savage, *Obama Outlines Calibrated Curbs on Phone Spying*, N.Y. TIMES, Jan. 18, 2014, at A1.

322. *See id.*

323. *See id.* ("[The NSA] will be able to scrutinize phone calls that are only two steps removed from a number associated with a terrorism suspect, rather than three.").

324. *See* Peter Baker & Jeremy W. Peters, *With Plan To Overhaul Spying, the Divisiveness Is in the Details*, N.Y. TIMES, Jan. 19, 2014, at A19.

325. *See* Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *22 (D.D.C. Dec. 16, 2013); *see also infra* note 353 and accompanying text.

a. The Government's Argument

The NSA argues that because the data collected by the program has all been voluntarily turned over to a third party, the subscribers have no reasonable expectation of privacy in it and there is no Fourth Amendment violation.[326] The government takes this position even while acknowledging that the information collected here is more extensive than the simple pen register at issue in *Smith*.[327]

The government bolsters its argument by pointing out that the Court affirmed its holding in *Smith* in subsequent cases, and lower courts have found that the holding in *Smith* goes beyond the narrow limitations of a classic pen register.[328] Under Supreme Court precedent, the reasoning in *Smith* applies "even if there is an understanding that the third party will treat the information as confidential."[329] For example, in *SEC v. Jerry T. O'Brien, Inc.*,[330] the Court stated that "when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities."[331] Additionally, in *United States v. Reed*,[332] the Ninth Circuit found that collecting call origination, length, and time information was nothing more than a pen register and trap-and-trace device, leaving the target with no reasonable expectation of privacy.[333] The government argues that *United States v. Jones* is easily distinguished from the issue here because it does not involve a physical trespass similar to the GPS in *Jones* and thus does not affect the current third-party doctrine.[334]

b. The Judicial Support: ACLU v. Clapper

In assessing the legality of the metadata collection program, Judge Pauley accepted the government's position that *Smith* controls. First, he accepted the premise that information voluntarily conveyed to a third party is no longer afforded the same level of privacy.[335] Moreover, he stated that "[t]he ACLU's reliance on the concurring opinions in *Jones* is misplaced" because the Court did not overrule *Smith*, and it is improper for lower courts to speculate on whether precedent will be overruled.[336] Therefore, at

326. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 19.
327. *Id.* at 20.
328. *See id*. at 21.
329. *Id.* at 20.
330. 467 U.S. 735 (1984).
331. *Id.* at 743.
332. 575 F.3d 800 (9th Cir. 2009).
333. *See id.* at 914.
334. *See* U.S. DEP'T OF JUSTICE, *supra* note 11, at 20.
335. *See* ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *21 (S.D.N.Y. Dec. 27, 2013).
336. *Id.* at *22.

least for now, lower courts are bound by *Smith* and do not have the freedom to ignore the third-party doctrine.[337]

2. *Smith v. Maryland* Is Distinguishable

Part II.C.2.a provides an overview of the privacy advocates' argument that *Smith* is distinguishable from the metadata collection program and therefore does not control a Fourth Amendment analysis. Judge Leon supported this outcome in his opinion in *Klayman v. Obama*, which is outlined in Part II.C.2.b.

a. The Privacy Advocates' Argument

Privacy advocates assert that the metadata collection program violates the Fourth Amendment on several grounds. First, privacy advocates argue that because the orders compel phone companies to turn over all records on a daily basis, they are general warrants, which are banned by the Fourth Amendment's particularity requirement.[338]

Privacy advocates further argue that *Smith v. Maryland* is distinguishable from the current facts and was wrongly decided.[339] *Smith* involved a single suspect, whereas the metadata collection program involves mass surveillance that can reveal more about an individual's habits and personal life than a simple pen register that only records what numbers are being called.[340] Moreover, the data collected here involves routing information, which includes data about the cell sites involved and the path of the call.[341] This type of data goes beyond what was collected in *Smith*, because it allows the NSA to track an individual's location to some degree.[342]

Privacy advocates suggest that even if *Smith* controls, the Court should reconsider the third-party doctrine in order to adapt to modern technology.[343] Advocates maintain the public is aware that records are turned over to their service providers, but there is no reason to assume those records are available beyond that closed universe.[344] In *Jones*, members of the Court suggested that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," because we live in a "digital age" where people are constantly revealing information about themselves to third parties.[345] Echoing Justice Marshall's dissent in *Smith*, it has become impossible for people to conduct their ordinary business without exposing

337. *See id.*
338. Cato Brief, *supra* note 15, at 10–11.
339. *Id.* at 14.
340. *Id.* at 18–19.
341. EPIC Petition, *supra* note 5, at 26–27.
342. *See id.* at 28.
343. Cato Brief, *supra* note 15, at 19.
344. *Id.* at 20.
345. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also supra* notes 69–73 and accompanying text.

themselves to the risk of surveillance.[346] These groups assert that the time for reconsideration has come and the metadata collection program provides the ideal platform to do so.[347]

b. The Judicial Support: Klayman v. Obama

In *Klayman v. Obama*, Judge Leon was the first non-FISC judge to evaluate the metadata collection program and was presented with arguments concerning both section 215 and the Fourth Amendment.[348] Judge Leon chose to grant the injunction on Fourth Amendment grounds. This became a controversial point, as some scholars feel that the metadata collection program rests on solid constitutional grounds given the *Smith* third-party doctrine, and that the real gray area is whether the program exceeds its statutory authority.[349] There is speculation that on appeal, "the constitutional issue will disappear from the case altogether."[350] Judge Leon, however, stated that the issue before the Court in *Smith* was "a far cry from the issue in this case," and that because *Smith* is such an old decision with respect to technological advances, it cannot be considered precedent for this issue.[351] Judge Leon emphasized that while the data itself might not be drastically different from that at issue in *Smith*, the relationship people now have with their phones, as opposed to thirty-four years ago when *Smith* was decided, significantly alters the legal landscape.[352] Judge Leon concluded that the plaintiffs had shown a significant likelihood that they would succeed on the merits of their claim, a requirement to obtain a preliminary injunction because the metadata collection program does not meet the standard for "special needs," another exception to the warrant requirement.[353] While his constitutional analysis raises interesting questions, the real issue on appeal will likely center on the statutory authority for the program.

346. *See supra* notes 56–57 and accompanying text.

347. Cato Brief, *supra* note 15, at 21.

348. *See* Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *23 (D.D.C. Dec. 16, 2013).

349. *See, e.g.*, Paul Rosenzweig, *The Lynchpin of the Meta-data Opinion*, LAWFARE BLOG (Dec. 16, 2013 3:23 PM), http://www.lawfareblog.com/2013/12/the-lynchpin-of-the-meta-data-opinion/ (calling Judge Leon's reasoning unpersuasive and speculating that it will be "not of long duration"); Benjamin Wittes, *Thoughts on Judge Leon's Section 215 Opinion*, LAWFARE BLOG (Dec. 17, 2013 12:06 AM), http://www.lawfareblog.com/2013/12/thoughts-on-judge-leons-section-215-opinion/ (suggesting that *Smith v. Maryland* squarely controls this issue, but as the case advances, higher courts may be willing to reconsider in light of technological advances).

350. Steve Vladeck, *Three Unrelated Tidbits on the NSA and* Klayman v. Obama, LAWFARE BLOG (Dec. 18, 2013 12:46 PM), http://www.lawfareblog.com/2013/12/three-unrelated-tidbits-on-the-nsa-and-klayman-v-obama/.

351. Klayman v. Obama, No. 13-0851(RJL), 2013 WL 6571596, at *18 (D.D.C. Dec. 16, 2013).

352. *See id.* at *21.

353. *Id.* at *22.

III. DEFINING RELEVANCE: PROPOSING A RETURN TO A MORE RESTRICTIVE VIEW OF SEARCHES AND KEEPING PRIVATE INFORMATION PRIVATE

Taking all of the arguments into account and considering the national security concerns, the ideal solution is a middle ground between the two sides where the NSA is not completely prevented from collecting data, but also has more limits on its authority and greater oversight to ensure the proper use of the records it does obtain. Part III.A argues that under current precedent, the metadata program is permissible, but in spite of this, the Court or Congress should step in to limit the NSA's power to collect bulk data. Part III.B outlines a potential framework for establishing a compromise between the two sides.

A. The Metadata Collection Program Is Legal but Should Be Limited in Scope

Ultimately, it appears that the metadata collection program is authorized based on current interpretations of the law. *Smith v. Maryland* provides the Fourth Amendment basis for obtaining the records, and although the Court has indicated that advances in technology might necessitate reevaluation, they have yet to do so.[354] The rationale for the metadata collection program currently rests largely on the fact that it has been approved by fifteen different FISC judges,[355] and outside of a common sense definition of "relevant," there is no overwhelming evidence that the statute has been wrongly interpreted. There is nothing to prevent the Court, however, from shifting back to a more restrictive view of searches. Technology is developing faster than ever before and, as a whole, Americans are more reliant on it than in previous decades. As such, the law needs to account for the inability of people to deny information to their third-party service providers and reevaluate the breadth of what is currently authorized by FISA.[356]

This goal can be achieved through either reform or elimination. Reform would entail providing for more stringent oversight or stricter criteria for what types of records can be collected and under what circumstances it can be compiled. Elimination, on the other hand, would involve a general

354. *See supra* Parts I.A.1.b.ii, II.C.1.

355. *See supra* note 220 and accompanying text.

356. This approach has been advocated previously in a more general Fourth Amendment context. *See, e.g.*, Timothy Casey, *Electronic Surveillance and the Right To Be Secure*, 41 U.C. DAVIS L. REV. 977, 1033 (2008) ("[W]e would do well to reconsider the modern contours of a reasonable expectation of privacy, and whether, owing to the pervasive capability of modern technology to easily intrude into the most intimate details of our life, the People have any expectation of privacy or right to be secure."); Russell L. Weaver, *The Fourth Amendment, Privacy and Advancing Technology*, 80 MISS. L.J. 1131, 1225 (2011) (discussing the potential shortcomings of the *Katz* reasonable expectation of privacy test and the possibility that it does not adequately address concerns in a more technologically advanced world).

prohibition on mass data collection entirely.[357] The current response seems to favor reform, and while it might be achieved by any of the three branches, it appears that any significant change is going to be the result of a collective effort. The current litigation gives the courts the appropriate platform for reining in bulk data collection, and the executive and legislative branches have taken initial steps in working towards long-term solutions.[358]

B. The Program Should Continue on a Smaller and More Defined Scale

The metadata collection program demonstrates the conflict between the need for secrecy and the value of transparency.[359] Clearly, for public safety, the government must be able to keep certain information classified, but at the same time, in order to maintain a free society, the public should be privy to certain information about government surveillance. Because the goals of ensuring national security and protecting the American public are worthy and important, the ideal choice—though intensive and likely a very lengthy process—would be an overhaul of the existing FISA structure.

1. Evaluating the Steps Already Taken

Short of changing Fourth Amendment jurisprudence (although some members of the Court have hinted that it may be time to do so), reform of FISA, rather than elimination, is the ideal solution. President Obama has taken the initial steps towards change,[360] but his solutions fall short of a long-term fix. For some of the more difficult and intricate decisions, the President has called on Congress to help. This, however, is problematic given the current divide on the issue as evidenced by the competing bills.[361] The Freedom Act goes too far in the opposite direction from the current state of electronic surveillance because it would essentially shut down the metadata collection program.[362] The data is meant to be useful in finding connections and working towards the goal of preventing terrorism, and without that information, national security is in jeopardy.[363] Patrick Kelley, acting general counsel of the FBI, indicated that the approach advocated in the Freedom Act is flawed because it presumes that there are specific targets, but it is not always entirely clear who intelligence officers are looking for until they have started analyzing the data.[364] The FISA

357. This approach is being contemplated in Congress through the Freedom Act. *See supra* notes 305–08 and accompanying text.

358. *See supra* notes 322–24 and accompanying text.

359. Kris, *supra* note 136, at 41; *see also* ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *1 (S.D.N.Y. Dec. 27, 2013) ("The natural tension between protecting the nation and preserving civil liberty is squarely presented by the government's bulk telephony metadata collection program.").

360. *See supra* notes 322–24 and accompanying text.

361. *See supra* notes 322–24 and accompanying text.

362. *See supra* notes 305–08 and accompanying text.

363. *See supra* note 127 and accompanying text.

364. *See* Favole, *supra* note 309.

Improvements Act, on the other hand, does not go far enough, as it primarily serves to codify the existing structure, which President Obama has decided against.[365]

2. Where Do We Go From Here? Scaling Back the Program

The success of the metadata collection program is controversial and it is not entirely clear how effective it has been in preventing terrorism. Some reports state that the NSA cannot point to any significant number of plots prevented by the program or any other objective measure of success.[366] Others, however, suggest that the program has been considerably beneficial. For example, Judge Pauley pointed to three separate times in 2009 where metadata was queried in connection with terrorist plots that were ultimately foiled.[367] These three instances, even standing alone, merit the continuance of the metadata collection program in some form. Preventing just one act of terrorism indicates success, but the bigger question is how much individual privacy the American public should have to sacrifice to achieve that success. At this time, there is not enough reported value in the program to warrant its continuance on its current scale.

Even accepting that the program may have prevented a number of terrorist plots, the NSA has not explained why less obtrusive measures would be inadequate to achieve the goal of preventing terrorist activities. Because the data can only be queried if it is one of the identified, RAS-approved numbers,[368] there is no reason why the NSA could not request those records specifically in the order. Arguably, this is a more cumbersome process, as any numbers that are in contact with the identifier would then also need to be requested and so on until the third hop (or second after President Obama's changes are implemented)[369] was completed.

Since it would be burdensome and inefficient to collect the records this way, the best alternative seems to be limiting the scope of what FISC orders may request, which would, in essence, eliminate bulk data collection with few exceptions. With the level of technology available, it would certainly be feasible to obtain a group of records for numbers in contact with identified terrorist numbers. Essentially, this approach could allow the NSA to obtain the data for the three hops that its analysts are currently permitted to query without obtaining data beyond that. This would not act as a blanket prohibition on metadata collection and would even permit large amounts of records to be obtained simultaneously, but would afford the general population a greater level of privacy protection than the current

365. *See supra* notes 310–14 and accompanying text.

366. Yochai Benkler, *Fact: The NSA Gets Negligible Intel from Americans' Metadata. So End Collection*, GUARDIAN (Oct. 8, 2013, 12:02 EDT), http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

367. *See* ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *25 (S.D.N.Y. Dec. 27, 2013).

368. *See supra* notes 138–39 and accompanying text.

369. *See supra* notes 322–24 and accompanying text.

system permits. Service providers would be responsible for keeping the data, as they already are, and would only provide the necessary information to government officials.[370] Also, this approach would not require the court order that President Obama has implemented. While court approval sounds good in theory, the FISC has proven that it is inclined to rubber-stamp anything the NSA requests. The proceedings would also still be secretive and one-sided, therefore resulting in no added protection to the current system, while slowing the process down.

The costs of the current FISA structure have proven to far outweigh its benefits. Although the right to be free from searches and seizures is not absolute, the metadata collection program in its current form constitutes an unreasonable level of intrusion. The NSA points out that there are stringent oversight procedures[371] in place, but even with those, there have been significant compliance breaches[372] that seem unlikely to be fixed if the statute remains in its current form. By creating more transparency—even if that means just providing more detailed information to Congress—and limiting the number and types of records that can be obtained with one order, the objectives of the metadata program could be fulfilled while sacrificing less privacy.

CONCLUSION

Public opinion is changing and, as such, the law needs to be modified to account for those perceptions. Because technology is constantly evolving and plays such a significant role in our daily lives, the law needs to adapt to this shift and take a more expansive view of the expectation of privacy. It seems fairly clear that current Fourth Amendment precedent permits this type of surveillance, but the Court has indicated a willingness to potentially reconsider this structure.

Combined with the ambiguity of the terminology in 50 U.S.C. § 1861 and the far-reaching effects of the metadata collection program, it seems now is the perfect time to do just that. The term "relevant" cannot reasonably be understood to encompass the phone records of all Americans, but the national security interests that the program seeks to protect are still extremely important. Rather than discontinuing the program entirely, limitations need to be imposed that clearly delineate when and how records can be collected and data may be used.

370. This particular suggestion was also one of the forty-six recommendations advocated for by the presidential task force. *See supra* note 316 and accompanying text.

371. *See supra* note 232 and accompanying text.

372. *See supra* notes 145–49, 228 and accompanying text.