NOTE

ACLU v. Clapper: The Fourth Amendment in the Digital Age

ERIN E. CONNARE†

INTRODUCTION

On June 6, 2013, the British newspaper *The Guardian* published the first of several leaks of classified information regarding the United States Government's intelligence surveillance and collection programs.[1] A classified document, provided by former National Security Agency ("NSA") contract employee and whistleblower Edward Snowden,[2] revealed a Secondary Order issued by Judge Roger Vinson of the Foreign Intelligence Surveillance Court ("FISC") on April 25, 2013.[3] The FISC order, set to expire on July 19, 2013, compelled Verizon Business Network Services ("Verizon") to

† Executive Publications Editor, *Buffalo Law Review*; J.D. Candidate, 2015, SUNY Buffalo Law School; B.A. in Psychology and Social Sciences, SUNY at Buffalo. Very special thanks to my editor, Paul Bartlett, Ryan Ganzenmuller, and the members of the *Buffalo Law Review* for all of their hard work in readying my Note for publication. Finally, I would like to thank my family for their undying love and support, without which I would not be where I am today.

1. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

2. Glenn Greenwald, Ewen MacAskill & Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

3. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Secondary Order, BR 13-80 (FISA Ct. Apr. 25, 2013).

"produce . . . and continue production on an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[4] The order further provided that "no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order."[5] In response to *The Guardian*'s unauthorized disclosure, the U.S. Government confirmed the existence of the NSA's Bulk Telephony Metadata Collection Program ("the Program").[6] Shortly thereafter, *The Guardian* published additional information regarding secret NSA surveillance programs, including revealing the Internet data-collection program PRISM[7] and the data-mining tool Boundless Informant.[8]

These public revelations have led to the filing of several lawsuits.[9] This Note assesses *ACLU v. Clapper*, an action brought before the District Court for the Southern District of New York and decided by Judge William H. Pauley III on December 27, 2013.[10] In *Clapper*, the American Civil Liberties Union ("ACLU"), the American Civil Liberties Union Foundation, the New York Civil Liberties Union, and the New York Civil Liberties Foundation brought suit against several Executive Branch department and agency

4. *Id.* at 1-2. (omission added).

5. *Id.* at 2.

6. *See, e.g.*, ADMINISTRATION WHITE PAPER: BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT (Aug. 9, 2013), *available at* http://big.assets.huffingtonpost.com/Section215.pdf [hereinafter WHITE PAPER].

7. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, THE GUARDIAN (June 7, 2013), http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

8. Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.

9. *See, e.g.*, *In re* Elec. Privacy Info. Ctr., 134 S. Ct. 638 (2013); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

10. *Clapper*, 959 F. Supp. 2d at 724.

heads—Director of National Intelligence James Clapper, NSA Director and Central Security Service Chief Keith Alexander, Secretary of Defense Charles Hagel, Attorney General Eric Holder, and FBI Director James Comey.[11] Plaintiffs sought a declaratory judgment that: (1) the Program exceeded the statutory authority granted by Section 215 of the USA Patriot Act; and (2) the Program violated the First and Fourth Amendments of the United States Constitution.[12] In addition, Plaintiffs sought a permanent injunction enjoining the Government from continuing collection of their telephony metadata.[13] After an extremely in-depth analysis of the issues presented, Judge Pauley rejected Plaintiffs' claims and granted the Government's motion to dismiss.[14]

I. THE NSA'S BULK TELEPHONY METADATA COLLECTION PROGRAM

To fully comprehend Judge Pauley's ruling, it is important to understand just what exactly the Bulk Telephony Metadata Collection Program is and what it does. The Program's central purpose is terrorism prevention.[15] The Program operates under the "business records" provision of the Foreign Intelligence Surveillance Act ("FISA").[16] The business records provision of FISA allows the Director of the Federal Bureau of Investigation ("FBI"), or an authorized designee of the Director, to apply to the FISC for

> an order requiring the production of any "tangible things" for an investigation to obtain foreign intelligence information not concerning a United States person *or* to protect against

11. *Id.* at 730.

12. *Id.* at 735.

13. *Id.*

14. *See id.* at 757.

15. Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency ¶ 44, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-3994) [hereinafter Shea Declaration].

16. 50 U.S.C. § 1861(a)(1) (2012). This provision of FISA was enacted by Section 215 of the Patriot Act. USA Patriot Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272.

> international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution.[17]

These applications must include both "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation," and "an enumeration of the minimization procedures" in place.[18]

Since May 2006, the FBI has used Section 215 to obtain FISC orders directing designated telecommunications service providers to produce all business records created that contain information about communications between telephone identifiers relating to telephone calls made between the United States and a foreign country and those wholly within the United States.[19] The NSA collects pre-existing business records of the telecommunications providers, and does not itself create or record any of the information.[20] Since May 2006, at least fifteen different FISC judges have entered at least thirty-five such orders authorizing the NSA's bulk collection of telephony metadata.[21] The telephony metadata that FISC orders authorize the Government to collect include the telephone numbers that placed and received the call, other session-identifying information, trunk identifier, telephone calling card number, and the date, time, and duration of the call.[22] The FISC orders do not authorize the Government to collect the content of any call, nor the cell site locational

---

17. 50 U.S.C. § 1861(a)(1) (2012) (alterations added) (emphasis added).

18. *Id.* § 1861(b)(2)(A)-(B).

19. *Clapper*, 959 F. Supp. 2d at 734; Shea Declaration, *supra* note 15, ¶¶ 13-14.

20. Shea Declaration, *supra* note 15, ¶ 18.

21. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], Primary Order, BR 13-80 (FISA Ct. Apr. 25, 2013) [hereinafter Primary Order]; Declaration of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation ¶ 11, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-3994) [hereinafter Holley Declaration]; Shea Declaration, *supra* note 15, ¶ 14.

22. Shea Declaration, *supra* note 15, ¶ 15.

information, names, addresses, or financial information of any parties to any call.[23]

After receiving telephony metadata information from telecommunications providers, the NSA compiles and stores the information in one database under "carefully controlled circumstances" and may keep the information for up to five years.[24] The NSA may access the stored telephony metadata only through queries using metadata identifiers.[25] An identifier used to commence a query, called a "seed," must be approved by any of twenty-two designated officials.[26] To approve a seed, one of the approving officials must determine that "based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried" is in association with an international terrorist organization subject to an FBI investigation, but that association cannot be solely based on activities protected under the First Amendment.[27]

Analysis is not limited strictly to the approved identifier, but also extends to second- and third-tier contacts of the identifier, known as "hops."[28] The identifiers directly in contact with the seed identifier are contained in the first hop, those identifiers in direct contact with the first hop identifiers comprise the second hop, and those identifiers in direct contact with the second hop constitute the third hop.[29] NSA officials analyze this information to see which results

---

23. *Id.*

24. Primary Order, *supra* note 21, at 14; Shea Declaration, *supra* note 15, ¶¶ 16, 23, 30.

25. A common example of an identifier is a telephone number that is associated with a foreign terrorist organization. Shea Declaration, *supra* note 15, ¶ 19.

26. Primary Order, *supra* note 21, at 7; Shea Declaration, *supra* note 15, ¶ 20.

27. Primary Order, *supra* note 21, at 7. "The RAS requirement ensures an ordered and controlled querying of the collected data" and is intended "to prevent any general browsing of [such] data." Shea Declaration, *supra* note 15, ¶ 20.

28. Shea Declaration, *supra* note 15, ¶ 22.

29. *Id.*

are likely to be of investigative value to the FBI.[30] While extremely high volumes of data are collected pursuant to the Program, only a small percentage is reviewed by analysts.[31] If the FBI chooses to investigate a telephone number tipped to it through the Program, "the FBI must rely on publicly available information, other available intelligence, or other legal processes in order to identify the subscribers of any of the numbers that are retrieved."[32]

In accordance with Section 215, there are several minimization procedures in place to help control the Program.[33] First, the NSA stores and processes the metadata in repositories within secure networks, and access is permitted only for purposes allowed under the FISC's order.[34] Second, stored "metadata must be destroyed no later than five years after [its] initial collection."[35] Third, as previously noted, no one other than any of twenty-two designated officials "can make findings of RAS that a proposed seed identifier is associated with a *specified* terrorist organization."[36] And, for identifiers associated with United States persons, it must also be determined that the RAS finding "is not based solely on activities protected by the First

---

30. *Id.* ¶ 26.

31. *Id.* ¶ 5. In 2012, for example, "fewer than 300" unique identifiers met the RAS standard and were used as seeds to query data. *Id.* ¶ 24. While the number of metadata records responsive to these queries is not known, due to the three-tiered "hop" analysis, the number is "substantially larger than 300," but is still a very small percentage of the total metadata collected. *Id.*

32. WHITE PAPER, *supra* note 6, at 4. An example provided in the White Paper is of the FBI's use of

> a grand jury subpoena to a telephone company to obtain subscriber information for a telephone number. If . . . the FBI were able to develop probable cause to believe [the number] was being used by an agent of a foreign terrorist organization, the FBI could [then] apply to the FISC for an order under Title 1 of FISA to authorize interception of the contents of future communications to and from that telephone number.

Id. (alterations and omission added).

33. *See* 50 U.S.C. § 1861(g) (2012).

34. Shea Declaration, *supra* note 15, ¶ 30.

35. WHITE PAPER, *supra* note 6, at 5; Shea Declaration, *supra* note 15, ¶ 30.

36. Shea Declaration, *supra* note 15, ¶ 31 (emphasis added).

Amendment."[37] Fourth, "no [query] results may be disseminated outside of the NSA except in accordance with the minimization and dissemination requirements and established NSA procedures."[38] Prior to the dissemination of any United States person's information, one of a few high-ranking NSA officials "must determine that the information is *in fact* related to counterterrorism information, and is necessary to understand the counterterrorism information or assess its importance."[39] Fifth, the NSA uses "stringent and mutually reinforcing technological and personnel training measures to ensure that queries will be made only as to identifiers about which RAS has been established."[40] Sixth, the program is subject to both internal and external oversight.[41] Compliance issues identified by any of the overseeing parties are reported to the FISC, and significant compliance issues are reported to the Intelligence and Judiciary Committees of both houses of Congress.[42] Despite the various controls in effect, the Government has acknowledged and responded to compliance and implementation incidents that have taken place since the program's inception.[43]

II. *ACLU V. CLAPPER*

In *ACLU v. Clapper*, Judge Pauley opened his opinion with a brief recollection of the 9/11 terrorist attacks, focusing on calls made by 9/11 hijacker Khalid al-Mihdhar to an al-Qaeda safe house in Yemen that were intercepted by the

37. *Id.*

38. *Id.* ¶ 32.

39. *Id.* (emphasis added).

40. *Id.* ¶ 33. "Intelligence analysts receive comprehensive training on the minimization procedures applicable to the use, handling, and dissemination of the metadata, and technical controls that prevent NSA intelligence analysts from seeing any metadata unless as the result of a query using an approved identifier." *Id.*

41. *Id.* ¶ 34. For example, the Program is monitored by the Department of Justice, FISC, and Congress. *Id.*

42. *Id.* ¶ 35.

43. *See, e.g.*, WHITE PAPER, *supra* note 6.

NSA.[44] Judge Pauley went on to state that the intelligence used by the NSA did not capture Mihdhar's telephone number identifier, and as a result, the NSA mistakenly concluded Mihdhar was outside the United States.[45] "Learn[ing] from its mistake," the Government launched new intelligence counter-measures, including the Program.[46] Judge Pauley called the Program a "blunt tool," one that "only works because it collects everything" and that could "imperil[ ] the civil liberties of every citizen" if it was unrestrained.[47] According to Judge Pauley, the Program, despite highlighting the "natural tension between protecting the nation and preserving civil liberty," was lawful.[48]

Before launching into his discussion of the Program, Judge Pauley first discussed the Program's relevant background. Judge Pauley discussed the enactment of FISA in 1978 and its subsequent expansion by Section 215 of the USA Patriot Act in the aftermath of the 9/11 terrorist attacks.[49] He commented on the "extensive oversight" the Program is subjected to, the steps the Government must take to obtain judicial approval for its collection under the Program, and the reporting requirements the Government owes to the intelligence committees of the House and Senate.[50] The opinion also addressed the various compliance issues regarding the Program, but concluded the NSA reported the issues to the FISC and Congress and had since "addressed these problems."[51]

The first issue the court addressed in *Clapper* was whether Plaintiffs had standing to sue.[52] The requirement that plaintiffs first establish their standing to sue comes from

---

44. 959 F. Supp. 2d 724, 729 (S.D.N.Y. 2013).

45. *Id.*

46. *Id.* at 729-30.

47. *Id.* at 730.

48. *Id.*

49. *Id.* at 731-32.

50. *Id.* at 732.

51. *Id.*

52. *Id.* at 735-36.

the case-or-controversy requirement of Article III of the United States Constitution.[53] Article III standing requires that an injury be "concrete, particularized, and actual or imminent; fairly traceable to the defendant's challenged action; and redressable by a favorable ruling."[54] Plaintiffs alleged injury in the Government's collection of their telephony metadata, the search of the collected metadata resulting from any query by the NSA, and the chilling effect on the ACLU's potential and current clients who will not contact the ACLU because of the Government's collection.[55] The Government, in opposition, relied on the Supreme Court's recent decision in *Clapper v. Amnesty International*[56] and argued that none of Plaintiffs' alleged injuries met the requirements of Article III.[57] Judge Pauley, agreeing with Plaintiffs that they satisfied the standing requirement, distinguished *Amnesty International*. Unlike *Amnesty International*, which was decided before the Program was revealed,[58] there was "no dispute" that the Government collected Plaintiffs' telephony metadata, thus constituting actual injury.[59]

The court then addressed Plaintiffs' statutory claims. In particular, Plaintiffs claimed that the NSA exceeded its authority under FISA's "tangible things" provision in violation of the Administrative Procedure Act ("APA").[60]

---

53. *See* U.S. CONST. art. III, § 2.

54. Horne v. Flores, 557 U.S. 433, 445 (2009) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

55. *Clapper*, 959 F. Supp. 2d at 736.

56. 133 S. Ct. 1138, 1148 (2013) (holding plaintiffs' "highly speculative fear" that their communications would be intercepted was based on a "highly attenuated chain of possibilities" and thus insufficient to show the immanency required to establish injury in fact).

57. *Clapper*, 959 F. Supp. 2d at 736.

58. *Amnesty International* was decided on February 26, 2013, over three months before the first revelations about the NSA's Program. *See Amnesty Int'l*, 133 S. Ct. at 1138; *supra* Introduction.

59. *Clapper*, 959 F. Supp. 2d at 738.

60. *Id.* at 738-42. Section 706 of the APA provides, in relevant part, that a reviewing court "shall . . . hold unlawful and set aside agency action, findings, and

Pursuant to Section 702 of the APA, a person "suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action" is permitted to sue the United States for "relief other than money damages."[61] However, this waiver of sovereign immunity[62] can be overcome where "congressional intent to preclude judicial review is 'fairly discernible in the statutory scheme.'"[63] Congressional intent can be determined by examining specific language, specific legislative history, or inferences of intent drawn from the statutory scheme as a whole.[64]

Judge Pauley, examining the USA Patriot Act and FISA's overall statutory scheme, concluded that "Congress withdrew the APA's waiver of sovereign immunity for section 215."[65] Congress's concern, noted Judge Pauley, was to provide redress for policy violations in cases where the Government took steps to *generate* evidence, but not where the Government obtained evidence created solely in the ordinary course of business of a third party.[66] Even under Section 701 of the APA, which withdraws sovereign immunity "to the extent [the relevant] statutes preclude judicial review,"[67] Judge Pauley found support in FISA's statutory scheme that "section 215 does not provide for any person other than a recipient of an order to challenge the orders' legality or otherwise participate in the process," and to hold otherwise would "undermine the Government's vital interest" in the secrecy of the Program.[68]

---

conclusions found to be . . . in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706 (2012).

61. 5 U.S.C. § 702 (2012).

62. "The United States, as sovereign, is immune from suit unless it unequivocally consents to be sued." *Clapper*, 959 F. Supp. 2d at 738 (citing United States v. Mitchell, 445 U.S. 535, 538 (1980)).

63. Block v. Cmty. Nutrition Inst., 467 U.S. 340, 351 (1984).

64. *Clapper*, 959 F. Supp. 2d at 739 (quoting *Block*, 467 U.S. at 349).

65. *Id.* at 740.

66. *Id.*

67. 5 U.S.C. § 701 (2012).

68. *Clapper*, 959 F. Supp. 2d at 741 (citation omitted). Even more than undermining a vital Government interest, Judge Pauley would consider it absurd

Even though it decided Plaintiffs' statutory claims were precluded, the court assessed the merits of the claims. When seeking a preliminary injunction, plaintiffs must establish four things: that (1) they are likely to succeed on the merits; (2) they are likely to suffer irreparable harm in the absence of a preliminary injunction; (3) the balance of equities tips in their favor; and (4) an injunction is in the public interest.[69] The court held that Plaintiffs failed to demonstrate a likelihood of success on the merits of their statutory claim.[70] The court addressed Plaintiffs' contentions that Section 215 needed to be interpreted narrowly to avoid conflict with the Stored Communications Act ("SCA"), that collection under the Program was overbroad because it covered voluminous amounts of irrelevant data, and whether Congress ratified the Government's interpretation of Section 215.[71]

On the first matter, the court held that harmony between the SCA and Section 215 existed if the SCA was read to allow the collection of telephony metadata through Section 215 orders.[72] The SCA allows communication providers to divulge subscribers' records to government entities if the government obtains a warrant, an administrative subpoena, a grand jury or trial subpoena, an order issued under 18 U.S.C. § 2703, or a national security letter.[73] However, the records sought must always be "relevant" to an authorized investigation of international terrorist or clandestine intelligence activities.[74] Section 215, in similar fashion, permits the government to require the production of "tangible things" so long as the Government provides facts showing that there are reasonable grounds to believe the tangible things sought are "relevant" to a foreign intelligence investigation.[75] These

---

if the "lawbreaking conduct by a government contractor that reveals state secrets . . . could frustrate Congress's intent." *Id.* at 742.

69. *Id.* (quoting Winter v. Nat'l Res. Def. Council, 555 U.S. 7, 20 (2008)).

70. *Id.*

71. *Id.* at 742-49.

72. *Id.* at 743.

73. *See* 18 U.S.C. §§ 2701–12 (2012).

74. *See id*. § 2709(b)(1).

75. *See* 50 U.S.C. § 1861 (2012).

Section 215 orders, according to the court, are "functionally equivalent to grand jury subpoenas," and thus allowing such orders to be obtained is in harmony with the SCA.[76]

On the second matter—whether the Program was overbroad—the court employed a highly deferential stance in the Government's favor.[77] Tangible items are relevant, according to the court, if they bear on or could reasonably lead to other matter that could bear on the investigation.[78] The Program required the collection of "virtually all" telephony metadata in order to be comprehensive.[79] Since there was no way for the Government to know *in advance* what telephony metadata might lead to counterterrorism information, aggregated collections of the information was necessary.[80] The court concluded that telephony metadata, as a category, was relevant and thus not overbroad as Plaintiffs alleged.[81]

On the third matter, the court found that Congress had ratified the Government's interpretation of Section 215. Congress is presumed to be aware of a statute's interpretation, and to adopt that interpretation when it re-enacts a statute without change.[82] On a semi-annual basis, the Government must provide reports to the House and Senate intelligence and judiciary committees that include a summary of any significant FISC interpretations involving Section 215 matters and any FISC documents including significant constructions or interpretations of Section 215.[83] In 2010, the court noted, the Executive Branch produced a classified five-page document discussing the Program that was made available to the entire body of Congress.[84] An

76. *Clapper*, 959 F. Supp. 2d at 743.

77. *Id.* at 747.

78. *Id.* at 746.

79. *Id.*

80. *Id.* at 747.

81. *Id.* at 748.

82. *Id.* at 743-44 (quoting Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239-40 (2009)).

83. *See id.* at 744 (citing 50 U.S.C. § 1871 (2012)).

84. *Id.* at 744.

updated version of this document was made available again to the entire body of Congress in 2011.[85] In both 2010 and 2011, after the documents were made available, Congress re-authorized Section 215 without change.[86] This, according to the court, showed that Congress ratified the Executive's interpretation of Section 215.[87]

Despite finding that it could not hear Plaintiffs' statutory claims, the court was not precluded from addressing their constitutional claims.[88] Plaintiffs' Fourth Amendment claim was grounded in the idea that the Program's long-term recording and aggregation of telephony metadata invaded their reasonable expectation of privacy and thus constituted a search under the Fourth Amendment.[89] Plaintiffs concluded that this search violated the Fourth Amendment because it was warrantless and lacked any indicia of reasonableness.[90] Plaintiffs' First Amendment claim alleged that the Program violated their rights to private association and free speech.[91] The Program, according to Plaintiffs, "chill[ed]" their associational and expressive freedoms and exposed all of their (often-sensitive) contacts to Government monitoring.[92]

The court rejected Plaintiffs' Fourth Amendment argument. The Fourth Amendment guarantees the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[93] A search occurs under the Fourth Amendment when the Government violates a "subjective expectation of privacy that

85. *Id.* at 745.

86. *Id.* at 744.

87. *Id.* at 745.

88. *Id.* at 749.

89. *See, e.g.*, Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss at 26-29, ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (No. 13-cv-3994).

90. *See id.* at 26-35.

91. *See id.* at 35.

92. *See id.* at 35-40.

93. U.S. CONST. amend. IV.

society recognizes as reasonable."[94] Thus, the threshold Fourth Amendment question faced in *Clapper* was whether telephone subscribers have a reasonable expectation of privacy in their telephony metadata.[95] If the answer to this question was yes, a Fourth Amendment search occurred, and the inquiry turns to whether the individual's subjective expectation of privacy is one that society is willing to recognize as reasonable.[96]

The main focus of the court's Fourth Amendment analysis was the 1979 Supreme Court case *Smith v. Maryland*.[97] In *Smith*, the Supreme Court held that telephone subscribers have "no legitimate expectation of privacy" in the numbers they dial.[98] Telephone customers, *Smith* held, have no subjective expectation of privacy because they knowingly "convey numerical information to the phone company . . . [knowing] the phone company has facilities for recording this information . . . and [knowing] the phone company does in fact record this information for . . . business purposes."[99] Even if a telephone user *did* have a subjective expectation of privacy in the numbers dialed, continued the Court, this expectation was "not 'one that society is prepared to recognize as reasonable,'" because there is no legitimate expectation of privacy in information voluntarily turned over to third parties.[100]

Judge Pauley rejected Plaintiffs' contention that the Program allowed the "creation of a rich mosaic" that revealed deeply personal and intimate aspects of a person's life.[101]

---

94. Kyllo v. United States, 533 U.S. 27, 33 (2001) (citing Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

95. ACLU v. Clapper, 959 F. Supp. 2d 724, 749-52 (S.D.N.Y. 2013).

96. *See* Samson v. California, 547 U.S. 843, 848 (2006).

97. 442 U.S. 735 (1979); *see Clapper*, 959 F. Supp. 2d at 749-50.

98. *Smith*, 442 U.S. at 743.

99. *Id.* (alterations and omissions added).

100. *Id.* at 743-44 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

101. *Clapper*, 959 F. Supp. 2d at 750. In particular, Plaintiffs alleged the Program could "reveal a person's religion, political associations, use of a telephone-sex hotline, contemplation of suicide, addiction to gambling or drugs,

Judge Pauley pointed out that the NSA could not query the telephony metadata without additional legal justification, the information obtained when queries were performed only extended three hops from the identifier, and the NSA could not tell who the identifiers belonged to.[102] Judge Pauley also dismissed Plaintiffs' contentions that the Government could perform its three-hop analysis without building an aggregated database as "judicial-Monday-morning-quarterbacking."[103] Such after-the-fact evaluations were dangerous, according to the court, and there is no requirement that only the "least intrusive" searches are reasonable under the Fourth Amendment.[104]

Another problem the court had with Plaintiffs' Fourth Amendment argument was their "fundamental misapprehension" about ownership of the telephony metadata. The "tangible things" obtained by the FISC orders—the business records—were not Plaintiffs' records, but *Verizon's* records.[105] This distinction was important for the court, because it triggered the third-party doctrine,[106] under which a person forfeits his right to privacy in information voluntarily conveyed to third parties.[107] Additionally, since the records belong to Verizon—and not Plaintiffs—their subsequent querying did not implicate any Fourth Amendment interest of Plaintiffs.[108]

Finally, the court examined Plaintiffs' reliance on a recent case, *United States v. Jones*,[109] in the context of *Smith v. Maryland*. In *Jones*, the Supreme Court held that a search occurred where a GPS tracking device was attached, without a warrant, to a suspect's car and monitored for twenty-eight

---

experience with rape, grappling with sexuality, or support for particular political causes." *Id.*

102. *Id.* at 750-51.

103. *Id.* at 751.

104. *Id.* (quoting City of Ontario v. Quon, 560 U.S. 746, 763 (2010)).

105. *Id.*

106. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979).

107. *Id.* at 742-43.

108. *Clapper*, 959 F. Supp. 2d at 751.

109. 132 S. Ct. 945 (2012).

days.[110] The Court held that this constituted a search because it was a physical intrusion for the purpose of obtaining information.[111] Two concurring opinions, authored by Justices Alito and Sotomayor, found the surveillance also constituted a search because it invaded reasonable expectations of privacy.[112] Plaintiffs contended the search in *Clapper* was the same kind of search—if not more intrusive—as that considered by the concurring Justices, and that the court should follow the reasoning of the *Jones* concurrences, not *Smith*'s.[113]

In response to this argument, however, Judge Pauley pointed to the fact that *Jones* did *not* overrule *Smith*. If Supreme Court precedent has direct application to a case, even where it "appears to rest on reasons rejected in some other line of decisions," inferior courts "should follow the case which directly controls" and "leav[e] to [the Supreme] Court the prerogative of overruling its own decisions."[114] The Program does not violate the Fourth Amendment, Judge Pauley held, because *Smith*, as "[c]lear precedent," held that a telephone "subscriber has no legitimate expectation of privacy in telephony metadata created by third parties."[115] This result is not changed by the ubiquity of cell phones or the different relationship that exists between persons and their phones now as opposed to when *Smith* was decided.[116] The increase in the number of calls made and the versatility and multiple uses of cell phones do not change this result.[117]

---

110. *Id.* at 948-49.

111. *Id.* at 949.

112. *Id.* at 955-56 (Sotomayor, J., concurring) (finding individuals have a "reasonable societal expectation of privacy in the sum of [their] public movements" that is violated by continuous GPS monitoring); *id.* at 964 (Alito, J., concurring) ("the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.").

113. Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss, *supra* note 89, at 27-29.

114. Rodriguez de Quijas v. Shearson/American Exp., Inc., 490 U.S. 477, 484 (1989) (alterations added); *see also* Agostini v. Felton, 521 U.S. 203, 237 (1997).

115. ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

116. *Id.*

117. *Id.*

Most importantly, Judge Pauley acknowledged, "what metadata is has not changed over time . . . [a]s in *Smith*, the *types* of information at issue in this case are relatively limited: [tele]phone numbers dialed, date, time, and the like."[118] Since he found no search occurred, Judge Pauley did not address the question of reasonableness.[119]

Having concluded that no Fourth Amendment search occurred, Judge Pauley turned to address Plaintiffs' First Amendment claim.[120] Plaintiffs alleged that the Program violated the First Amendment because it was likely to have a "chilling effect" on individuals who would otherwise contact them.[121] The court, once again, rejected Plaintiffs' argument. First, the court agreed with the Government's position that "surveillance consistent with Fourth Amendment protections . . . does not violate First Amendment rights, even though it may be directed at communicative or associative activities."[122] The court further concluded that *Clapper v. Amnesty International* compelled the conclusion that the Program did not substantially burden First Amendment rights.[123] Like in *Amnesty International*, Plaintiffs' speculative "[f]ear that telephony metadata" would be queried "relie[d] on a highly attenuated chain of possibilities."[124] This fear was insufficient to establish a violation of First Amendment rights.[125]

The court thus concluded that Plaintiffs failed to state a claim and that their case must be dismissed. Before finishing

---

118. *Id.* (quoting Klayman v. Obama, 957 F. Supp. 2d 1, 35 (D.D.C. 2014)) (emphasis and alteration in original) (internal quotation marks omitted).

119. *Id.* at 749-52.

120. The First Amendment states, "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for redress of grievances." U.S. CONST. amend. I.

121. *Clapper*, 959 F. Supp. 2d at 753.

122. *Id.* (quoting Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983)) (omission in original).

123. *Id.* at 753-54.

124. *Id.* at 754 (quoting Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1148 (2012)) (alterations added).

125. *Id.*

his opinion, however, Judge Pauley engaged in a balancing of the equities and public interest to show that, even if Plaintiffs *could* show a likelihood of success on the merits, a preliminary injunction would still be inappropriate. The Government's interest in combating terrorism, he held, seriously outweighed any privacy interest Plaintiffs could point to, and "proper deference" was owed to the Government on the subject of national security.[126] While it was restricted on the information it could share, the Government offered illustrations of three situations in which the Program allegedly helped combat terrorism.[127] Judge Pauley found "ample justification" in these three examples, concluding the "effectiveness of bulk telephony metadata collection cannot be seriously disputed."[128]

In the conclusion of his opinion, Judge Pauley returned to where he started: the 9/11 terrorist attacks. By its own design, he noted, the Program "vacuums up" mass quantities of information so the Government can detect terrorist relationships and avoid tragic results like the 9/11 attacks.[129] The court's role was to "reject as false, claims in the name of civil liberty," like those brought by Plaintiffs, that would "paralyze or impair [the Government's] authority" to protect the nation.[130] The bigger danger to civil liberties, proffered Judge Pauley, was the success of a terrorist attack on American soil.[131] Thus, he concluded the Program was lawful and granted the Government's motion to dismiss.[132]

---

126. *Id.*

127. Holley Declaration, *supra* note 21, ¶¶ 24-26. For example, the NSA, through the Program, gave information to the FBI about an individual in Kansas City with ties to an overseas al-Qaeda extremist. Working off this tip, the FBI discovered a previously unknown plot to attack the New York Stock Exchange and identified and arrested several individuals involved. *Id.* ¶ 24.

128. *Clapper*, 959 F. Supp. 2d at 755.

129. *Id.* at 757.

130. *Id.* (alteration added).

131. *Id.*

132. *Id.*

III. *KLAYMAN V. OBAMA*

On January 2, 2014, the ACLU filed its notice of appeal to the Second Circuit.[133] On appeal, the most contested issue is likely to be whether the Program violates the Fourth Amendment. Despite Judge Pauley's ruling that the Program does not constitute a search under, and thus does not constitute a violation of, the Fourth Amendment, this view is not universally accepted. In fact, only eleven days before *Clapper* was decided, a case in the District Court of the District of Colombia, *Klayman v. Obama*, yielded a conflicting result.[134] As it did in *Clapper*, the Government relied on *Smith v. Maryland*, contending that no one has an expectation of privacy in the telephony metadata that telephone providers hold as business records.[135] Judge Leon, presiding over the case, concluded not only that the Program constituted a search that was likely unreasonable under the Fourth Amendment, but also that *Smith* could not adequately guide his decision.[136]

In fact, Judge Leon found the question he faced in *Klayman* to be a "far cry" from the question presented in *Smith* thirty-four years prior.[137] The question for Judge Leon was not "whether the installation and use of a pen register constitutes a 'search' within the meaning of the Fourth Amendment," but "when do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that

133. ACLU v. Clapper, 959 F. Supp. 2d 724, No. 13-cv-3994 (S.D.N.Y. Dec. 27, 2013), *appeal filed*, Notice of Appeal, No. 13-cv-3994 (2d Cir. Jan. 2, 2014).

134. 957 F. Supp. 2d 1 (D.D.C. 2013).

135. *See, e.g.*, Government Defendants' Opposition to Plaintiffs' Motions for Preliminary Injunctions at 46-47, Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (Nos. 1:13-cv-0851, 1:13-cv-0881).

136. *Klayman*, 957 F. Supp. 2d at 32-37.

137. *Id.* at 31.

a precedent like *Smith* simply does not apply?"[138] Judge Leon answered: "now."[139]

According to Judge Leon, the Government's present-day surveillance capabilities, citizens' phone habits, and the NSA's relationship with telecommunication companies had become "so thoroughly unlike" the situation faced in *Smith* that *Smith*'s precedent could no longer apply.[140] First, whereas the pen register used in *Smith* were in use "for only a matter of days,"[141] and there was no expectation that the records obtained through it would be retained after the investigation's finish, the NSA's program involved the creation of a historical database containing five years' worth of metadata and was potentially endless.[142]

Second, the relationship between the police and the phone company in *Smith* and the relationship between the NSA and telecom companies in the present case were vastly different. Whereas the phone company in *Smith* installed an individual pen register at the police's request, telecom companies, pursuant to FISC orders, must turn over call detail records to the NSA "*on a daily basis*," with order renewals happening frequently over several years.[143] For Judge Leon, this "formalized policy" permitting the "daily, all-encompassing, indiscriminate dump" of telephony metadata to the NSA went far beyond the individualized request for data seen in *Smith*.[144] The "almost-Orwellian" technology at issue in *Klayman* was "at best . . . the stuff of science fiction" when *Smith* was decided.[145]

Most importantly for Judge Leon was the vast difference in peoples' usage of and relationships with their personal

138. *Id.*

139. *Id.*

140. *Id.*

141. *Id.* at 32.

142. "[T]here is the very real prospect that the program will go on for as long as America is combating terrorism, which realistically could be forever!" *Id.*

143. *Id.* (emphasis in original).

144. *Id.* at 33.

145. *Id.* (omission added).

phones between 1979 and the present-day.[146] While conceding that what metadata is has not changed since 1979, Judge Leon found that the nature and quantity of the information contained in telephony metadata is much greater now than it was in 1979.[147] In addition to the drastic increase in the ubiquity of mobile phones, their use has drastically transformed as well, with mobile phones most often used as "multi-purpose devices."[148] According to Judge Leon, due to our now "phone-centric culture," telephony metadata has the potential to reveal "'a wealth of detail about [a person's] familial, political, professional, religious, and sexual associations'[149] . . . an entire mosaic—a vibrant and constantly updating picture of the person's life."[150] These "trends," Judge Leon proposed, have led to "*greater* expectation[s] of privacy and a recognition that society views [those] expectation[s] as reasonable."[151] In light of these Fourth Amendment violations, Judge Leon granted the *Klayman* plaintiffs' requests for a preliminary injunction, but stayed his order pending appeal.[152] On January 3, 2014, the Government filed its notice of appeal to the Circuit Court for the District of Colombia.[153]

IV. *CLAPPER* VERSUS *KLAYMAN*: WHO WAS RIGHT?

The conflicting opinions of *Clapper* and *Klayman* pose interesting questions. On appeal, should the Second Circuit adhere to Judge Pauley's reasoning on the Fourth Amendment issue and affirm, or should it adopt the

146. *Id.* at 33-34.

147. *Id.* at 34-35.

148. *Id.* at 34 ("They are now maps and music players. . . . [t]hey are cameras. . . . [t]hey are even lighters people hold up at rock concerts.").

149. *Id.* at 36 (quoting United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)) (alteration added).

150. *Id.*

151. *Id.* (alterations added) (emphasis in original).

152. *Id.* at 9-10.

153. Klayman v. Obama, 957 F. Supp. 2d 1, Nos. 1:13-cv-00851, 1:13-cv-00881 (D.D.C. Dec. 16, 2013), *appeal filed*, Government Defendants' Notice of Appeal, Nos. 1:13-cv-00851, 1:13-cv-00881 (D.C. Cir. Jan. 3, 2014).

reasoning of Judge Leon? The answer is not clear-cut, but the argument weighs in Judge Pauley's favor. Even so, the concerns echoed in *Klayman* must not be ignored.

As articulated by Judge Pauley, Supreme Court precedent binds inferior courts.[154] If Supreme Court precedent has direct application to a case, even where it "appears to rest on reasons rejected in some other line of decisions," inferior courts should follow the controlling case.[155] Since the information obtained through the Program is the same information obtained in *Smith*, its application is clear: the NSA's collection of telephony metadata is "squarely controlled" by *Smith*.[156] Like a pen register, the Program does not obtain the contents of communications or locational information.[157] The Program merely obtains the telephone numbers that have been dialed, when the call occurred, and the length of the call.[158]

Some, like the *Klayman* and *Clapper* plaintiffs, seem to suggest that *Smith*'s holding has been eroded by the Supreme Court's recent decision in *United States v. Jones*.[159] However, the Program does not present the same issue as that addressed in *Jones*. *Jones* considered the constitutionality of attaching a GPS device to a suspect's vehicle and monitoring the vehicle's movement over a twenty-eight-day period.[160] The Court unanimously agreed this constituted a search, but the majority concluded only on the basis that this was a physical trespass.[161] The *Jones* Court declined to address the question

154. ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).

155. *See* Rodriguez de Quijas v. Shearson/American Exp., Inc., 490 U.S. 477, 484 (1989) (alterations added); *see also* Agostini v. Felton, 521 U.S. 203, 237 (1997).

156. *See In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], BR 13-109, at 6 (FISA Ct. Aug. 29, 2013).

157. *But see* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law*, *Not Fact*, 70 MD. L. REV. 681 (2011) (arguing that cell phone users have a reasonable expectation of privacy in their cell phone location data under the Fourth Amendment).

158. *See supra* Part I.

159. *See* Plaintiffs' Memorandum of Law in Opposition to Defendants' Motion to Dismiss, *supra* note 89, at 27-29.

160. *See* United States v. Jones, 132 S. Ct. 945, 948-49 (2012).

161. *Id.* at 949-50.

of whether such long-term tracking would constitute a search *absent* physical trespass.

In her concurring opinion, Justice Sotomayor opined that long term monitoring infringes upon an individual's reasonable expectation of privacy, and thus constitutes a search under the Fourth Amendment. Long-term monitoring, she said, "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[162] While the *Jones* concurrences appeared to suggest changing technologies might lead to increased expectations of privacy under the Fourth Amendment,[163] this suggestion neither controlled the court nor undermined *Smith*. *Smith* has still not been eroded with respect to numbers dialed, and has in fact been extended to a degree.[164]

In her concurrence, Justice Sotomayor also criticized the third-party doctrine as "ill suited [sic] to the digital age."[165] Despite facing criticism, the third-party doctrine—one of the key underpinnings of *Smith*—has not been discarded.[166] The principle that individuals who voluntarily disclose information to third parties lose Fourth Amendment protection, as echoed in *Smith*, stands firm. Just as in 1979, telephone subscribers voluntarily disclose the numbers they dial to their telephone companies. Just as in 1979, telephone

---

162. *Id.* at 955 (Sotomayor, J., concurring).

163. *See id.* at 955-56 (Sotomayor, J., concurring) (arguing that individuals have a "reasonable societal expectation of privacy in the sum of [their] public movements" that is violated by continuous GPS monitoring) (alteration added); *id.* at 964 (Alito, J., concurring) (arguing that "the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy").

164. *See* United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (holding, in light of *Smith*, that e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the website they visit because they voluntarily turn that information over to third parties).

165. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

166. *See, e.g.*, Jeremy H. Rothstein, *Track Me Maybe: The Fourth Amendment and the Use of Cell Phone Tracking to Facilitate Arrest*, 81 FORDHAM L. REV. 489, 506-10 (2012) ("*Smith* remains strong as applied to information analogous to numbers dialed . . . .").

subscribers *should* know that their telephone providers have the facilities for recording that information. Just as in 1979, telephone subscribers *should* know that their telephone provider would record that information for business purposes. Where, as here, telephone subscribers should reasonably know their telephone providers will record this information in the ordinary course of business, they cannot legitimately expect privacy. And, where there is no subjectively reasonable expectation of privacy, no Fourth Amendment search has occurred. And, where one individual does not have a Fourth Amendment interest, grouping together numerous similarly situated individuals will not create a Fourth Amendment interest "*ex nihilo*."[167]

However, in today's digital age, it would be nearly *impossible* for an individual to enjoy use of their cell phone without needing to go through a third-party cell phone provider. Furthermore, in today's digital age, it would be foolhardy to suggest that an individual forego use of his cell phone in order to retain protection under the Fourth Amendment. Cell phones are more than just casual means of communication: they are maps, music players, business planners, and cameras. While Supreme Court precedent demands the result that cell phone users relinquish Fourth Amendment protection in their telephony metadata through use of a cell phone provider, this result only serves to underscore the outdated state of Fourth Amendment jurisprudence.

CONCLUSION

In *Clapper*, the court refused to ignore the important national security interest in fighting terrorism and dismantle a vital tool for identifying terrorist threats. In *Clapper*, the court refused to substitute its own judgment for that of the at least fifteen FISC judges who concluded the Program was lawful on at least fifteen occasions.[168] In *Clapper*, the court refused to depart from binding Supreme Court precedent and

167. *In re* Application of the FBI for an Order Requiring the Prod. of Tangible Things from [REDACTED], Docket No. BR 13-109, at 9 (FISA Ct. Aug. 29, 2013).

168. ACLU v. Clapper, 959 F. Supp. 2d 724, 756 (S.D.N.Y. 2013).

predict whether the Supreme Court would later overrule a precedent.

In light of existing Fourth Amendment jurisprudence, *Clapper* was correctly decided. However, what *Clapper* demonstrates, more than anything, is the need to revisit Fourth Amendment protection in light of changing technology. Intervention—whether by the Supreme Court, Congress, or the Executive itself—is needed. Until then, some peace of mind can be found in the fact that the Program concerns contentless information. As previously explained, the Program only obtains the ten-digit telephone numbers on the dialing and receiving ends of a call, when the call occurred, and how long the call lasted. There is no identifying or locational information collected by the Program. And, in order to use the information collected to achieve such a goal, additional legal and investigative moves would need to be taken by the FBI or other investigating agency. In light of these additional—and heavily restricted—steps, it appears impossible for the Program to create a "record of a person's public movements" that is detailed enough to reveal intimate details of a person's life.[169]

Only time will tell if the Supreme Court will step in and settle the debate, if Congress will change the laws upon which the Program is grounded, or if the Executive will alter the Program to increase oversight and transparency. Until then, *Clapper* should be limited to its facts and must not be extended to other types of intelligence surveillance, such as those that would include content information.

169. *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).