Klayman v. Obama: The D.C. District Court Misinterprets the NSA Metadata Collection Program as a Violation of Individual Fourth Amendment Rights

I. OVERVIEW

An unauthorized disclosure of classified material by former National Security Agency (NSA) contractor Edward Snowden exposed a July 2013 United States Foreign Intelligence Surveillance Court (FISC) order requiring Verizon Business Network Services (Verizon) to transfer "daily . . . call detail records" to the intelligence agency.[1] Subsequent declassification of the FISC order revealed the collection of telephone metadata was backed by a foreign intelligence surveillance statute, which permits access to business records for foreign intelligence and international terrorism investigations pursuant to the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).[2] The seven-year-old program continuously "consolidates the metadata records provided . . . into one database" from which searches for terror-related communications can be made given that "reasonable, articulable

1. Klayman v. Obama, 957 F. Supp. 2d 1, 10 (D.D.C. 2013) (quoting Secondary Order at 2, *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc., No. BR 13–80 (FISC Apr. 25, 2013)); Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

2. Metadata is "information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted." *Klayman*, 957 F. Supp. 2d at 14 (citing Primary Order at 3 n.1, *In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 13–158 (FISC Oct. 11, 2013)); 50 U.S.C. § 1861 (2012); *Klayman*, 957 F. Supp. 2d at 10; Secondary Order, *supra* note 1, at 1.

suspicion" exists.[3] Full declassification of the program led to the legal involvement of the political advocacy group Freedom Watch.[4]

The pair of lawsuits that followed (combined into the noted case by joinder) alleged "a secret and illegal government scheme to intercept and analyze vast quantities of domestic telephonic communications" and "communications from the Internet and electronic service providers."[5] While both suits were brought by a class of "subscribers, users, [and] customers" headed by Freedom Watch founder and public interest attorney Larry Klayman, the first suit targeted the NSA and Verizon and requested an injunction preventing further violation of individual rights under the Fourth Amendment.[6] The United States District Court for the District of Columbia *held* that the NSA's metadata collection program is "indiscriminate" and an "arbitrary invasion" amounting to a violation of the Fourth Amendment's protection against unreasonable searches and seizures. *Klayman v. Obama*, 957 F. Supp. 2d 1, 42 (D.D.C. 2013).

II. BACKGROUND

A. FISA and the USA PATRIOT Act as Statutory Backing

More than forty years ago, the United States Supreme Court made a distinction between "criminal surveillances and those involving domestic security," signaling to the United States Congress the need for "protective standards for the latter" to be considered.[7] As a result, the Foreign

---

3. *Klayman*, 957 F. Supp. 2d at 14-15 (citing Declaration of Teresa H. Shea, Signals Intelligence Director, National Security Agency ¶ 23, *Klayman*, 957 F. Supp. 2d 1 (No. 13–0851 (RJL)) [hereinafter Shea Declaration]); *id.* at 16 (quoting Declaration of Acting Assistant Director Robert J. Holley, Federal Bureau of Investigation ¶¶ 15-16, *Klayman*, 957 F. Supp. 2d 1 (No. 13-0851 (RJL)) [hereinafter Holley Declaration]). "Through [these] targeted computerized searches . . . the NSA tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States." *Id.* at 15 (citing Holley Declaration, *supra*, ¶ 5; Shea Declaration, *supra*, ¶¶ 8-10, 44). The communications sought are (1) domestic numbers calling foreign terror-linked numbers, (2) foreign terror-linked numbers calling the United States, and (3) "possible terrorist-related communications" between domestic numbers. *Id.* at 18 (quoting Shea Declaration, *supra*, ¶ 44).

4. "Freedom Watch will not stand by and 'watch' the rights of American citizens be abused by the government and our legal system and will have and will take strong action to protect the privacy of our citizens here and around the world." *Issues*, FREEDOM WATCH, http://www.freedomwatchusa.org/issues (last visited Sept. 10, 2014, 4:45 PM).

5. *Klayman*, 957 F. Supp. 2d at 11 (quoting Second Amended Complaint ¶ 2, *Klayman*, 957 F. Supp. 2d (No. 13–851)); *id.* (quoting Amended Complaint ¶ 2, *Klayman*, 957 F. Supp. 2d 1 (No. 13–881)).

6. *Id.* (citing Second Amended Complaint, *supra* note 5, ¶¶ 1, 99). Violation of the Administrative Procedure Act (APA) was also alleged but the Court held the claim lacked subject matter jurisdiction. *Id.* at 19-20.

7. United States v. U.S. Dist. Ct. for E. Dist. of Mich. (*Keith*), 407 U.S. 297, 322 (1972).

Intelligence Surveillance Act of 1978 (FISA) was enacted to "authorize electronic surveillance to obtain foreign intelligence information."[8]

The statute "require[d] the Government to obtain warrants or court orders for certain foreign intelligence surveillance activities and created the FISC" to evaluate such applications.[9] Since the court's establishment, FISC proceedings have been secret unless declassified, given that the panel of judges hears subject matter almost exclusively concerning matters of national security.[10] Inherently, such lack of transparency has been questioned; however, the court has only seen its powers expanded in recent years.[11]

The Intelligence Authorization Act for Fiscal Year 1999 inserted a new section into FISA titled Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations.[12] Title V's supplement to FISA authorized access to such records as long as the application provided "specific and articulable facts giving reason to believe that the person to whom the records pertain [was an] agent of a foreign power."[13]

Title V powers further expanded after the September 11, 2001, domestic terrorist attacks and subsequent USA PATRIOT Act legislation. The Act, implemented to "deter . . . terrorist acts in the United States and . . . enhance law enforcement investigatory tools," replaced the existing Title V provisions completely, authorizing access to business records in "investigation to protect against 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 [First Amendment]."[14]

Allowances of the USA PATRIOT Act were narrowed by amendment in 2006, when Congress replaced the provision requiring that FISC applications "specify . . . the records concerned [were] sought for" with a requisite "statement of facts showing . . . reasonable grounds to

---

8. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

9. ACLU v. Clapper, 959 F. Supp. 2d 724, 731 (S.D.N.Y. 2013); *see* 50 U.S.C. § 1803 (2012).

10. *See* 50 U.S.C. § 1803(c).

11. *See* S. REP. NO. 108-40, 108th Cong., 1st Sess. (2003).

12. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2396, 2410 (1998).

13. *Id.* § 502.

14. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, § 501(a)(1), 115 Stat. 287 (2001).

believe the tangible things sought are relevant to . . . protect against international terrorism or clandestine intelligence activities."[15]

The current version of the statute, in force since March 2006, further imposes the requirement that applications for business records contain "minimization procedures" for the "retention and dissemination . . . of any tangible things to be made available."[16] Such minimization is defined as

> specific procedures . . . reasonably designed in light of the purpose . . . of an order . . . to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting [citizens] consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.[17]

For such an order to be approved and the "tangible things released," an FISC judge must find that both the reasonable grounds and the minimization procedures are met.[18]

The USA PATRIOT Improvement and Reauthorization Act of 2005 also implemented a system of judicial review, which allows a "person receiving an order to produce any tangible thing [to] challenge the legality of that order."[19] Petitions for review are screened by a pool of three FISC judges and are granted only if the order is found to either be unlawful or violate the statute's requirements.[20] Following a ruling on the petition, further petitions to the FISC Court of Review for either an en banc hearing or appeal may follow.[21] Any petition for appeal of the review court's written decision must be made to the Supreme Court.[22]

B. Metadata Collection Program as a Search

The Fourth Amendment provides individuals "[t]he right . . . to be secure in their persons, houses, papers, and effects, against unreasonable

---

15. 50 U.S.C. § 1861; USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(b), 120 Stat. 192 (2001).

16. In force by means of the USA PATRIOT Improvement and Reauthorization Act of 2005, the USA PATRIOT—Extension of Sunsets Act of 2010 (Pub. L. No. 111-141, 124 Stat. 37), FISA Sunsets Extension Act of 2011 (Pub. L. No. 112-3, 125 Stat. 5), and the PATRIOT Sunsets Extension Act of 2011 (Pub. L. 112-14, 125 Stat. 216) making the statute effective through June 1, 2015. 50 U.S.C. § 1861(b)(2)(B).

17. 50 U.S.C. § 1861(g)(2)(A).

18. *Id.* § 1861(c)(1).

19. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106(f), 120 Stat. 198.

20. 50 U.S.C. §§ 1803(e)(1), 1861(f)(2)(B).

21. *Id.* §§ 1803(a)(2)(A), 1861(f)(3).

22. *Id.* §§ 1803(b), 1861(f)(3).

searches and seizures."[23] In the Supreme Court case *Katz v. United States*, Justice Harlan defined a "search" with regard to the Fourth Amendment as a violation of an individual's "constitutionally protected reasonable expectation of privacy."[24]

In *Smith v. Maryland*, the Supreme Court addressed the constitutionality of the warrantless use of a pen register—a "device or process that traces outgoing signals from a specific phone . . . produc[ing] a list of the phone numbers . . . contacted, but does not include substantive information transmitted."[25] The telephone company in *Smith*, like Verizon in the noted case, recorded numbers dialed from an individual's telephone at the request of law enforcement.[26] Justice Blackmun's majority concluded that "[g]iven a pen register's limited capabilities," their use does not constitute a Fourth Amendment search as defined by Justice Harlan in *Katz*, due to the absence of a "legitimate expectation of privacy" in numbers telephone users dial.[27]

The *Smith* opinion, while more than thirty years old, has served as a "bedrock holding" with regard to information individuals voluntarily provide to third parties and is the primary case against which challenges to the NSA's metadata collection program are construed.[28]

III. THE COURT'S DECISION

In the noted case, the D.C. District Court contrasted the issue at present with the framework laid by the Supreme Court in *Smith* in evaluating the constitutionality of government collection of telephone metadata.[29] While both courts sought to address whether warrantless law enforcement collection of numbers dialed from individuals' telephones constitutes an unreasonable Fourth Amendment search, the court in the noted case distinguished the issue from *Smith*, finding that a search occurred in the context of the Fourth Amendment.[30] After Judge Leon found a search to have occurred, he further evaluated the balance

---

23. U.S. CONST. amend. IV.

24. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

25. Smith v. Maryland, 442 U.S. 735 (1979); *Pen Register*, LEGAL INFO. INST., http://www.law.cornell.edu/wex/pen_register (last visited Sept. 4, 2014).

26. *Smith*, 442 U.S. at 737.

27. *Id.* at 742-43 ("All telephone users realize that they must 'convey' phone numbers to the telephone company, . . . that the phone company has facilities for making permanent records of the numbers they dial, . . . and that the phone company does in fact record this information.").

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

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

30. *Id.* at 29, 31, 37 ("[The] question that the Supreme Court confronted in *Smith* . . . is a far cry from the issue in this case."); *see Smith* 442 U.S. at 737.

between individual privacy expectations and government counter-terrorism efforts in concluding that such a "search" is unreasonable.[31]

Despite the D.C. District Court's acknowledgment that the Supreme Court's *Smith* decision determined that individuals have "no reasonable expectation of privacy in [phone] numbers dialed . . . because [they are] voluntarily transmitted . . . to [the] phone company," Judge Leon first distinguished the issue in the noted case.[32]

> Indeed, the question in this case can more properly be styled as follows: 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 a precedent like *Smith* simply does not apply?[33]

The court found the "landmark opinion" to not apply on the premise of four distinctions.[34] First, short-term metadata collection in *Smith* as opposed to the NSA program that could "go on for as long as America is combatting terrorism, which realistically could be forever!"[35] Second, phone company metadata collection and subsequent transfer to law enforcement as opposed to government creation of a "formalized policy" under which the phone company collects metadata for law enforcement.[36] Third, use of metadata on a "small-scale investigation" basis as opposed to the "almost-Orwellian" large-scale NSA collection of metadata.[37] Fourth, and "most importantly," modern metadata collection, storage, and analysis capabilities as opposed to those in 1979.[38] Despite admittance that "what metadata is has not changed over time," Judge Leon ultimately concluded that given the increased "quantity of information that is now available and . . . what that information can tell the Government about people's lives," it is "significantly likely" that the NSA program constitutes a Fourth Amendment search.[39]

The court's evaluation of whether such a "search" is unreasonable contrasted individual privacy expectations against the government's "special needs" (counterterrorism efforts) through consideration of two

---

31. *Klayman*, 957 F. Supp. 2d at 39, 42.
32. *Id.* at 30-31 (citing *Smith*, 442 U.S. at 742-44).
33. *Id.* at 31.
34. *Id.* at 30.
35. *Id.* at 32.
36. *Id.* at 33.
37. *Id.*
38. *Id.* at 33-34.
39. *Id.* at 35-37.

factors.[40] First, as established in the contrasting of *Smith*, the "nature of the privacy interest allegedly compromised" and "the character of the intrusion imposed" were held to be "very significant."[41] Second, the "nature and immediacy of the government's concerns and the [search's] efficacy . . . in meeting them" were deemed insufficient given the government's emphasis on "rapidly detect[ing]" terror threats and the subsequent finding that none of the attacks prevented "involved any apparent urgency."[42]

Judge Leon ultimately found that taken together, such an "indiscriminate" program "surely" constitutes an infringement on individual privacy rights promised in the Fourth Amendment.[43]

IV. ANALYSIS

Apart from conflicting with precedent, the D.C. District Court's finding that the NSA metadata collection program is an "arbitrary invasion" of privacy seems misguided given the limited and unchanged nature of telephone metadata and the immense importance of domestic counterterrorism efforts.[44]

A. Smith *as Indistinguishable Precedent*

Distinguishing the noted case from *Smith* on the basis of the pen register being "operational for only a matter of days" or used on a "small-scale investigation" basis holds no weight.[45] As the United States District Court for the Southern District of New York noted in *American Civil Liberties Union v. Clapper*, "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[46] Regardless of the amount of metadata collected or the length of the collection, the Supreme Court made clear in *Smith* that "[t]he installation and use of a pen register [is] not a search."[47]

---

40. *Id.* at 38 (citing Bd. of Educ. v. Earls, 536 U.S. 822, 830-34 (2002)).
41. *Id.* at 38-39 (quoting *Earls*, 536 U.S. at 830, 832).
42. *Id.* at 39-40 (quoting *Earls*, 536 U.S. at 834; Shea Declaration, *supra* note 3, ¶ 46).
43. *Id.* at 42.
44. *Id.* at 41-42 ("I realize, of course, that such a holding might appear to conflict with other trial courts.").
45. *See id.* at 32-33.
46. ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (referencing United States v. Dionisio, 410 U.S. 1, 13 (1973) ("Where single grand jury subpoena did not constitute unreasonable seizure, it could not be 'rendered unreasonable by the fact that may others were subjected to the same compulsion.'")).
47. Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

In finding a "search" regardless, the noted case contends that modern metadata collection and pen register use are discernible given "the nature and quantity of the information contained in people's [modern] metadata is much greater"[48]—this despite Judge Leon subsequently finding that "what metadata *is* has not changed over time."[49] His ad nauseam statistical assurance that "there [has been] a whopping [increase in] mobile subscriber connections in the United States" over the past thirty-plus years and notes that cell phones "are now maps and music players" and have "even [become] lighters that people hold up at rock concerts" are irrelevant.[50] Metadata collected by the NSA (just as in *Smith*) consists of "what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted."[51] Though Judge Leon draws a link between the increased quantities of metadata available and "what that information can tell the Government about people's lives," the concern is unnecessary—"the Government does not know who any of the telephone numbers belong to[, rather,] all the Government sees is that telephone number A called telephone number B. It does not know who subscribes to telephone numbers A or B."[52] Again as noted in *Clapper*, this issue only concerns telephones used as telephones—"[t]he fact that there are more calls placed does not undermine the Supreme Court's finding [in *Smith*] that a person has no subjective expectation of privacy in . . . metadata."[53]

Given consensus acceptance of the government's explanation of the program's operation, there is no question that the D.C. District Court misinterpreted it as a Fourth Amendment "search."[54]

---

48. *Klayman*, 957 F. Supp. 2d at 33-34.

49. *Id.* at 35.

50. *See id.* at 34.

51. *Id.* at 14 (citing Holley Declaration, *supra* note 3, ¶ 5; Shea Declaration, *supra* note 3, ¶ 7).

52. *Id.* at 36; ACLU v. Clapper, 959 F. Supp. 2d 724, 751 (S.D.N.Y. 2013).

53. *Clapper*, 959 F. Supp. 2d at 752.

54. *See id.* at 751 n.17 ("[Government] testimony on this point is crystal clear: '[they] are not authorized to go into the data, nor are [they] data mining, or doing anything with the data other than [authorized searches], period. [They]'re not authorized to do it. [They] aren't doing it.'" (quoting *How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Adversaries: Hearing Before the H. Permanent Select Comm. on Intelligence*, 113th Cong. 66 (2013) (testimony of General Keith Alexander, Dir., National Security Agency) [hereinafter Alexander Testimony]); *see also* United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009) ("'[C]all origination, length, and time of call' [data] encompasses the information collected by [a] pen register [and thus] there is no Fourth Amendment 'expectation of privacy.'").

B. Domestic Counterterrorism as a Special Need

The court's determination that domestic counterterrorism efforts are not a "special need" relied in part on the misguided finding that "a very significant expectation of privacy [is violated] in an aggregated collection of . . . metadata."[55] However, it also relied on a finding that the nature and immediacy of domestic terrorism concerns and the program's effectiveness are insufficient.[56]

Though Judge Leon notes that "identifying unknown terrorist operatives and preventing terrorist attacks" is "an interest that everyone . . . agrees is 'of the highest order of magnitude,'" he misconstrues the government's primary interest as being "not merely to investigate potential terrorists, but rather, to do so *faster* than other investigative methods might allow."[57] However, the notion seems paradoxical given that the program's requisite efficacy as a "special need" relies on its ability to rapidly process metadata.[58] What Judge Leon describes as the government's central interest in investigating potential terror threats "*faster* than other investigative methods" is more aptly categorized as an interest in preventing domestic terror attacks they might otherwise be unable to prevent.[59] FISA Title V powers expanded after September 11, 2001, for just this reason: "Prior to September 11th, [the] NSA did not have [such] capability. '[The Government] couldn't connect the dots because [they] didn't have the dots.'"[60]

Though Judge Leon's holding ultimately rested upon his "serious doubts about the efficacy of the metadata collection program" given "the utter lack of evidence that a terrorist attack has ever been prevented" by it, labeling the program as ineffective given the unsettling nature of immediate modern domestic terrorism threats would be in haste.[61]

In effect, and assuming *arguendo* that such analysis of the program's reasonableness as a search should even be considered, the court's decision infers that a privacy expectation already rejected by the Supreme Court outweighs the nature and immediacy of domestic

---

55. *Klayman*, 957 F. Supp. 2d at 39.

56. *See id.* at 37-41.

57. *Id.* at 39-40 (quoting *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008)).

58. *See Clapper*, 959 F. Supp. 2d at 748.

59. *Id.* ("This new ability to query aggregated . . . metadata significantly increases the NSA's [ability] to detect the faintest patterns left behind by individuals affiliated with foreign terrorist organizations."); Shea Declaration, *supra* note 3, ¶¶ 46, 48.

60. *Clapper*, 959 F. Supp. 2d at 748 n.15 (quoting Alexander Testimony, *supra* note 54, at 61).

61. *Klayman*, 957 F. Supp. at 40-41.

terrorism concerns—a dangerous precedent given "[i]t is obvious and unarguable that no governmental interest is more compelling than the security of the Nation."[62]

Joshua M. Mastracci*

62. *See id.* at 39 (quoting Haig v. Agee, 453 U.S. 280, 307 (1981)); *see also* Smith v. Maryland, 442 U.S. 735, 742 (1979).

* © 2014 Joshua M. Mastracci. Junior Member, Volume 17, *Tulane Journal of Technology and Intellectual Property.* J.D. candidate 2016, Tulane University Law School; B.A. 2013, Economics, Boston College. The author would like to thank his family for their support and the editors of the *Tulane Journal of Technology and Intellectual Property*.