Northern Illinois University Law Review

Volume 34 | Issue 3 Article 5

7-1-2014

Modern Private Data Collection and National Security Agency Surveillance: A Comprehensive Package of Solutions Addressing Domestic Surveillance Concerns

Shaina Kalanges

Modern Private Data Collection and National Security Agency Surveillance: A Comprehensive Package of Solutions Addressing Domestic Surveillance Concerns

"The advancement and diffusion of knowledge is the only guardian of true liberty." – James Madison[1]

1. STEVE COFFMAN, WORDS OF THE FOUNDING FATHERS: SELECTED QUOTATIONS OF FRANKLIN, WASHINGTON, ADAMS, JEFFERSON, MADISON AND HAMILTON, WITH SOURCES 127 (2012); *The Daily Show* (Comedy Central television broadcast 2013) (commenting on NSA surveillance practices stating, "[i]t's like Benjamin Franklin once said: 'Those who would trade liberty for security should never find out that that decision has already been made for them'").

I. INTRODUCTION

Section 702 of the Foreign Intelligence Surveillance Act (FISA) mandates warrantless electronic surveillance of suspected foreign communications by the National Security Agency (NSA).[2] Section 215 of the 2001 USA Patriot Act,[3] an amendment to FISA, also allows for a sweeping collection of domestic and foreign business records from private phone companies, to be queried with a deferential showing of the information's relevance to foreign intelligence.[4] The NSA may accordingly subpoena and buy data stored by private companies to conduct mechanical searches to find foreign intelligence.[5] Meanwhile, companies like Facebook and Google sell analyzed information on individuals to advertisement companies, while research empires create massive data collection and analysis systems targeting consumers.[6] Like these social networking websites and search engines, a private corporation, Apple, is gathering personal information from Siri requests and storing it in Apple's "data farm."[7] Siri requests and information are stored for two years while the NSA's telephony metadata surveillance program[8] stores business communication records for up to five

---

2. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (1978), *amended by* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act), 50 U.S.C.A. § 1881 (West 2008).

3. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, *amended by* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001, 50 U.S.C. § 1861 (2001).

4. *Compare* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (rejecting the proposition that the telephony metadata collection program is unconstitutional), *with* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013) (holding the telephony metadata surveillance program unconstitutional).

5. *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1941 (2013).

6. *See id.*

7. *See* Robert McMillan*, Apple Finally Reveals How Long Siri Keeps your Data*, WIRED (Apr. 19, 2013); Nick Hide, *Apple Keeps your Recorded Siri Questions on File for Two Years*, CNET UK (Apr. 19, 2013, 4:02 PM), http://crave.cnet.co.uk/mobiles/apple-keeps-your-recorded-siri-questions-on-file-for-two-years-50010987/; Patrick C. Toomey, *'Let's Put the Whole Elephant out There': President Obama's Speech and Bulk Searches of Americans' Emails*, ACLU BLOG (Aug. 12, 2013, 6:21 PM), http://www.aclu.org/blog/national-security/lets-put-whole-elephant-out-there-president-obamas-speech-and-bulk-searches.

8. Telephony metadata collection describes bulk collection and analysis of information pertaining to virtually every phone call a person targeted for foreign surveillance makes. This includes the duration of calls, phone numbers, dates, and times. This infor-

years.[9] Also, Apple did not openly inform customers of the collection and storing of their personal information, just like the NSA did not inform United States citizens that their communications may be swept.[10] The Apple iPhone licensing agreement asserts that Siri requests "will be recorded and sent to Apple in order to convert what you say into text."[11] But the agreement fails to specify how long the data will be stored and what other information Siri is storing, including addresses and other personal data.[12] The NSA PRISM[13] program, created pursuant to section 702, has a direct connection to not only information stored by Apple, but also Google, Facebook, and other companies engaging in data collection, storage, and communication facilitation.[14] While the targeted information collected through PRISM and telephony metadata collection is foreign intelligence,[15] intelligence officials argue that surveillance programs naturally cannot find foreign targets without initially looking through both foreign and domestic data.[16] Consequently, domestic privacy concerns about personal information storage and use by private companies as well as the NSA deserve closer scrutiny.

President Barack Obama announced reforms on NSA surveillance practices, including those of section 702 and section 215, on January 17, 2014.[17] Additionally, a series of nearly thirty legislative proposals in 2013 aimed to overturn the 2008 FISA Amendments Act (FAA),[18] or otherwise modify FISA, while keeping most surveillance powers intact and improving

---

mation is analyzed to acquire foreign intelligence such as the location of the communicating targets. *See infra* text accompanying notes 72 and 80.

9. *See infra* text accompanying notes 72 and 80; *Klayman*, 957 F. Supp. 2d at 14.

10. *See also* Richards, *supra* note 5, at 1941.

11. Robert McMillan, *IBM Worries iPhone's Siri Has Loose Lips*, CNN (May 24, 2012, 9:05 AM), http://www.cnn.com/2012/05/23/tech/mobile/ibm-siri-ban.

12. *Id.*

13. There is no known acronym for PRISM. *See, e.g.*, *Klayman*, 957 F. Supp. 2d at 11.

14. *See infra* text accompanying note 218.

15. 50 U.S.C.A. §§ 1861, 1881a (West 2011).

16. *See, e.g.*, *infra* text accompanying note 154.

17. *See Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, WASH. POST, Jan. 17, 2014, http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html; Mark Mazzetti & Scott Shane, *Threats Test Obama's Balancing Act on Surveillance*, N.Y TIMES, Aug. 9, 2013, http://www.nytimes.com/2013/08/10/us/threats-test-obamas-balancing-act-on-surveillance.html?_r=0.

18. 50 U.S.C.A. § 1881a (West 2011) (amending FISA to extend surveillance practices to intercept the contents of foreign communications under section 702 until 2017 and provide guidelines for modern warrantless foreign intelligence electronic surveillance).

NSA data collection practices.[19] The Privacy and Civil Liberties Oversight Board (PCLOB), created by executive order back in 2004 to oversee NSA surveillance with civil liberties in mind, also kick started investigations on section 215 Patriot Act and section 702 FISA surveillance following unfavorable media reports on the NSA.[20] The American Civil Liberties Union (ACLU), with some success, vigorously advocates for exposure of NSA practices that impinge on Fourth Amendment rights by unreasonably searching and seizing domestic data.[21] Finally, the Federal Trade Commission (FTC) is implementing a series of reforms to give consumers more control over and information about mass data collection of personal information.[22]

These actions appear to provide a promising foundation for securing the electronic privacy rights of United States citizens. Yet President Obama proposed legislation, and a handful of court opinions uphold much of the current NSA surveillance practices, projecting that the program will continue relatively unchanged.[23] With the expansion or continuation of phone records surveillance, there is also potential for collection of virtually every Siri request made by anyone since Apple began storing these requests.[24] If practices of collecting targeted communications continue as they did prior

19. *See, e.g.*, H.R. 2818, 113th Cong. (2013) (repealing "the USA PATRIOT Act and the FISA Amendments Act of 2008, and for other purposes"); S. 1215, 113th Cong. (2013) (strengthening "privacy protections, accountability, and oversight related to domestic surveillance conducted pursuant to the USA PATRIOT ACT and the Foreign Intelligence Surveillance Act of 1978"); H.R. 2849, 113th Cong. (2013) (amending the "Foreign Intelligence Surveillance Act of 1978 to establish an Office of the Privacy Advocate General").

20. *See* 42 U.S.C.A. § 2000ee (West 2011); PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, SEMI-ANNUAL REPORT, MARCH 2013 – SEPTEMBER 2013 7 (2013), *available at* http://www.pclob.gov/All%20Documents/PCLOB%20Semi-Annual%20Report%20to%20the%20President%20Nov%202013.pdf (explaining that since the board is a new organization, recent activities included moving into a permanent office space in addition to beginning investigations on sections 215 and 702 FISA surveillance).

21. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 1 (D.D.C. 2013); Chitra Marti, *ACLU Attorney Speaks on NSA: 'The Fourth Amendment in the Era of Mass Dataveillance*,' PRINCETONIAN (Nov. 14, 2013), http://dailyprincetonian.com/news/2013/11/aclu-attorney-speaks-on-nsa-the-fourth-amendment-in-the-era-of-mass-dataveillance/ (analyzing ACLU claims referencing phone companies as "'buffets of information' for government authorities," and the NSA impinging on Fourth Amendment rights).

22. Julie Brill, Commissioner, Federal Trade Commission, Keynote Address at the Twenty-Third Computers Freedom and Privacy Conference: Reclaim your Name (June 26, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/public_statements/reclaim-your-name/130626computersfreedom.pdf.

23. *See, e.g.*, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 724 (S.D.N.Y. 2013); H.R. 2818, 113th Cong. (2013) ; United States v. Graham, 846 F. Supp. 2d 384, 390-405 (D. Md. 2012); United States v. Gordon, No. 09-153-02 (RMU), 2012 WL 8499876, at *1-2 (D.D.C. Feb. 6, 2012).

24. See *infra* text accompanying notes 148-49.

to 2014, the system would go something like this: the Siri requests of one user may be collected, then the requests of any other users who contacted the first Siri user within five years would be collected, then any Siri user requests of any users who possibly contacted all of those users could be collected.[25] President Obama's January 2014 reform of the section 215 program only eliminates the last step of this analysis, the collection of the third set of contacts who possibly contacted all of the users in the first two categories.[26] Additionally, President Obama hopes to keep records in the hands of a private entity and directed Congress to investigate how this may be done.[27] So Apple's storage of Siri information already mirrors this future goal. Inevitably, domestic communications and information of all types are subject to the perpetual growth of intrusive surveillance if policy reform continues to ignore the future implications of increased technology and big data collection.[28]

Accordingly, to address the concerns introduced above in Part I, this Comment will analyze policy reform in NSA section 702 and section 215 FISA surveillance practices throughout and conclude by highlighting the best methods for gaining some control over surveillance practices in the past, present, and future. In Part II, this Comment will provide background on the history of NSA surveillance, developing case law, and competing legislative proposals addressing policy concerns. Part III will explain how surveillance works by using the big data collection methods developed by private companies to gather and search through information. Part IV introduces the Federal Trade Commission (FTC) and discusses how the FTC proposes to deal with big data collection in the private realm. Part V will reconcile the structure of NSA surveillance practices with the aforementioned legislative proposals and emerging FTC proposals pertaining to private companies. Additionally, Part V will group each analysis of the most adequate NSA surveillance legislation, forward-thinking policy, FTC proposals, and judicial decisions with executive reforms to create a comprehensive package of suggestions for remedying past and future surveillance concerns. Finally, Part VI will conclude by highlighting the best suggestions for the legislature, judiciary, and executive to preserve domestic privacy in an era of big data collection.

---

25. *See Klayman*, 957 F. Supp. 2d at 16-17.

26. *See Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, *supra* note 17.

27. *See id.*

28. *See infra* text accompanying notes 148-49.

II. BACKGROUND

A. FISA AND THE 2001 PATRIOT ACT

The Foreign Intelligence Surveillance Act of 1978 (FISA) and subsequent amendments, including those made to FISA by the Patriot Act, provide the foundation for modern NSA data collection.[29] FISA implemented NSA electronic surveillance with guidelines in 1978.[30] However, the warrantless surveillance of U.S. citizens' communications was a commonplace exercise of executive power by the time Congress implemented FISA.[31] The Supreme Court hinted to Congress in *United States v. United States District Court for the Eastern District of Michigan (Keith)*, that Congress may consider a distinct set of rules for protections on domestic security surveillance, to be distinguished from criminal surveillance.[32] In response, the Church Committee, created by Congress in 1975, investigated and reported on NSA surveillance practices with a specific focus on the violation of Fourth Amendment rights.[33] FISA was created to protect, rather than hinder American civil liberties as a result of these investigations.[34]

Decades later, FISA amendments added physical searches, pen registers, and trap and trace devices in the 1990s.[35] These additions provided the foundation for President Bush to respond to the 9/11 terrorist attacks by implementing the 2001 Patriot Act, and eventually issuing executive orders amending Executive Order 12,333, which outlined the basic purpose of NSA surveillance back in 1981.[36] The Patriot Act developed FISA further

---

29. 50 U.S.C.A. § 1801 (West 2011).

30. *See id.*

31. *Compare* Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform*, 18 B.U. PUB. INT. L.J. 269, 275 (2009) (providing a timeline of various forms of surveillance on U.S. citizens from President Roosevelt in 1940 to the NSA in 1975), *with* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 730-31 (S.D.N.Y. 2013) (reflecting that FISA was created to protect Fourth Amendment liberties of U.S. citizens).

32. United States v. U.S. District Court for E. Dist. of Mich., 407 U.S. 297, 322 (1972).

33. *Volume 5: The National Security Agency and Fourth Amendment Rights*, THE ASSASSINATION ARCHIVES & RES. CENTER, http://www.aarclibrary.org/publib/contents/church/contents_church_reports_vol5.htm (investigating mainly into "Project MINARET," an NSA surveillance program of black rights and peace groups).

34. *See Clapper*, 959 F. Supp. 2d at 730-31.

35. *See id.*; 50 U.S.C.A. § 1822 (West 2011) (allowing "physical searches for foreign intelligence purposes"); 50 U.S.C.A. § 1842 (West 2011) (authorizing "Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations").

36. *See* Cooper Blum, *supra* note 31, at 275. *See, e.g.*, Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981), *amended by* Exec. Order No. 13,355, 69 Fed. Reg. 53,593

by employing mass "surveillance techniques in a broader range of circumstances without a showing of probable cause, so long as a 'significant purpose' of the intrusion is to collect foreign intelligence."[37] As a consequence, the use of surveillance to collect foreign intelligence became accepted public policy to maintain national security.[38] The modern querying method of bulk telephony metadata collection of phone records, domestic and foreign, began in May 2006.[39] In 2008, the Foreign Intelligence Surveillance Amendments Act (FAA) expanded FISA surveillance powers further into 2017, and now opponents of the NSA surveillance practices trace the evolution of these practices to domestic privacy considerations.[40]

The mass collection of U.S. citizens' phone records gained support from *Smith v. Maryland*,[41] a case which held that the government could conduct surveillance on an individual's phone calls by using a pen register device.[42] The majority reasoned that it was doubtful whether citizens generally maintained an actual expectation of privacy concerning who they make calls to.[43] The telephone company has to receive that particular information and can make permanent records of those numbers to conduct business practices.[44] Therefore, installing a pen register is not a search under the Fourth Amendment.[45] Attorney Catherine Crump, for the ACLU, asserted that *Smith* sets a difficult precedent for opponents of the telephone metadata collection to deal with.[46]

However, just over thirty years later, after massive surveillance evolution from technological developments, Justice Sotomayor's concurrence in

---

(Aug. 24, 2004). These executive orders do provide background on the evolution of NSA surveillance objectives, but executive orders are excluded from analysis in this Comment because it is generally difficult to ascertain their exact impact. *E.g.*, John C. Duncan, Jr., *A Critical Consideration of Executive Orders: Glimmerings of Autopoiesis in the Executive Role*, 35 VT. L. REV. 333 (2010). For commentary on the interplay between the aforementioned amended executive orders and congressional oversight of the Bush Administration, see Tara M. Sugiyama & Marisa Perry, *The NSA Domestic Surveillance Program: An Analysis of Congressional Oversight During an Era of One-Party Rule*, 40 U. MICH. J.L. REFORM 149, 150 (2006).

37. Ellen Yaroshefsky, *Secret Evidence Is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 OFSTRA L. REV. 1063, 1077 (2006).

38. *See President Bush's Address*, N.Y. TIMES, Dec. 17, 2005, http://www.nytimes.com/2005/12/17/politics/17text-bush.html.

39. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 15 (D.D.C. 2013).

40. *See* H.R. 2818, 113th Cong. (2013).

41. Smith v. Maryland, 442 U.S. 735, 746 (1979).

42. *See* Marti, *supra* note 21.

43. *See Smith*, 442 U.S. at 745-46.

44. *Id.*

45. *Id.*

46. Marti, *supra* note 21.

United States v. Jones revisited the issue of surveillance jurisprudence.[47] In *Jones*, the Court held that a warrant is generally required for law enforcement to put GPS tracking devices on motor vehicles.[48] Justice Sotomayor asserted that the Supreme Court may need to revisit jurisprudence maintaining that people cannot reasonably expect information to remain private when they provide this information to third parties.[49] This premise does not fit with:

> the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . [p]erhaps, as Justice [Alito] notes, some people may find the 'tradeoff' of privacy for convenience 'worthwhile,' or come to accept this 'diminution of privacy' as 'inevitable,' . . . and perhaps not.[50]

Justice Sotomayor went on to assert that people will only be protected by the Fourth Amendment, in this age of surveillance, if the Supreme Court stops requiring secrecy to protect private communications.[51] The issues in *Smith* and *Jones* inevitably overlap by shaping the privacy expectations of U.S. citizens.[52] *Smith* continues to be used by the government as a justification for metadata collection of U.S. citizens' phone calls to conduct foreign intelligence surveillance.[53] Justice Sotomayor merely pointed out in *Jones* that this long line of jurisprudence fuels big data surveillance practices by opening the door to arguments that few forms of electronic communications and information are actually private.[54]

ACLU attorney Alexander Abdo presents compelling arguments against the government, maintaining that the surveillance in *Smith* is drastically different from NSA phone record surveillance.[55] Abdo takes support

---

47. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). Although now with the heavy increase in data collection and storage by companies to analyze and sell, it appears a phone company, among others, should provide U.S. consumers with more information about what exactly happens to their very revealing personal data. *See infra* text accompanying notes 234-40.

48. *Jones*, 132 S. Ct. at 946.

49. *Id.* at 957 (citing *Smith,* 442 U.S. at 742; United States v. Miller*,* 425 U.S. 435, 443 (1976).

50. *Id.* at 957 (citing Alito, J., concurring at 962).

51. *Id.*

52. *See id.*

53. *See* Marti, *supra* note 21.

54. *See id.*

55. David Kravets, *How a Purse Snatching Led to the Legal Justification for NSA Domestic Spying*, WIRED (Oct. 2, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/10/nsa-smith-purse-snatching/.

from Sotomayor's concurrence in *Jones*, which points out that citizens provide phone numbers to almost every consumer enterprise.[56] The Supreme Court decided *Smith* on a very narrow set of facts, involving one particular phone company.[57] The NSA's collection of phone records involves *every* possible outlet of communication, and these records are readily available.[58]

B. NSA JURISPRUDENCE IN 2013: IS BULK TELEPHONY METADATA COLLECTION CONSTITUTIONAL OR UNCONSTITUTIONAL?

In *Klayman v. Obama*, Judge Leon of the D.C. Circuit agreed with Abdo and Justice Sotomayor in *Jones*, in his reasoning granting an injunction and ordering the NSA to destroy any telephony metadata collected on two individual plaintiffs, with a stay on the order pending appeal.[59] Judge Leon maintained that the Supreme Court in 1979 could not even envision the scope of telephony metadata collection, let alone the amount of people constantly communicating in different ways on telephones anywhere and everywhere.[60] Judge Leon asserted:

> Whereas some may assume that these cultural changes will force people to 'reconcile themselves' to an 'inevitable' 'diminution of privacy that new technology entails,' I think it is more likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable.[61]

Accordingly, Judge Leon held that constitutional claims against section 215 of the Patriot Act are valid and that the *Smith* precedent should not apply when considering the constitutionality of sweeping telephone record surveillance on U.S. citizens who have done nothing wrong.[62] Rather, Justice Leon held that the sweeping surveillance of phone records violated the Fourth Amendment, because the program conducted unreasonable searches, and an injunction was appropriate to protect against irreparable harm and serve the public interest.[63]

---

56. *Id.*
57. *See* Smith v. Maryland, 442 U.S. 735, 745-46 (1979).
58. *See, e.g.*, Kravets, *supra* note 55.
59. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 1 (D.D.C. 2013).
60. *Id.* at 32.
61. *Id.* at 36 (citing United States v. Jones*,* 132 S.Ct. 945, 962 (2012) (Alito, J., concurring)).
62. *Id.* at 37.
63. *Id.* at 40-3.

On the other hand, Judge Pauley from the Southern District of New York delivered an opposite ruling in *ACLU v. Clapper*, nearly ten days after Judge Leon ruled in *Klayman*.[64] Judge Pauley reasoned that the NSA could not achieve its objective of combating future terrorist attacks if it could not conduct a sweeping collection of every telephone record.[65] Like Judge Leon, Judge Pauley described the querying system the NSA uses on surveillance targets.[66] However, unlike Judge Leon, Judge Pauley discerned a greater purpose behind the queries and held that the system was constitutional and kept with the *Smith* precedent.[67] Judge Pauley applied *Smith* to find that the communication records were already handed over to private companies by citizens who could not expect that the information could still be considered private to the individual.[68] Judge Pauley took his analysis a step further and bolstered a need to keep FISC matters secret by citing historical deference to the executive when it comes to matters of national security.[69] Judge Pauley dismissed the ACLU's claim and held that the program was meant to remain classified and unchallenged and that telephony metadata collection is constitutional.[70]

Also, Judge Pauley held that a mere fear of chilling of free speech does not provide standing to challenge telephony metadata collection.[71] While cellular technology evolved since *Smith*, Judge Pauley cited the *Klayman* court and maintained that metadata remains unchanged and that the information gathered only contains phone numbers, dates, and times.[72] Judge Pauley also commented on the previous issues FISC faced, explaining that the FISC followed court rules to weed out issues of noncompliance in the past.[73] The Intelligence Committees received detailed reports of those noncompliance issues, which were addressed with tighter standards on the NSA from the FISC.[74] Accordingly, the NSA director also did comprehensive evaluations of section 215 practices and established the position of the director of compliance.[75]

---

64. Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 724 (S.D.N.Y. 2013).

65. *Id.* at 747-48.

66. *Id.* at 750-51.

67. *Id.*

68. *See id.* at 751.

69. *See Clapper*, 959 F. Supp. 2d at 731 (citing 5 U.S.C. § 552(b)(1)(A)); THE FEDERALIST NO. 70, at 472 (Alexander Hamilton) (J. Cooke ed., 1961).

70. *Id.*

71. *Id.* at 754.

72. *See Clapper*, 959 F. Supp. 2d at 752.

73. *Id.* at 732-33.

74. *Id.*

75. *Id.*

While Judge Pauley reasoned that any issues with noncompliance were weeded out of the current surveillance process, one legislative proposal, which gained nearly eighty-five sponsors, reacts to this issue quite differently and suggests that more may be done to insure American civil liberties.[76] Additionally, Judge Leon in *Klayman* picked apart the examples of metadata collection that the government provided to demonstrate the metadata program's progress in preventing terrorist attacks.[77] The *Klayman* court discerned that any uncovered terrorists were already found with other evidence that the metadata program merely corroborated.[78] Judge Pauley, in *Clapper*, held to the contrary and used some examples to demonstrate how section 215 surveillance stops terrorist attacks before they take place.[79] Judge Pauley even explained that the current program would have identified and prevented 9/11 hijacker Khalid Al-Mihdhar from carrying out his attack.[80]

Nonetheless, both Judge Leon and Judge Pauley agreed on one point: that the legislature constructed FISA to exclude third party surveillance targets from challenging the NSA's compliance with the statute.[81] But both judges agreed that claims challenging the *constitutionality* of the statute were not precluded.[82] While *Smith* may never be overturned, distinguishing NSA surveillance from the surveillance in *Smith* may open the door to new Supreme Court precedent setting or suggesting constitutional guidelines for certain domestic surveillance practices.[83]

The ACLU and the Supreme Court may have the potential to shape domestic privacy expectations with the Constitution under their belt, but Judge Pauley was correct in holding that deference should be granted to the executive in dealing with matters of national security.[84] Ultimately, the executive will decide where NSA surveillance is headed.[85] The Supreme Court will have Judge Pauley's point in mind and avoid appearing to undermine executive determinations if any ruling on the constitutionality of

---

76. The USA Freedom Act, H.R. 3361, 113th Cong. (2013).

77. *See* Klayman v. Obama, 957 F. Supp. 2d 1 40 (D.D.C. 2013).

78. *See id.*

79. *See Clapper*, 959 F. Supp. 2d at 755.

80. *See id.* at 724.

81. *See id.* at 740; *Klayman*, 957 F. Supp. 2d at 22.

82. *See Clapper*, 959 F. Supp. 2d at 742; *Klayman*, 957 F. Supp. 2d at 24.

83. *See* Smith v. Maryland, 442 U.S. 735, 735 (1979).

84. *See Clapper*, 959 F. Supp. 2d at 754. However the executive should still prove that surveillance is not arbitrary and dealing exclusively with matters of national security. *See Klayman*, 957 F. Supp. 2d at 40.

85. *Full Transcript: President Obama's December 20 News Conference*, WASH. POST, Dec. 20, 2013, http://www.washingtonpost.com/politics/running-transcript-president-obamas-december-20-news-conference/2013/12/20/1e4b82e2-69a6-11e3-8b5b-a77187b716a3_story.html.

NSA practices emerges.[86] Accordingly, since President Obama approved continued surveillance under section 702 and section 215, the greatest policy changes in NSA practices may likely be implemented through legislative action that a Supreme Court ruling would heavily influence by articulating some constitutional guidelines, furthering down the path of *Keith*.[87]

C. CONGRESSIONAL RESPONSE TO FISA CHALLENGES

On the legislative end, congressional proposals address issues of transparency, properly reporting information, ensuring that only foreign intelligence is under surveillance, and providing whistle blowers with an outlet to report misbehavior.[88] Congress proposed nearly thirty pieces of legislation to tackle the exposed NSA program issues with the surveillance process, lack of transparency, and interaction with the FISC.[89] One proposed amendment for section 702(1) of FISA outlined tasks of the Inspector General of the Intelligence Community who will assess the NSA's programs and system rules with security of domestic privacy rights in mind.[90] This includes evaluating the boundaries set out in subsections (b), (d), (e), and (f) of the law pertaining to surveillance of United States citizens and the application of those boundaries.[91] In addition to the suggestion of increased scrutiny on the NSA from the inspector general, the proposals also discuss reform of minimization features that are already included in FISA.[92] Minimization features are in place to protect the privacy rights of U.S. citizens from foreign intelligence data collection.[93] The proposals simply charge the inspector general with ensuring these procedures are followed.[94]

The legislative proposals may appear to be a congressional response to the NSA activities that were leaked by Edward Snowden.[95] Edward Snowden was an independent contractor employed by the NSA to work on de-

---

86. *E.g.*, *Klayman*, 957 F. Supp. 2d at 43 (staying order pending appeal because "significant national security interests . . . and the novelty of the constitutional issues" at stake in this case).

87. United States v. U.S. District Court for E. Dist. of Mich., 407 U.S. 297, 322 (1972).

88. *See id.*; S. 1215, 113th Cong. (2013); H.R. 2849, 113th Cong. (2013).

89. Michelle Richardson, *Dianne Feinstein's Fake Surveillance Reform Bill*, ACLU BLOG (Nov. 8, 2013, 10:55 AM), https://www.aclu.org/blog/national-security/dianne-feinsteins-fake-surveillance-reform-bill.

90. H.R. 2849, 113th Cong. (2013).

91. *Id.*

92. *See id.*

93. See *id.*

94. *See id.*

95. *See* H.R. 2818, 113th Cong. (2013).

veloping surveillance technology.[96] Snowden had access to NSA files and leaked a vast amount of information to media outlets such as The Guardian and The New York Times.[97] While Snowden's actions may seem like the beginning of a push for reform, issues with the FISC and the NSA, which both judges addressed in *Clapper* and *Klayman*, developed prior to the Snowden controversy.[98]

The FISC is the "secret court" that oversees NSA surveillance actions.[99] Snowden's media leak of classified NSA documents led to increased news coverage on the inner workings of the NSA big data collection programs and the FISC.[100] News reports revealed confusion amongst FISC lawyers and judges concerning the NSA's big data program.[101] A lack of understanding of big data surveillance processes kept the FISC from monitoring and remedying NSA bulk data collection.[102] In response to Freedom of Information Act (FOIA) claims before the FISC, some FISC opinions were declassified.[103] In 2009, the FISC explained that the court lacks the confidence it needs to trust that the government is following FISC orders because domestic records were still collected in spite of sworn oaths and minimization procedures.[104]

An October 3, 2011 FISC decision held some NSA internet data collection proposals unconstitutional and unauthorized by the Patriot Act.[105] Edward Snowden's leak of classified documents revealed a massive series

---

96. Mirren Gidda, *Edward Snowden and the NSA Files – Timeline*, THE GUARDIAN, Jul. 25, 2013, http://www.theguardian.com/world/2013/jun/23/edward-snowden-nsa-files-timeline.

97. *See id.*

98. Spencer Ackerman, *NSA Violations Led Judge to Consider Viability of Surveillance Program*, THE GUARDIAN, Sept. 10, 2013, http://www.theguardian.com/world/2013/sep/10/nsa-violated-court-rules-data-documents.

99. 50 U.S.C.A. § 1803(a)(1) (West, Westlaw current through P.L. 113-93 (excluding P.L. 113-79)).

100. *See* Gidda, *supra* note 96.

101. *See* Ackerman, *supra* note 98.

102. *See id.*

103. *FISA Court Orders Declassification Review of Rulings on NSA Spying in Response to ACLU Request*, ACLU (Sept. 13, 2013), https://www.aclu.org/national-security/fisa-court-orders-declassification-review-rulings-nsa-spying-response-aclu-request. Judge Pauley in *Clapper* showed disdain for the claims brought forth on section 215 metadata collection because he reasoned the nature of the collection was never meant to be unclassified in the first place. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013).

104. *In re* Prod. of Tangible Things from [redacted], No. BR 08-13, 2009 WL 9150913, at *6 (F.I.S.C. Mar. 2, 2009).

105. Electronic Frontier Foundation, *October 3, 2011 FISC Opinion Holding NSA Surveillance Unconstitutional*, EFF.ORG, https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional.

of NSA violations of FISC orders.[106] The Post reported, "[t]hree government sources told the Post that the 2,776 infractions would in fact be much higher had the audit included all NSA data collection centers. Each of the 2,776 violations could have potentially encompassed thousands of communications."[107] Judge Bates, the Presiding Judge of the FISC, commented on 2009 issues with telephony metadata surveillance explaining that the court was deeply concerned about the scope of NSA Internet transaction surveillance, which was substantially misrepresented to the FISC, marking the third misrepresentation in under three years.[108]

Still, in 2013 the FISC Judge Eagan asserted that collecting nearly every phone record is a necessity because the NSA is in charge of analyzing the data and connecting the dots to find foreign intelligence before the information is sent to the Federal Bureau of Investigation (FBI).[109] Judge Leon also maintained that the 2009 issues were caught and corrected previously, allowing bulk metadata collection to continue.[110] But this reasoning fails to take into account the potential chilling effect this type of surveillance may have on free speech.[111] Additionally, a failure to regulate the type of data potentially collected from online sources may have a damaging effect not only on privacy but also on the accuracy of the NSA's analysis, so greater scrutiny should be employed.

D. LEGISLATIVE IMPACTS ON NSA POLICY

Although the NSA is permitted to purchase or subpoena some information from private companies, it is still uncertain whether or not the NSA actually stays within the bounds mandated by the Patriot Act or the FISC when acquiring data.[112] This revelation of FISC issues may better explain the congressional push towards further supervision of the NSA that a court like the FISC had difficulty monitoring, even with an increase in judges from seven to eleven granted by the Patriot Act.[113] A coauthor of the Patriot Act, Congressman Jim Sensenbrenner, maintains that congressional and

---

106. *Uncontrolled by FISA Court, NSA Commits Thousands of Privacy Violations per Year*, RT.COM *(*Aug. 16, 2013, 3:54 PM), http://rt.com/usa/nsa-thousands-privacy-violations-report-553/.

107. *See id.*

108. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 18 (D.D.C. 2013) (detailing further issues of NSA noncompliance with minimization procedures before the FISC in the past).

109. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 746 (S.D.N.Y. 2013).

110. *See id.*

111. *See Klayman*, 957 F. Supp. 2d at 42.

112. *See id.*

113. *See* 50 U.S.C. § 1861 (2001); *In re* Prod. of Tangible Things from [redacted], No. BR 08-13, 2009 WL 9150913, at *2 (F.I.S.C. Mar. 2, 2009).

FISC oversight of NSA actions failed due to the realization of metadata collection of phone records of U.S. citizens.[114] Sensenbrenner resolved to propose the USA Freedom Act to end metadata collection, publicize any policy changes, and allow phone companies to publicly state how many government requests are received for information.[115]

Alternatively, the emergence of a legislative proposal from Senator Dianne Feinstein, just days after Sensenbrenner's, actually works to counteract Sensenbrenner's proposals.[116] Senator Feinstein, Chairwoman of the Senate Select Committee on Intelligence, proposed the FISA Improvements Act of 2013 to keep metadata collection of phone calls in the United States.[117] The USA Freedom Act and FISA Improvements Act are vastly different and have more momentum compared to the other almost thirty congressional proposals on the subject.[118] While the FISA Improvements Act appears to address emerging issues with FISA mandated surveillance, the Act actually aims to solidify the current bulk telephony metadata collection of all records, does little to improve oversight, and will fail to respond to the issues that the USA Freedom Act addresses.[119]

E. THE USA FREEDOM ACT v. THE FISA IMPROVEMENTS ACT

1. The USA Freedom Act: Congressman Jim Sensenbrenner

The USA Freedom Act addresses issues of transparency, notice, proper reporting to the FISC, privacy oversight, and the detailed concerns about each area of surveillance.[120] The USA Freedom Act is incredibly thorough in comparison to the aforementioned legislative proposals that aimed to repeal the 2008 FAA and increase minimization procedures.[121] The Act aims to clarify and improve minimization and surveillance on phone records, business records, pen registers, and trap and trace devices, while adding judicial oversight and intelligence assessments by the inspector general.[122]

In addressing minimization procedures, the USA Freedom Act amendment allows FISC judges to evaluate fulfillment of minimization

---

114. *See* Jim Sensenbrenner, *How Obama Has Abused the Patriot Act*, L.A. TIMES, Aug. 19, 2013, http://articles.latimes.com/2013/aug/19/opinion/la-oe-sensenbrenner-data-patriot-act-obama-20130819.

115. *See id.*

116. *See id.*; S. 1631, 113th Cong. (2013).

117. S. 1631, 113th Cong. (2013).

118. *See* Richardson, *supra* note 89.

119. S. 1631, 113th Cong. (2013).

120. H.R. 3361, 113th Cong. (2013).

121. *Id.*

122. *Id.*

requirements by examining the conditions surrounding the acquisition, storage, or distribution of data pertaining to U.S. citizens, either prior to or after approval or "extension" of a "pen register or trap and trace device."[123] The suggested implementation of further judicial review to improve minimization procedures allows for more judicial scrutiny on NSA actions while also calling for more oversight from the Inspector General.[124]

The USA Freedom Act also calls for "comprehensive audits of the effectiveness and use, including any improper or illegal use, of pen registers and trap and trace devices under title IV of the Foreign Intelligence Surveillance Act of 1978."[125] These audits would be conducted by the inspector general and would examine surveillance from January 1, 2010 to December 31, 2013.[126] The proposal also details the new requirement of an Intelligence Assessment of the January 1, 2010 to December 31, 2013 surveillance period, which would look at significance of surveillance activity; investigate how information is obtained, evaluated, and distributed; explain important facts and conditions surrounding FISA; and scrutinize minimization procedures and how, if at all, they are securing constitutional liberties of U.S. citizens.[127] This assessment would be complete by the end of 2014.[128]

The audit and assessment exemplify the USA Freedom Act's attempt to review and correct any past NSA practices that developed to impinge on the privacy rights of U.S. citizens.[129] This is because Sensenbrenner maintains that the original laws were meant for foreign surveillance, and not the domestic intrusions reported to date.[130] This legislative proposal appears to primarily aim to correct any errors of the past while securing a proper use of the rule in the future.[131] In turn, the USA Freedom Act intends to implement what were probably Sensenbrenner's original goals in formulating the Patriot Act: providing national security for citizens while respecting their privacy rights.[132] Additionally, the Act would somewhat help restructure FISA with the original intent of the 1978 legislature responding to the

123. *Id.*
124. H.R. 3361, 113th Cong. (2013).
125. *Id.* at § 202.
126. *Id.*
127. *Id.*
128. *Id.*
129. H.R. 3361, 113th Cong. (2013). The audit requirement suggests that issues of oversight with the FISC on the NSA were not resolved by prior cleanups that Judge Pauley cited in his *Clapper* opinion. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 732 (S.D.N.Y. 2013).
130. *See* Sensenbrenner, *supra* note 114.
131. *See* H.R. 3361, 113th Cong. (2013).
132. *See* Sensenbrenner, *supra* note 114.

Church Committee: protecting Fourth Amendment rights in a surveillance state.[133]

The USA Freedom Act also contains a clarification in section 301, which would amend section 702(b) of the Foreign Intelligence Surveillance Act of 1978.[134] This clarifies that the "collections of communications of United States persons [cannot be searched] . . . to find communications of a particular United States person (other than a corporation)."[135] With a few exceptions, the amendment provides:

> [N]o information obtained or evidence derived from an acquisition pursuant to a certification or targeting or minimization procedures subject to an order under clause (i) concerning any United States person shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the acquisition shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of the United States person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.[136]

Currently, section 1881 liberalizes the original surveillance mandate of FISA.[137] No demonstration of probable cause is needed to show "that the target of the electronic surveillance is a foreign power or an agent of a foreign power."[138] Further, "[section] 1881a 'diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion minimization procedures (though the Government still

---

133. *See Volume 5: The National Security Agency and Fourth Amendment Rights*, *supra* note 33.

134. *See* H.R. 3361, 113th Cong. (2013).

135. *Id.*

136. *Id.*

137. FISHMAN & MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 12:6.50 (3d ed. 2013).

138. *Id.* (citing Clapper v. Amnesty Intern. USA, 133 S. Ct. 1138, 1144, *comparing* 50 U.S.C. § 1805(a)(2)(A), (a)(2)(B) (*see* §§ 12:34 to 12:35 of this treatise, *infra*), *with* 50 U.S.C. § 1881a(d)(1), (i)(3)(A), and citing 1 KRIS & WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS (Westlaw database NSTAP) § 16:16, at 584).

must use court-approved general minimization procedures).'"[139] Nonetheless, there are already minimization and procedural measures in place that must be followed for an acquisition.[140] But this USA Freedom Act amendment to section 1881a(b) adds specificity by explaining what can actually happen to acquired intelligence pertaining to U.S. citizens, which would likely end the sweeping collection of both domestic and foreign communications for analysis.[141]

Moreover, the role of the special advocate outlined in the USA Freedom Act aims to clarify recently exposed issues of oversight with the FISC.[142] Under the amendment, the Privacy and Civil Liberties Oversight Board (PCLOB) will compile a list of five candidates for nomination as special advocate.[143] The special advocate will review FISC and FISC Review court decisions and advocate rigorously for decisions that protect civil liberties.[144] In turn, the special advocate could bolster the intended effect of the PCLOB on surveillance policy.[145]

In strong opposition to this section of the USA Freedom Act, general counsel for the Office of the Director of National Intelligence, Robert Litt, accused the potential special advocate of possibly lacking standing and giving terrorists more protection in the FISC than U.S. citizens.[146] But the PCLOB cannot currently challenge the government's decisions on secrecy and also lacks enforcement power.[147] However, the board does have the power to review classified documents.[148] It appears that the special advocate would merely be an extension of the PCLOB planted at the FISC.[149] The special advocate may bring greater understanding to FISC actions in the future and would probably have standing to do so as an arm of the PCLOB, provided that any constitutional issues would be worked out be-

---

139. *Id.* (citing *Clapper*, 133 S. Ct. at 1157 (Breyer, J., dissenting) (citing 50 U.S.C. § 1881a(e))).

140. *See id.*

141. H.R. 3361, 113th Cong. (2013).

142. *See* Ackerman, *supra* note 98.

143. H.R. 3361, 113th Cong. (2013).

144. *See id.*

145. *See id.*; 42 U.S.C.A. § 2000ee (West, Westlaw current through P.L. 113-93 (excluding 113-79)) (creating the PCLOB to enhance "check and balances" and "ensure that the Government uses its powers for the purposes for which the powers were given").

146. Grant Gross, *U.S. Intelligence Officials: NSA Reform Bill Is Fflawed,'* PCWORLD (Nov. 4, 2013 10:50 AM), http://www.pcworld.com/article/2060660/us-intelligence-officials-nsa-reform-bill-is-flawed.html.

147. 42 U.S.C.A. § 2000ee.

148. 42 U.S.C.A. § 2000ee(g) (authorizing access to classified information from any agency or branch to the extent necessary to carry out PCLOB duties).

149. *See id.*

fore actual creation of the position.[150] Therefore, the special advocate's role in helping the FISC keep surveillance practices in check is substantial and would heavily depend on the recognition of the intricacies of NSA surveillance systems that the FISC may not have.[151]

Finally, in a section on third party reporting, the amendments address electronic service providers to complete the comprehensive focus on the collection of phone records.[152] PCLOB member, James Dempsey, questioned Litt during a PCLOB public hearing on this particular issue.[153] Dempsey asked, "[w]hat if the government were to decide that it wanted to go back and start using 215 for Internet metadata . . . . [W]ould the rational for telephony metadata apply to Internet metadata?"[154] Litt maintained that the two types of collection bring up different issues, but the general parameters of section 215 telephony metadata collection could be applied to an additional set of rules for internet metadata collection in the future.[155] This particular spillover concern is another reason why the tighter constraints the USA Freedom Act imposes on section 215 telephony metadata collection are important.[156]

Sensenbrenner's main goals are to clean up access to domestic phone records, which Sensenbrenner maintains were never meant to fall under the Patriot Act.[157] But FBI general counsel Patrick Kelley argued that:

> [T]he proposal is flawed in the sense that it has the assumption or presumption that we *know* the person we're after, and that's the essence of terrorism prevention: *we don't know* . . . if we are limited to

150. *See, e.g.*, ANDREW NOLAN ET AL., CONG. RESEARCH SERV., INTRODUCING A PUBLIC ADVOCATE INTO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT'S COURTS: SELECT LEGAL ISSUES (2013), *available at* http://justsecurity.org/wp-content/uploads/2013/10/CRS-Report-FISC-Public-Advocate-Oct.-25-2013.pdf. This report provides a thorough analysis of the Appointments Clause and Article III standing issues involved in the creation of a public advocate at the FISC.

151. *See* H.R. 3361, 113th Cong. (2013); Ackerman, *supra* note 98.

152. *See* H.R. 3361, 113th Cong. (2013).

153. Privacy and Civil Liberties Oversight Board Public Hearing, *Consideration of Recommendations for Change: The Surveillance Programs Operated Pursuant to Section 215 of the USA Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act*, at 98 (Nov. 4, 2013) (statement of James Dempsey), *available at* http://www.pclob.gov/SiteAssets/4%20Nov%2013%20Public%20Hearing%20Transcript%20-%20Session%20I.pdf.

154. *Id.* (statement of James Dempsey).

155. *Id.* (statement of Robert Litt).

156. *See id.*

157. Jake Sherman, *Jim Sensenbrenner: NSA Violated Law*, CONGRESSMAN JIM SENSENBRENNER (June 6, 2013), http://sensenbrenner.house.gov/news/documentsingle.aspx?DocumentID=337099.

> seeking numbers from a known [suspect], then we're not going to be very effective.[158]

While Sensenbrenner's arguments to end metadata collection of domestic phone records are compelling, it is uncertain whether or not ending dragnet techniques by the government will eliminate the collection of other types of internet metadata in the future.[159] Litt argued that adopting the USA Freedom Act would basically "shut down" the telephony metadata collection program, while National Security Division Deputy Assistant Attorney General Brad Wiegmann claimed the proposals would force the NSA to return to the pre-9/11 surveillance techniques which failed to stop the hijacker mentioned in the recent *Clapper* decision.[160]

Nonetheless, the USA Freedom Act contains favorable proposals that may correct some allegedly intrusive surveillance errors of the past three years and put promising constraints on future practices.[161] If enacted, the NSA would not be able to search domestic communications for surveillance targets without a warrant issued, unless the agency obtains a court order.[162] The Act also draws more attention to the protective measures already put into place and attempts to clarify and emphasize them.[163] Still, looking beyond the section 215 collection of phone numbers, calls made, and locations, addressing the role of private companies is a necessary step in surveillance reform.[164] Additionally, if the USA Freedom Act passes and ends bulk collection of all telephony metadata containing domestic communications, the NSA may seek out foreign intelligence through alternative means, such as internet metadata collection in bulk, if parameters are not well spelled out by the legislature.

---

158. Jay Stanley, *The Flawed Logic of Secret Mass Surveillance*, ACLU BLOG (Dec. 16, 2013, 10:50 AM), https://www.aclu.org/blog/national-security-technology-and-liberty/flawed-logic-secret-mass-surveillance (emphasis added).

159. H.R. 3361, 113th Cong. (2013).

160. *See* Gross, *supra* note 146; Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 729 (S.D.N.Y. 2013).

161. H.R. 3361, 113th Cong. (2013).

162. *Id. See* Gross, *supra* note 146 (leading into the discussion of Patrick Kelley's claim that the surveillance program does not have specific targets available to adhere to such limits).

163. *See* H.R. 3361, 113th Cong. (2013).

164. Private companies are directly linked to NSA surveillance, and legislation is needed to provide information to subscribers about each company's role in data collection. *E.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 27 (D.D.C. 2013) (emphasizing the vast amount of section 215 metadata collection that includes several private telephone service providers).

2. *The FISA Improvements Act: Senator Diane Feinstein*

In contrast to the USA Freedom Act, Senator Feinstein's FISA Improvements Act does little to narrow the surveillance mechanisms in place and appears to exist more for the sake of public relations than to create change.[165] The FISA Improvements Act asserts that collecting business records in bulk is generally prohibited unless supplemental procedures are satisfied.[166] Supplemental procedures include a ban on collecting content of communications, a time limit of up to ninety days on bulk collection authorization unless extended by the court, security measures made by the court, and limited access to collected data.[167] But the issue with security measures is really the FISC's lack of knowledge and control over NSA surveillance programs.[168] Still, the Act does allow for the appointment of amicus curiae to help the FISC review covered applications.[169] Alternatively, the special advocate in the USA Freedom Act would be a more effective security measure because the advocate would be specially selected through a nomination process intricately tied to the PCLOB to work with the FISC to advocate for better understanding of what rights may or may not be infringed in each instance.[170]

However, the limited access to data provision on business records appears to sound more promising because section 2(j)(1)(D)(i) asserts that there needs to be "a reasonable articulable suspicion that the selector was associated with international terrorism or activities in preparation therefor."[171] But this suggestion is one already ordered by the FISC back in 2009.[172] The FISC reported that the RAS standard was not followed because communications were collected in bulk without discerning whether they qualified as domestic or foreign.[173] The PCLOB revealed in its November 4, 2013 hearing that RAS selectors run searches on communications, gather selections, and then send the collections to an NSA collection facility.[174] The PCLOB demonstrated that with little understanding of how the surveillance program works, it is difficult to understand what a reasona-

---

165. S. 1631, 113th Cong. (2013).

166. *Id.*

167. *Id.*

168. *In re* Prod. of Tangible Things from [redacted], No. BR 08–13, 2009 WL 9150913, at *2 (F.I.S.C. Mar. 2, 2009).

169. S. 1631, 113th Cong. (2013).

170. *See* H.R. 3361, 113th Cong. (2013).

171. S. 1631, 113th Cong. (2013).

172. *In re* Prod. of Tangible Things from [redacted], No. BR 08–13, 2009 WL 9150913, at *2 (F.I.S.C. Mar. 2, 2009).

173. *See id.*

174. Privacy and Civil Liberties Oversight Board Public Hearing, *supra* note 153, at 97.

ble articulable suspicion actually means.[175] The FISC demonstrated that even with knowledge of what RAS means, it is difficult for the NSA to adhere to this standard when collecting both foreign and domestic communications in bulk.[176]

While section 2(j)(1)(D)(i) seems to clarify the purpose of FISA surveillance, section 2(j)(1)(D)(iii) adds a different perspective.[177] The latter section asserts that access may be granted to information whenever it is needed "for technical assurance, data management or compliance purposes, or for the purpose of narrowing the results of queries, in which case no information produced pursuant to the order may be accessed, used, or disclosed for any other purpose, unless [it] is" responding to pre-authorized queries.[178] This provision is too broad and allows for a multitude of exceptions to accessing bulk communication records.[179] Perhaps this catchall is in here to assist with some flaws in NSA data collection that make it difficult for analysts to discern where a communication is actually coming from and whether or not the communication is foreign or domestic.[180] Possibly to account for questions on this particular process, the Act suggests a record requirement to record the object of surveillance, who made the determination, when the determination was made, and that the RAS requirement was met under section 2(j)(1)(D)(i).[181] But there is no record requirement for determinations under section 2(j)(1)(D)(iii).[182] The amendments go on to outline the scope of the queries that will be performed once authorized.[183] This does appear to provide some assurance of the process of surveillance analysis, but it does not describe how information is gathered and assessed to be approved.[184] Still, NSA employees are suspected of having free reign over mass amounts of information, and this makes a miniscule effort to reign in suspicions.[185]

---

175. *See id.*

176. *In re* Prod. of Tangible Things from [redacted], No. BR 08–13, 2009 WL 9150913, at *2 (F.I.S.C. Mar. 2, 2009).

177. *Id.*

178. *Id.*

179. *See id.*

180. *See, e.g.*, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 748 (S.D.N.Y. 2013) (reasoning that when conducting surveillance, certain types of materials may be relevant, though not all information found within these materials may end up being necessary to an investigation).

181. S. 1631, 113th Cong. (2013).

182. *See id.*

183. *Id.*

184. *See id.*; *Clapper*, 959 F. Supp. 2d at 734-35 (explaining that telephony metadata is first collected and analyzed by the program, and a miniscule amount of this is looked at by actual analysts).

185. *See infra* text accompanying note 204.

Section 6 of the FISA Improvements Act amends section 702 of FISA by adding that querying

> the contents of communications acquired under this section with a selector known to be used by a United States person may be conducted by personnel of elements of the Intelligence Community only if the purpose of the query is to obtain foreign intelligence information or information necessary to understand foreign intelligence information or to assess its importance.[186]

Section 6 appears to function in the same way section 2(j)(1)(D)(iii) does in allowing the analysis of domestic communications in order to find out if a communication actually has any foreign intelligence contained within.[187] This is another catchall provision that provides an exception for domestic surveillance.[188] Perhaps these catchall provisions are the reason ACLU legislative counsel Michelle Richardson maintains that "[n]o matter how you cut it, the Feinstein bill is a big step backwards for privacy, and the USA Freedom Act is an incredibly important step forward."[189]

Furthermore, Feinstein's amendment also specifies that records collected pursuant to surveillance powers will be stored for up to five years.[190] The government cannot query any data past three years of that storage time unless approved by the Attorney General.[191] Annual reports of the queried records and the number of court orders issued for the queries are added by the amendment; however, unlike investigations in the USA Freedom Act, these reports do nothing to analyze past acts of NSA surveillance that led to previous violations of court orders.[192]

Nonetheless, the FISA Improvements Act does propose a review of surveillance procedures approved by the attorney general at least once every five years. The review would assess how developments in technology and methods of communication affect "privacy protections" given to U.S. citizens "whose nonpublic communications are incidentally acquired by an element of the intelligence community" in the "most recently approved" NSA procedures.[193] This section calls for a report on any possibility that technology could intrude on the privacy rights of U.S. citizens, but the reports would be done infrequently and no records would be kept of processes

186. S. 1631, 113th Cong. (2013).
187. *See id.*
188. *See id.*
189. *See id.*; Richardson, *supra* note 89.
190. S. 1631, 113th Cong. (2013).
191. *Id.*
192. *See id.*; H.R. 3361, 113th Cong. (2013).
193. S. 1631, 113th Cong. (2013).

that demonstrate how analysts actually develop a suspicion on a foreign surveillance target.[194] However, there is a provision mandating that any data obtained on U.S. citizens be turned over to the FISC in compliance with minimization procedures and providing a "[r]emedy for improper determinations."[195] The court, in finding that the retention of U.S. citizen data is unlawful, may terminate the records, in whole or in part, or request that the information be eliminated.[196] If a report is required at least once every five years, some of the methods that yielded improper results may not end up in the report because they may not be kept on record.[197] Semi-annual reports with significant decisions interpreting the FISA rules and procedures and exact numbers and types of surveillance targets would be done by the attorney general and later released in an unclassified summary format to the public.[198] The description of querying processes of foreign intelligence, record keeping, and reporting mechanisms outlined in the amendment fail to attempt to correct any past wrongs and really miss the point of public concern about bulk collection of records.[199] Rather, the FISA Improvements Act is best supported by Judge Pauley's line of thinking in *Clapper*: collecting everything and showing extreme deference to determinations of relevancy are necessary parts of the analysis.[200] The FISA Improvements Act actually attempts to solidify the 2009 telephony metadata program that President Obama wants to continue, though in the future the initial analysis would be done through a private entity.[201] Alternatively, the USA Freedom Act provides mechanisms for reform that will bolster domestic privacy and stop the sweeping collection of records that might be foreign but must be analyzed to discern whether or not they really are.[202]

---

194. *See id.*

195. *Id.*

196. *See id.*

197. *See* S. 1631, 113th Cong. (2013).

198. *Id.*

199. *See id.*; *See* H.R. 3361, 113th Cong. (2013).

200. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 742-43, 747-48 (S.D.N.Y. 2013).

201. *See* 50 U.S.C. § 1861 (2001); *Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, *supra* note 17.

202. *See* S. 1631, 113th Cong. (2013) (containing the aforementioned "catchall" provisions which open the door to continued across the board surveillance of communications); H.R. 3361, 113th Cong. (2013) (providing amendments to reign in past abuses of data collection which assessed the communications of U.S. citizens).

3. The First Landmark Attempt to Prompt Legislative Reform?

Edward Snowden's leak of classified information informed the public about the scope of NSA surveillance techniques.[203] Snowden reported accusations of the NSA continuously violating federal laws and FISC rulings, hacking into "communications links of major data centers" worldwide to gain access to user information, breaking online "encryption systems," and blatantly lying about collecting information on U.S. citizens to Congress.[204] Now Snowden faces criminal charges of espionage and theft.[205] Russia granted Snowden political asylum in August 2013 to escape prosecution in the United States.[206] Snowden fled the U.S. in fear of receiving an unfair trial following his leak to the press.[207] However, there is some disagreement as to whether or not Snowden did anything wrong.[208]

Snowden told the media he leaked the classified documents to inform innocent citizens of the constant surveillance on them.[209] But NSA advocates explain that this information only pertains to foreign citizens and protects U.S. citizens from foreign threats.[210] Therefore, declassifying this information threatens national security and an ongoing, highly technical anti-terrorism movement.[211] But Snowden revealed a process of bulk collection of hundreds of millions of bits of information on individuals who never aided in thwarting terrorist attacks.[212] Moreover, Snowden's status as an independent contractor left him unprotected by whistleblower protections within the NSA.[213] Snowden's political asylum "means that Russia implicitly rejected the U.S. argument that Snowden is not a whistleblower, but a rogue contractor accused of a felony who is a huge risk to the national security of the U.S."[214] Backlash from the international community was appar-

---

203. *See* Lisa O'Carroll, *Guardian Partners with New York Times over Snowden GCHQ Files,* THE GUARDIAN, Aug. 23, 2013, http://www.theguardian.com/uk-news/2013/aug/23/guardian-news-york-times-partnership.

204. *Edward Snowden, Whistle-Blower*, N.Y. TIMES, Jan. 1, 2014, http://www.nytimes.com/2014/01/02/opinion/edward-snowden-whistle-blower.html?_r=0.

205. *Id.*

206. Bruce Zagaris, *Russia Grants Snowden Temporary Asylum, Frustrating U.S. Extradition Efforts*, 9 INT'L ENFORCEMENT L. REP. 10, at 372 (Oct. 2013).

207. *Id.*

208. *See Edward Snowden, Whistle-Blower*, *supra* note 204.

209. Barbara Starr & Holly Yan, *Man Behind NSA Leaks Says He Did it to Safeguard Privacy, Liberty*, CNN (June 23, 2013), http://www.cnn.com/2013/06/10/politics/edward-snowden-profile/index.html.

210. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 732 (S.D.N.Y. 2013).

211. *See* S. Res. 198, 113th Cong. (2013).

212. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 40 (D.D.C. 2013).

213. *Edward Snowden, Whistle-Blower*, *supra* note 204.

214. Zagaris, *supra* note 206.

ent at the UN General Assembly when the United States was accused by Brazilian president, Dilma Rousseff, of "violating international law" through NSA surveillance.[215] It seems that Snowden's leak of classified methods of surveillance hurt diplomatic relations more than terrorist investigations.[216]

In response to the national skepticism, President Obama explained that government transparency was an eventual and inevitable stage in NSA surveillance, and Edward Snowden merely acted as a catalyst to set reform in motion.[217] Additionally, in the international sector, Obama assured Rousseff that a review of surveillance techniques is happening to align surveillance with privacy expectations of U.S. citizens and foreign allies.[218] President Obama's 2014 reform further responded by adding transparency provisions for foreign surveillance to only engage in surveillance of the "heads of state and government of our close friends and allies" if "there is a compelling national security purpose."[219] The President also asked his "national security team, as well as the intelligence community, to work with foreign counterparts to deepen . . . coordination and cooperation in ways that rebuild trust going forward."[220] To bring transparency to the United States, President Obama's 2014 reform directs the attorney general and the director of national intelligence to do annual reviews of FISC opinions to work towards declassification of court opinions that touch on privacy concerns.[221] Still, whether or not Snowden is a reformer, a whistleblower, or a potential felon, examining the inner workings of big data collection and NSA surveillance practices reveal a multitude of cautions, concerns, and also benefits concerning the evolution of data collection.

---

215. Julian Borger, *Brazilian President: U.S. Surveillance a 'Breach of International Law*,' THE GUARDIAN, Sept. 24, 2013, http://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance.

216. *See id.*; *Klayman*, 957 F. Supp. 2d at 40.

217. *See* Ezra Klein, *Edward Snowden, Patriot*, WASH. POST, Aug. 9, 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/08/09/edward-snowden-patriot/. *But see* Sugiyama, *supra* note 36 (noting that back in 2006 complaints leaked from within the FBI, where officials were concerned about the NSA's unnecessary surveillance of U.S. citizens).

218. Borger, *supra* note 215.

219. *See Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, *supra* note 17.

220. *Id.*

221. *See id.*

III. METHODS OF SURVEILLANCE: HOW BIG IS THE BIG DATA CONNECTION?

PRISM enables direct "NSA access to Internet data, such as email, chat, videos, photos, and file transfers held by leading Internet companies, including Google, Microsoft, Facebook, Yahoo, Skype, Apple, Paltalk, Youtube, and AOL."[222] While the program sounds invasive, corporate attorneys for these entities oversee government orders for information on specific individuals before access may be granted to PRISM.[223] On the other hand, the revelation of statutory violations by the NSA leaves some room for questioning the validity of NSA requests.[224] It is necessary to examine how PRISM and big data surveillance work in order to ascertain how invasive government surveillance may be.

PRISM emerged in 2007 with the Protect America Act, which amended FISA.[225] When the NSA wants to acquire information from a corporation the Protect America Act explains:

> [T]he Director of National Intelligence and Attorney General may direct a person to—(1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target; and (2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain. (f) The Government shall compensate, at the prevailing

222. Maria Tzanou, *Is Data Protection the Same as Privacy? An Analysis of Telecommunications' Metadata Retention Measures*, 17 J. INTERNET L. 21 (2013).

223. Timothy B. Lee, *Here's Everything we Know About PRISM to Date*, WASH. POST, June 12, 2013, http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

224. *See Uncontrolled by FISA Court, NSA Commits Thousands of Privacy Violations per Year*, *supra* note 106.

225. *See* Protect America Act of 2007, Pub. L. No. 110–55, 121 Stat. 552 (2007). *See also NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

> rate, a person for providing information, facilities, or assistance pursuant to subsection (e).[226]

PRISM put the words of the Protect America Act in motion by enabling an efficient connection between companies housing user information and the NSA.[227] However, PRISM is different from section 215 metadata collection of communication records, which captures, stores, and analyzes information that is moving past surveillance channels.[228]

Telephony metadata collection pursuant to section 215 of the Patriot Act works by doing a complete sweep of all available domestic and foreign phone records.[229] When a target is identified and approved for query by an RAS selector, NSA analysts follow a particular procedure.[230] The procedure looks at phone calls, dates, times, and locations.[231] The surveillance target is referred to as a "seed," and analysts (because of minimization requirements) may only examine communications found, now two hops,[232] yet formerly, "three 'hops' from the seed."[233] Hop one encompasses all of the outgoing and incoming calls made to and from the seed in a five-year span.[234] Hop two collects all contact numbers that every single incoming and outgoing caller has contacted in the past five years.[235] Finally, the former hop three gathers all of the contacts that all of the hop two numbers "called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 'second hop' numbers, or 1,000,000 total)."[236] The NSA also collected email communications using a similar data mining technique of seeds and hops.[237] But, unlike gathering identifiers like email addresses rather than phone numbers, the mining captured IP addresses and

---

226. *See* Protect America Act of 2007.
227. *See id.*
228. *See id.*
229. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 14-16 (D.D.C. 2013).
230. *See id.*
231. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013).
232. *See Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, *supra* note 17.
233. *See Klayman*, 957 F. Supp. 2d at 16.
234. *See id.*
235. *See id.*
236. *Id.*
237. *See* Glenn Greenwald & Spencer Ackerman, *NSA Collected U.S. Email Records in Bulk for More than Two Years Under Obama*, THE GUARDIAN, June 27, 2013, http://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama.

subject lines for data analysis.[238] The email collection does not currently take place, but other types of Internet data collection remain intact.[239]

The abovementioned capture and analysis of moving data describes metadata or "data about data,"[240] which is born from the information collected in various spots. Small pieces of data are collected and then grouped with other small pieces.[241] One small piece may not tell the surveyor anything, but when grouped with other small pieces, the information can be revealing.[242] The NSA conducts this sort of process to find surveillance targets or seeds to determine if they meet the RAS standard and perform queries on them.[243] Private corporations also use this process to gather small pieces of information on a mass of individuals to sell it to advertisers.[244] This "data mining" practice of collecting information on individuals is increasingly popular amongst big business advertisers.[245] Companies can locate individuals and calculate which ads will best fit with what they are doing.[246] Once an individual is on a company's radar for a few years, that company is able to look at collected data and figure out minute details of a person's life.[247] IBM engineer Jeff Jonas elaborated on the process, stating "[w]ith 87% certainty, I can tell you where you'll be next Thursday at 5:35 p.m."[248] While data analysis may aid in advertising, it is also becoming commonplace in developing individual profiles called dossiers, and credit ratings that give companies a quick glimpse into an individual's day-to-day status.[249]

Big data is sparking concerns with the Federal Trade Commission (FTC) because analysis on consumers creates potentially unfair and inaccurate reports.[250] Algorithms are the computer science tools that provide methods for organizing small pieces of data in order to create consumer

---

238. *Id.*

239. *See id.*

240. Craig Ball, *Beyond Data About Data: The Litigator's Guide to METADATA* 2 (2005), http://www.craigball.com/metadata.pdf.

241. *Id.*

242. Cent. Intelligence Agency v. Sims, 471 U.S. 159, 178 (1985) (quoting Halperin v. Cent. Inetlligence Agency, 629 F.2d 144, 150 (D.C. Cir. 1980).

243. *In re* Prod. of Tangible Things from [redacted], No. BR 08-13, 2009 WL 9150913, at *2 (F.I.S.C. Mar. 2, 2009).

244. Lucas Mearian, *Big Data to Drive a Surveillance Society*, COMPUTERWORLD (Mar. 24, 2011), http://www.computerworld.com/s/article/9215033/Big_data_to_drive_a_surveillance_society?pageNumber=1.

245. *Id.*

246. *Id.*

247. *Id.*

248. *Id.*

249. *See* Mearian, *supra* note 244. *See also* Brill, *supra* note 22.

250. Brill, *supra* note 22.

profiles or scores, or more easily analyze collected data.[251] Scores called eScores are created from collected online information to form a consumer-based profile.[252] The eBureau website markets eScores to "any business-to-consumer enterprise or government agency that wishes to leverage data and analytics to improve decisions and results."[253] The Protect America Act provides a foundation for this market to government enterprises by setting the stage for PRISM to align with the private big data collection process.[254] Basically, by creating a direct shortcut via PRISM, big data professionals create algorithms to form reports, and in the future (if surveillance goes unchecked) the NSA may simply order the information with the work already complete. Essentially, "[m]ass data retention is a central element in mass surveillance."[255] The issue is whether or not the completed works of these big data programs produce fair and accurate results.

This issue is magnified in the example of the evolution of the Transportation Security Administration (TSA).[256] TSA began recruiting big data enterprises to produce an optimum airline passenger security scanning system after 9/11.[257] The algorithms used produced inaccurate and unnecessary security concerns on particular U.S. citizens, similar to the inaccurate and unnecessary collection of communications of U.S. citizens by the NSA.[258] The TSA programs mirror NSA metadata storage and analysis of information taken from individuals using online databases and services.[259] Private corporations vehemently competed to build the best TSA security system that would identify terrorists and keep them off of planes.[260] Lexis Nexis was a key player in the corporate competition that led to the adoption of a big data system to boost airport security.[261] Like the NSA, TSA employed outsiders working in the private realm to come up with an optimum sys-

---

251. *See* Xindong Wu et al., *Top 10 Algorithms in Data Mining*, 14 KNOWL. INF. SYS. 1, 3 (2008), http://www.cs.uvm.edu/~icdm/algorithms/10Algorithms-08.pdf.

252. Brill, *supra* note 22, at *3.

253. *eScore Overview*, EBUREAU, http://www.ebureau.com/escore (last visited Sept. 15, 2013).

254. *See* Tzanou, *supra* note 222.

255. Kristy Hughes, *Mass Surveillance or Just Big Data?*, XINDEX (July 29, 2013), http://www.indexoncensorship.org/2013/07/mass-surveillance-or-just-big-data/.

256. ROBERT O'HARROW, NO PLACE TO HIDE: BEHIND THE SCENES OF OUR EMERGING SURVEILLANCE SOCIETY 231-52 (2005).

257. *Id.* This recruitment of private entities to build an optimum scanning system is potentially the same sort of recruitment that the NSA and attorney general may need to use to continue section 215 surveillance with the data stored elsewhere. *See Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, *supra* note 17.

258. O'HARROW, *supra* note 256, at 228-30 (providing several accounts of U.S. citizens inaccurately identified as potential terrorists by TSA's big data security system).

259. *See id.*

260. *See id.*

261. *See* O'HARROW, *supra* note 256, at 238-40.

tem.[262] While airline passengers consent to increased airport security, citizens going about day-to-day activities in a hyper-information society should not be susceptible to detrimental surveillance errors in big data intelligence systems conducting "arbitrary" surveillance.[263]

IV. THE FEDERAL TRADE COMMISSION (FTC): PROVIDING POSSIBLE GUIDELINES FOR CONSTRAINTS ON FUTURE SURVEILLANCE OF U.S. CITIZENS

The FTC works with state, federal, and international entities to ensure consumer protection and fair but strong competition in the marketplace.[264] The FTC is keeping an eye on big data collection to minimize harmful risks to consumers.[265] The FTC aims to educate consumers about controlling methods like the Fair Credit Reporting Act (FCRA), while implementing policies of "transparency" and "notice and choice."[266] FTC spokeswoman Julie Brill elaborated on the FTC's plan of attack on big data beginning first with the FCRA.[267]

Although some issues that may affect consumers do not always fall under the act,[268] for the decisions that do fall under the FCRA, the FTC tells companies that consumers should have "notice, access, and correction rights."[269] Additionally, the FTC has "consent decrees" which "monitor the activities of other apps and online services that have similarly wandered into FCRA territory."[270] The challenges for the FTC in enforcing the FCRA are figuring out all of the service providers who practice in "employment, credit, housing, and insurance" that are subject to it.[271]

The proposed program, called Reclaim Your Name, would help consumers identify brokers that are using their information and allow them to access this data to "opt-out" if it is revealed that brokers are using personal data for marketing, and allow consumers "to correct errors in information used for substantive decisions – like credit, insurance, employment, and other benefits."[272] However, current access and corrections rights don't do

---

262. *See id.* at 228-30.
263. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 42 (D.D.C. 2013).
264. *About the Federal Trade Commission*, FED. TRADE COMM'N, http://www.ftc.gov/ftc/about.shtm (last visited Sept. 9, 2013).
265. Julie Brill, *Big Data, Big Issues*, FED. TRADE COMM'N (Mar. 2, 2012), http://ftc.gov/speeches/brill/120228fordhamlawschool.pdf.?
266. Brill, *supra* note 22, at *3.
267. *Id.* at *3.
268. *Id.*
269. *Id.* at *3.
270. *Id.*
271. Brill, *supra* note 22, at *3.
272. *Id.* at *4.

much for citizens that don't understand big data programs.[273] This is why transparency is important for citizens hoping to set their records straight.[274] The FTC is also hoping to develop methods of notice and choice by implementing tools for consumer de-identification and the "scrubbing [of] sensitive data."[275] Additionally, spokeswoman Julie Brill urges for legislative reform that scales "notice, access, and correction rights to consumers" in accordance with "the sensitivity and use of the data at issue."[276] All of these FTC proposals provide an adequate model for NSA surveillance reform, though some explanation is necessary to explain the connection.

V. SUGGESTIONS FOR NSA REFORM

A. A COMPREHENSIVE PACKAGE FOR REMEDYING FUTURE ACTS OF SURVEILLANCE

While Judge Pauley held that NSA telephony metadata surveillance runs on secrecy and will only work effectively if all records are collected in one fell swoop, President Obama's elected panel of surveillance advisors asserted that these methods are overbroad and unnecessary for preventing attacks.[277] One suggestion of the panel was leaving the information in the hands of the private companies and obtaining court orders to conduct metadata surveillance.[278] President Obama went along with this suggestion and ordered the NSA and the attorney general to work toward figuring out a way to continue the dragnet telephony metadata program without the government storing all of the domestic and foreign data.[279] Getting rid of the third "hop" also appears to be a response to the panel's conclusion that querying methods were overbroad.[280] Before any "transition" to a new program, the metadata may "be queried only after a judicial finding or in the case of a true emergency."[281] Accordingly, clearer guidelines for judicial evaluations must emerge.

---

273. *Id.* at *4.
274. *Id.*
275. *Id.* at *5.
276. Brill, *supra* note 22, at *8.
277. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013); Ellen Nakashima & Ashkan Soltani, *Panel Urges New Curbs on Surveillance by U.S.*, WASH. POST, Dec. 18, 2013, http://www.washingtonpost.com/world/national-security/nsa-shouldnt-keep-phone-database-review-board-recommends/2013/12/18/f44fe7c0-67fd-11e3-a0b9-249bbb34602c_story.html.
278. *Id.*
279. *See Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, *supra* note 17.
280. *See id.*
281. *See id.*

If courts are to weigh in on whether or not queries may be conducted on identified surveillance targets, taking a tip from the FTC on what guidelines to follow is a necessary step.[282] In issuing a court order, judges should examine "the sensitivity and use of the data at issue," just like the private companies in the FTC proposals.[283] Private companies, whether or not they are connected to PRISM, should do the same.[284] In working to provide notice, user agreements must provide increased knowledge to U.S. citizens sharing information with programs that gather information spanning from an individual's geographic location to daily habits and preferences.[285] When companies store user data, just like the NSA, legislation must mandate that there is some knowledge about what kind of analysis is happening to domestic personal data and where. A sort of Fair Surveillance Reporting Act, like the Fair Credit Reporting Act, could provide some knowledge to those subject to surveillance.[286] If the information truly supplies foreign intelligence on terrorism or some sort of threat to safety, a court order would surely mandate classification and agency control over the information. This is addressed in the USA Freedom Act Amendment to section 1881a(b), which adds specificity by explaining what can actually happen to acquired intelligence pertaining to U.S. citizens.[287] Adopting the USA Freedom Act and adding the aforementioned considerations, which stem from FTC ideas, could bring more transparency, notice, and choice to the future of surveillance.[288]

B. A COMPREHENSIVE PACKAGE FOR REMEDYING PAST ACTS OF SURVEILLANCE

In taking tips from the FTC's vision, guidelines for officials looking into past indiscretions should follow Judge Leon's example of ordering the destruction of any stored records that are found unnecessary to surveillance objectives, like those of the two plaintiffs in *Klayman*.[289] Judge Leon's example is one application of the Reclaim Your Name scrubbing strategy suggested by the FTC.[290] Except in the realm of NSA surveillance, scrubbing of sensitive data and taking back control merely means judicial review

---

282. Brill, *supra* note 22, at *3.
283. *See id.* at *8.
284. *See id.*
285. *See* Mearian, *supra* note 244 (describing the technological capabilities of modern surveillance programs).
286. Brill, *supra* note 22, at *3.
287. H.R. 3361, 113th Cong. (2013).
288. *See id.*; Brill, *supra* note 22, at *3.
289. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 1 (D.D.C. 2013); Brill, *supra* note 22, at *3.
290. *See Klayman*, 957 F. Supp. 2d at 1; Brill, *supra* note 22, at *3.

of past procedures and court orders telling the NSA to erase all unnecessary data collected and stored in its systems.[291]

Like the issues the FTC points out, any access and correction rights to already collected data does not do much for those who do not understand how section 702 and 215 programs work.[292] The USA Freedom Act proposals do much by suggesting a comprehensive review of past metadata collection during the times where dragnet NSA surveillance went unchecked by the FISC.[293] The most effective comprehensive review would incorporate the USA Freedom Act proposals, along with a suggestion of providing notice and choice to past domestic targets of overbroad surveillance techniques that may opt their information out of the potential five-year storage.[294] This method would preserve some of the important secrecy that Judge Pauley highlighted in *Clapper*, while putting some control of information back in the hands of U.S. citizens.[295] Additionally, there would be a chance to weed out issues of possibly inaccurately analyzed information and reveal the true scope of surveillance operations to ensure better monitoring in the future.

Still, the Privacy and Civil Liberties Oversight Board has a large role to play in uncovering what exactly is going on with NSA surveillance techniques.[296] The PCLOB is attempting to understand the complicated ins and outs of surveillance programs, and questioning how things may spiral out of control if other programs continue to develop in the direction of section 215 telephony metadata collection.[297] Further suggested legislation outlining the parameters of surveillance beyond telephony metadata collection is necessary, and certainly feasible by the PCLOB if it continues investigating in the same direction.[298] Moreover, if the USA Freedom Act passes, the PCLOB will have the special advocate serving the FISC on its behalf, aiding in greater judicial understanding and control of surveillance techniques.[299]

---

291. *See Klayman*, 957 F. Supp. 2d at 1; Brill, *supra* note 22, at *3.
292. Brill, *supra* note 22, at *3.
293. H.R. 3361, 113th Cong. (2013).
294. *See Klayman*, 957 F. Supp. 2d at 1; Brill, *supra* note 22, at *3.
295. *See* Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724, 742 (S.D.N.Y. 2013).
296. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., *supra* note 20, at 7.
297. Privacy and Civil Liberties Oversight Board Hearing, *supra* note 153, at 97.
298. *See id.*
299. H.R. 3361, 113th Cong. (2013).

V. CONCLUSION

It is certain that the best way to correct past and present issues of comprehensive metadata collection is to adopt a combined approach of the four ideologies presented by the *Klayman* court, USA Freedom Act, the FTC in Reclaim Your Name, and the PCLOB in forward-looking investigations.[300] With a projected policy of placing greater influence on judicial approval and the actions of private companies, examining data's "sensitivity" and "use" in making decisions concerning U.S. citizens is necessary.[301] Transparency, notice, and choice will emerge with more informative user agreements and domestic reports detailing the possible analysis of personal data. Also, destroying storage of unnecessary records, creating opt outs, and performing comprehensive reviews of past procedures will help U.S. citizens achieve Reclaim Your Name scrubbing in the surveillance realm.[302] Correcting the scope of surveillance and eliminating inaccuracies are important improvements that will result from reviewing past actions. Finally, the PCLOB investigations will not only reveal the scope of surveillance, but also pave the way for legislation that will set the limits for all surveillance programs and increase understanding. The adoption of this comprehensive package will correct past wrongs and implement a policy of sensitivity going forward in judicial evaluations and legislative considerations. Hopefully, the sensitivity objective will be applicable in a future that mandates court orders in order to conduct queries on seeds targeted for surveillance, with less deference to the NSA in making determinations.[303]

This comprehensive package is necessary because of the looming future of technology that is directly linked to NSA surveillance. Young U.S. citizens are not even immune to data collection by private companies when they are at school.[304] A survey by Common Sense Media brought attention to private companies employed by schools that store student data with information on student health, grades, computer use, cafeteria meals, and disciplinary records.[305] There are not many restrictions on how these companies use and store this particular data.[306] Children and adults are also currently using a multitude of applications (apps), or software devices that

---

300. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 1 (D.D.C. 2013); H.R. 3361, 113th Cong. (2013); Brill, *supra* note 22, at *3; Privacy and Civil Liberties Oversight Board Hearing, *supra* note 153, at 97.

301. *See* Brill, *supra* note 22, at *8.

302. *See id.*

303. *See Klayman*, 957 F. Supp. 2d at 1.

304. Claudio Sanchez, *Survey: Students' Personal Data Are at Risk*, NPR (Feb. 17, 2014), http://www.npr.org/2014/02/17/278389264/survey-students-personal-data-are-at-risk.

305. *Id.*

306. *Id.*

perform different functions like creating games, location devices, and connections to subscribers.[307] Edward Snowden released documents detailing collaborations between the NSA and Britain's Government Communication Headquarters to gain access to data from a multitude of apps for collection and storage as early as 2007.[308] NSA surveillance of the Angry Birds app is one example of app spying that captures details like user sex, location, and age.[309] While allowing these intrusions now may not seem wholly detrimental to privacy, technological achievements in the future will make privacy virtually impossible for any software participants. The Google Brain project aims to program biology into computer systems so that phones and computers can form extremely intimate links with their owners in the future.[310] There is currently an "arms race" between major corporations like IBM, Google, Apple, Baidu, and Microsoft to find the most adequate algorithms for the creation of a computer brain.[311] In this future, apps and computer programs will be designed to read and interact with human emotion.[312] Lurking behind those programs will be surveillance and data collection. This is "going to take decades," but the project is already in motion and the NSA has already latched on to every major communication outlet.[313] If steps are not taken to implement the goals of the aforementioned comprehensive package in the United States, the bounds of the law will expand as technology expands, and privacy expectations will shrink in the shadow of human analysis and surveillance.

Still, reclaiming data collected and stored by the NSA could prove problematic, costly, and time consuming. But Judge Leon warned the government in *Klayman* that a failure to comply with his decision, if not overturned, would result in timely sanctions.[314] Remedying any past issues and instituting safeguards for future issues is of the utmost importance. The future of NSA surveillance may depend most largely on the direction of the

---

307. Marziah Karch, *Apps*, GOOGLE, http://google.about.com/od/a/g/apps_def.htm (last visited Feb. 17, 2014).

308. James Glanz et al., *Spy Agencies Tap Data Streaming from Phone Apps*, N.Y. TIMES,Jan. 27, 2014, http://www.nytimes.com/2014/01/28/world/spy-agencies-scour-phone-apps-for-personal-data.html?_r=0.

309. James Ball, *Angry Birds and 'Leaky' Phone Apps Targeted by NSA and GCHQ for User Data*, THE GUARDIAN, Jan. 28, 2014, http://www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data.

310. Daniela Hernandez, *The Man Behind the Google Brain: Andrew Ng and the Quest for the New AI*, WIRED (May 7, 2013), http://www.wired.com/wiredenterprise/2013/05/neuro-artificial-intelligence/2/.

311. *Id.*

312. *See id.*

313. *Id.*

314. *See* Klayman v. Obama, 957 F. Supp. 2d 1, 44 (D.D.C. 2013).

executive, but the legislature and the Supreme Court have a large role to play in setting out guidelines for the NSA and the judiciary and guidelines for how much privacy the Constitution affords information moving across channels that may currently be seized at any moment.[315]

SHAINA KALANGES*

315. *See, e.g.*, *Klayman*, 957 F. Supp. 2d at 1.

* Shaina Kalanges is a second-year law student at the Northern Illinois University College of Law with a Bachelor of Arts from the University of Illinois Urbana-Champaign. She is an Assistant Editor of the Northern Illinois University Law Review. Shaina would like to thank her family and friends, especially her parents, for their constant encouragement and support. Shaina would like to give special thanks to Professor Amy Widman, Professor Therese Clarke, Professor Robert Jones, Notes and Comments Editor Lars Okmark, the entire 2013-2014 Northern Illinois University Law Review staff, and Samuel Czervionke for encouraging the development and perfection of her Comment.