A Tale of Two Agencies: Exploring Oversight of the National Security Administration by the Federal Communications Commission

Audra Healey*

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2015; B.A. *magna cum laude*, in Political Science, concentration in Public Policy and Administration, minor Law and Public Policy, Northeastern University, December 2011. The author would like to thank her parents and grandparents for their love, support, and encouragement in all things.

I. INTRODUCTION

> "In the years to come, we will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are. That means reviewing the authorities of law enforcement, so we can intercept new types of communications, but also build in privacy protections to prevent abuse."
>
> -President Obama, May 23, 2013[1]

According to recent disclosures, the National Security Agency ("NSA") has been collecting information from hundreds of millions of email accounts and phone numbers, many belonging to Americans.[2] The NSA's strategy is to use this information to "draw detailed maps of a person's life, as told by personal, professional, political, and religious connections."[3] Former NSA director Gen. Keith Alexander argued that the agency's bulk collection of email and call detail records is necessary because the government "need[s] the haystack to find the needle."[4]

The NSA's extensive surveillance of U.S. citizens was brought into the spotlight by the recent disclosures of former NSA contractor Edward Snowden.[5] The first of Snowden's disclosures, released by The Guardian on Wednesday, June 5, 2013, revealed that the NSA was collecting phone call detail records from millions of U.S. consumers on a daily basis.[6] This has prompted widespread public concern about the extensive information collection policy of the NSA. As technology continues to develop and the Internet continues to play a major role in modern life, governmental monitoring of Internet activity will likely become an area of increasing concern. The best way to ensure proper oversight of this monitoring is by empowering an administrative agency: namely, the Federal Communications Commission (the "FCC").

---

1. Remarks by the President at the National Defense University, The White House, Office of the Press Secretary, May 23, 2013, *available a*t http://www.whitehouse.gov/the-press-office/2013/05/23/remarks-president-national-defense-university.

2. Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST, Oct. 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?ref=twttr.

3. *Id.*

4. *Id.*

5. *See, e.g.*, James Bamford, *Edward Snowden: The Most Wanted Man in the World*, WIRED (Aug. 13, 2014), http://www.wired.com/2014/08/edward-snowden/.

6. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

This Note will address what role the FCC could and should play in overseeing intelligence activities that implicate individual privacy on the Internet and telecommunications networks. This Note argues that the FCC, as the expert independent agency that routinely deals with the Internet and telecommunications networks, has both the tools and capacity to provide some oversight and protection for Internet users. Part II discusses the background of each agency, beginning with the NSA, then delves into the FCC and its efforts to keep pace with the ever-changing Internet. Part III argues that, because the existing mechanisms for overseeing governmental, domestic surveillance programs are inadequate, and given the FCC's long history of scrutinizing the interplay of national security and privacy involving telecommunications, Congress should empower the FCC to address privacy concerns raised by the NSA's surveillance of U.S. citizens. Part IV discusses how the FCC could address NSA surveillance activities, laying out possible, practical solutions that Congress should provide.

II. TWO CHANGING AGENCIES: THE NSA AND THE FCC

A. The NSA has increasingly turned its surveillance towards the American public.

The NSA, originally formed to monitor outside threats to the security of the United States, has increasingly turned its surveillance towards the American public.[7] The NSA was originally formed in 1952 growing out of intelligence and cryptology analytics developed during WWII, which naturally developed the agency's mission to monitor threats coming from outside the United States.[8] Today, the NSA is "authorized to collect, process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions, and to provide signals intelligence support for the conduct of military operations."[9]

Under the letter of the law, this power is significantly limited in the domestic arena. The Foreign Intelligence Surveillance Act of 1978 ("FISA") [10] bars the NSA from intercepting any domestic, electronic communications of persons inside the United States unless a judge on the

7. *See, e.g.*, Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. TIMES, Apr. 16, 2009, A1, *available at* http://www.nytimes.com/2009/04/16/us/16nsa.html.

8. *See generally* THOMAS L. BURNS, CTR. FOR CRYPTOLOGIC HISTORY, NAT'L SEC. AGENCY, THE ORIGINS OF THE NATIONAL SECURITY AGENCY: 1940–1952 (1990), *available at* https://www.nsa.gov/public_info/_files/cryptologic_histories/origins_of_nsa.pdf.

9. *Frequently Asked Questions: Oversight*, NAT'L SEC. AGENCY, http://www.nsa.gov/about/faqs/oversight.shtml (last visited Dec. 20, 2014) (citing Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,947–48 (Dec. 4, 1981)).

10. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801–1885c).

Foreign Intelligence Surveillance Court ("FISA Court") issues a warrant upon finding that "the purpose of the surveillance is to obtain foreign intelligence information . . . and there is probable cause to believe that the target of the surveillance is an agent of a foreign power."[11] FISA also places various restrictions on other forms of domestic surveillance activities that do not intercept the contents of communications, such as the "installation and use" of pen registers or trap and trace devices, which capture the origin and destination of phone calls or other communications to and from a particular telephone number or other device.[12] In 2001, Congress substantially expanded FISA with the USA PATRIOT Act,[13] adding, among other provisions, a section that authorizes the Director of the Federal Bureau of Investigation ("FBI")—or FBI agents designated by the Director—to petition the FISA Court for "an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[14] Moreover, under Executive Order 12,333, when the NSA conducts intelligence-gathering activities abroad—which are not regulated by FISA[15]—it may collect, retain, or disseminate information about United States persons "only in accordance with procedures established by the head of the agency and approved by the Attorney General."[16]

Despite its foreign-centric mission and the express limits on its domestic authority, the NSA has increasingly turned its attention to activities of persons within the United States in the wake of 9/11. For instance, in 2006, it was discovered that the NSA had created a call database in 2001 that collected tens of millions of citizens' phone records from data provided by AT&T, Verizon, and BellSouth.[17] "[T]he largest database ever assembled in the world" at the time, its goal was to log "every call ever made within the nation's borders."[18] The NSA itself has acknowledged its serious obligation

---

11. PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD 131 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; *see also* FISA § 104, 50 U.S.C. § 1804 (2012) (procedures for issuance of surveillance order); *but see* FISA § 102, 50 U.S.C. § 1802 (2012) (permitting President to authorize surveillance of "communications used exclusively between or among foreign powers").

12. FISA § 402, 50 U.S.C. § 1842 (2012) (authorizing a designated government attorney to apply for pen register or trap and trace order upon certifying its relevance to "international terrorism or clandestine intelligence activities").

13. Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended at scattered sections of U.S.C.).

14. *Id.* § 215 (codified as amended at FISA § 501, 50 U.S.C. § 1861 (2012)).

15. *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMC'NS TECHS., *supra* note 11, at 183; *see also* 50 U.S.C. § 1812 (2012).

16. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,950 (Dec. 4, 1981).

17. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 11, 2006, 10:38 AM), http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm.

18. *Id.* (internal quotation marks omitted).

to operate effectively in an increasingly interconnected and globalized world without stepping on the toes of civil liberties for the sake of national security.[19]

Additionally, the NSA's intrusions into domestic communications extend beyond call data to reach citizens' activity on the Internet.[20] For years, the NSA "unlawfully gathered tens of thousands of emails and other electronic communications between Americans" as part of the agency's broader collection of communications as they "flow across Internet hubs" under Section 702 of FISA.[21] Pursuant to these practices, the NSA may have intercepted as many as 56,000 domestic electronic communications through various methods, [22] some of which the FISA Court has found unconstitutional.[23]

The disclosure of these NSA practices triggered a substantial backlash. Many Americans reacted by taking steps to insulate themselves from what they considered unwarranted government intrusion on their private lives and activities.[24] Even though several crucial FISA Court rulings have been partially declassified and released to the public[25] in an effort to demonstrate that the NSA's powers are not unrestrained, public trust and confidence in the agency has clearly diminished.[26] In the wake of these disclosures, forty-five percent of Americans felt that the government went too far in its surveillance programs pursuant to anti-terrorism efforts.[27] This "massive

19. NSA, The NSA: Missions, Auths., Oversight and P'ships (Aug. 9, 2013) *available at* http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf [hereinafter NSA: Missions, Authorities, Oversight, & Partnerships].

20. Ellen Nakashima, *NSA Gathered Thousands of Americans' E-mails Before Court Ordered It to Revise Its Tactics*, WASH. POST (Aug. 21, 2013), http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html.

21. *Id.* (citing FISA § 702, 50 U.S.C. § 1881a (2012)).

22. *Id.*

23. Gov't's Ex Parte Submission of Reauthorization Certification and Related Procedures (Foreign Intelligence Surveillance Court Oct. 3, 2011) [hereinafter FISC Memorandum Opinion], *available at* http://apps.washingtonpost.com/g/page/national/fisa-court-documents-on-illegal-nsa-e-mail-collection-program/409/; *see also* Nakashima, *supra* note 20.

24. Grant Gross, *People Flock to Anonymizing Services After NSA Snooping Reports*, PCWORLD (Oct. 10, 2013 1:10 PM), http://www.pcworld.com/article/2054040/people-flock-to-anonymizing-services-after-nsa-snooping-reports.html (discussing people protecting themselves by anonymizing their own Internet traffic to hide from governmental surveillance).

25. *See, e.g.*, *Now Declassified: FISA Court Ruling Documents*, WALL ST. J. (Aug. 21, 2013, 5:17 PM), http://blogs.wsj.com/washwire/2013/08/21/now-unclassified-fisa-court-ruling-documents/.

26. *See* Jonathan D. Salant, *Snowden Seen as Whistle-Blower by Majority in New Poll*, BLOOMBERG (July 10, 2013 6:00 AM), http://www.bloomberg.com/news/2013-07-10/snowden-seen-as-whistlebloweer-by-majority-in-new-poll.html.

27. *Id.*

swing" in public opinion about government policies embodies "the public reaction and apparent shock at the extent to which the government has gone in trying to prevent future terrorist incidents."[28] Coupled with the steps that many Internet users are taking to prevent government intrusion on their online activities and communication, this shift in public opinion shows that Americans are dissatisfied with the reach of government surveillance.[29]

B. The Federal Communications Commission is a dynamic agency, adapting to new communications technology as it emerges.

The FCC makes a conscious effort to adapt to new technology. Established by the Communications Act of 1934,[30] the FCC regulates interstate and international communications by radio, television, wire, satellite, and cable in all 50 states, the District of Columbia, and U.S. territories.[31] As the agency's then-Chairman acknowledged in 2012, the FCC necessarily plays a role in facilitating the continuing development of the Internet.[32] Moreover, the FCC's governing statutes empower the agency to investigate and regulate actual and potential breaches in communications privacy that threaten customer proprietary network information ("CPNI"), among other types of customer information.[33] This authority encompasses not only traditional mediums of telecommunications,[34] such as the Public Switched Telephone Network,[35] but also newer mediums, such as the

28. *Id.* (quoting Peter Brown, assistant director of Quinnipiac's polling institute).

29. *Id.*; Gross, *supra* note 24.

30. Communications Act of 1934, ch. 652, 48 Stat. 1064 (codified as amended at 47 U.S.C. §§ 151–620 (2012 & Supp. 2013)).

31. *See* Communications Act § 1, 47 U.S.C. § 151.

32. Julius Genachowski, Chairman, FCC, Prepared Remarks on Cybersecurity at the Bipartisan Policy Center 2 (Feb. 22, 2012) [hereinafter Genachowski Cybersecurity Speech], *available at* http://www.fcc.gov/document/chairmans-remarks-cybersecurity-bipartisan-policy-center. Former Chairman Genachowski noted that "it's critical that we preserve Internet freedom and the open architecture of the Internet, which have been essential to the Internet's success as an engine of innovation and economic growth." *Id.*

33. *See, e.g.*, Communications Act § 222, 47 U.S.C. § 222 (2012) (imposing a duty on "[e]very telecommunications carrier . . . to protect the confidentiality of proprietary information" involving subscribers and other carriers); *see also* Alan J. Chang, *The Federal Communications Commission and the NSA Call Database: The Duty to Investigate*, 30 HASTINGS COMM. & ENT. L.J. 581, 586 (2008).

34. *See* Implementation of the Telecomms. Act of 1996, *Report and Order and Further Notice of Proposed Rulemaking*, FCC 07-22, 22 FCC Rcd. 6927, 6954–57, paras. 54–59 (2007), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-07-22A1.pdf (extending CPNI privacy rules to providers of "interconnected VoIP service").

35. For a detailed discussion of the PSTN and the FCC's role in regulating it, see Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 FED. COMM. L.J. 203, 205–07 (2014).

Internet, to the extent that the FCC considers providers of Internet traffic to be "telecommunications carriers."[36]

Communications privacy plays an important role in the FCC's formulation of policies and procedures to promote the use and development of the Internet, and the FCC may even have substantial authority to act in this area.[37] The agency recognizes that the adoption of broadband is affected by consumer's perception of their online privacy and security.[38] Indeed, the FCC has made a point of adapting to and fostering privacy and security on the Internet by developing industry standards to regulate communications providers as new technology has developed.[39] To that end, the agency puts a strong emphasis on working with industry leaders, academics, engineers, federal partners, as well as companies that work to build and expand Internet infrastructure and services, representatives from state and local entities, and Internet entrepreneurs and pioneers.[40] The FCC has thus made a point to stay abreast of new technological developments in Internet and broadband technology, while working to facilitate consumer use of and confidence in this technology.

III. OVERSIGHT IS NEEDED, AND THE FCC SHOULD PROVIDE IT

A. Existing executive and legislative oversight mechanisms are inadequate in promoting efficiency and public confidence in the NSA.

The executive and legislative mechanisms currently in place to provide oversight of the NSA are inadequate in promoting public confidence and effective national security. Ostensibly, the activities of the NSA are generally governed by the Constitution, federal law, executive orders, and regulations of the Executive Branch. [41] On the legislative side, there are two

36. *Cf.* Protecting and Promoting the Open Internet, *Notice of Proposed Rulemaking*, FCC 14-61, 29 FCC Rcd. 5561, 5612–16, paras. 148–55 (2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-14-61A1_Rcd.pdf (seeking comment on whether the FCC should reinterpret Title II of the Communications Act, 47 U.S.C. §§ 201–276, to include Internet service providers as telecommunications carriers).

37. *See* Verizon v. FCC, 740 F.3d 623, 644-46 (identifying § 706 of the Communications Act as the source of this authority).

38. Genachowski, *supra* note 32, at *3.

39. *See id.* at 4. Former Chairman Genachowski noted that, "[a]s the nation's expert agency on communications, the FCC has a long history of engagement on network reliability and security, working with commercial communications providers, wired and wireless, to develop industry-based, voluntary best practices that improve security and reliability." *Id.*

40. *Id.*

41. *Frequently Asked Questions Oversight*, NAT'L SEC. AGENCY, http://www.nsa.gov/about/faqs/oversight.shtml (last visited Feb. 20, 2015); *see About the*

congressional bodies—the House Permanent Select Committee on Intelligence ("HPSCI") and the Senate Select Committee on Intelligence ("SSCI") —that are responsible for ensuring that the NSA follows the applicable laws and regulations.[42] In the executive branch, NSA oversight is vested in the President's Intelligence Advisory Board, the Office of the Director of National Intelligence, and the Department of Justice. [43] Ostensibly, in addition to these legislative and executive oversight mechanisms, the NSA has also implemented internal controls: the Office of the Inspector General performs audits and investigations while the Office of Compliance operates to ensure that the NSA follows relevant standards.[44] However, despite the appearance of effective controls, these oversight mechanisms have failed to prevent the current public crisis in confidence that the NSA is fulfilling its mission with the least possible adverse impact on the privacy of U.S. citizens.

The authority of the NSA, subject to the above controls, is very limited on paper. Every intelligence activity that the NSA undertakes is purportedly constrained to the purposes of foreign intelligence and counterintelligence.[45] For instance, Executive Order 12,333 provides the authority for the NSA to engage in the "collection of communications by foreign persons that occur wholly outside the United States."[46] Additionally, FISA authorizes the NSA to compel U.S. telecommunications companies to assist the agency in targeting persons who are not U.S. citizens and are reasonably believed to be located outside the United States.[47]

However, despite the appearances of controls, both external and internal, the "communications of U.S. persons are sometimes incidentally acquired in targeting the foreign entities."[48] The varying types of data gathered can produce a "detailed map" of a given person's life based on those persons with whom they are in contact.[49] For instance, metadata can be used to piece together substantial information about relationships; this information includes who introduced two people, when they met, and their

---

Committee, U.S. SENATE SELECT COMM. ON INTELLIGENCE, http://www.intelligence.senate.gov/about.html (last visited Feb. 20, 2015) [hereinafter SENATE INTELLIGENCE COMM.]; *History and Juristiction*, U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/about/history-jurisdiction (last visited Feb. 20, 2015) [hereinafter HOUSE INTELLIGENCE COMM.]; Lynn Mattice, *Debating the NSA, Espionage and Hackers with Congressman Mike Rogers*, SECURITY MAG. (Oct. 1, 2013), http://www.securitymagazine.com/articles/84782-the-nsa-cyber-espionage-hackers-and-more.

42. *Frequently Asked Questions Oversight*, *supra* note 41; SENATE INTELLIGENCE COMM., *supra* note 41; HOUSE INTELLIGENCE COMM., *supra* note 41; Mattice, *supra* note 41.

43. *Frequently Asked Questions Oversight*, *supra* note 41.

44. *Id.*

45. NSA: Missions, Authorities, Oversight and Partnerships, *supra* note 19, at 2.

46. *Id.* at 3–4 (citing Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981)).

47. *Id.* at 5 (citing FISA § 702, 50 U.S.C. § 1881a) (2012)).

48. *Id.* at 4.

49. Gellman & Soltani, *supra* note 2.

general communication patterns, as well as the nature and the extent of their relationships.[50] The recently disclosed collection of contact lists by the NSA has not been authorized by Congress or FISA.[51] Additionally, while other collection policies that touch upon domestic communications, such as those under Section 702, have authorization, often neither lawmakers nor the public have even a rough estimate of how many communications of U.S. citizens are being acquired.[52]

The NSA is easily able to operate around its apparent lack of authority. One anonymous official has been quoted as saying that the NSA consciously avoids the restrictions placed on it by FISA by collecting this information from access points all over the world.[53] This method means that the NSA is not required to restrict itself to collecting contact lists belonging to specified intelligence targets.[54] The collection mechanism ostensibly operates under the assumption that the bulk of the data collected through the overseas access points is not data from American citizens.[55] However, this is not necessarily true due to the globalized nature of the Internet as a communications infrastructure, as "data crosses boundaries even when its American owners stay at home."[56]

The oversight mechanisms currently applied to this collection program require the NSA only to satisfy its own internal oversight mechanisms or to answer possible inquiries from executive branch that there is a "valid foreign intelligence target" in the data collected. [57] Moreover, congressional oversight is not effective because members of Congress have candidly said they do not know precisely the right questions to ask NSA officials.[58] Often,

---

50. TEDx Talks, *The Power of Metadata: Deepak Jagdish and Daniel Smilkov at TEDxCambridge 2013*, YOUTUBE (Sept. 25, 2013), http://www.youtube.com/watch?v=i2a8pDbCabg. The talk encompasses the subject of how metadata can be used to determine the nature, extent, and timeline of a given relationship between two people based on the metadata in their emails. *Id.*

51. Gellman & Soltani, *supra* note 2.

52. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 147 (2014) [hereinafter PCLOB REPORT II], *available at* http://www.pclob.gov/library/702-Report.pdf. In surveillance "[u]nder Section 702, the government acquires the contents of telephone calls and Internet communications from within the United States, without individualized warrants or court orders, so long as the acquisition involves targeting non-U.S. persons reasonably believed to be located outside the United States, for foreign intelligence purposes." *Id.* at 146.

53. Gellman & Soltani, *supra* note 2.

54. *Id.* This is supposing, pending information to the contrary coming to light, that the anonymous official is correct about the NSA's methods and the motives behind them.

55. *Id.*; *see also* PCLOB Report II *supra* note 52, at 141 (discussing foreigness and foreign purpose requirements).

56. *Id.*

57. *Id.*

58. Mike Masnick, *Even Senate Intelligence Committee Admits That NSA Oversight Is Often a Game of 20 Question*s, TECHDIRT (Oct. 15, 2013, 11:58 AM), http://www.techdirt.com/articles/20131014/17191824879/even-dianne-feinstein-admits-that-nsa-oversight-is-often-game-20-questions.shtml. It is important to note, however, that

in congressional hearings, NSA officials and other senior members of the intelligence community are evasive unless directly pressed, and the congressional committees are stymied by their lack of knowledge regarding just which questions need asking.[59]

Given the realities of the NSA overstepping its authority, there is no indication to the public that the agency, even as it has been collecting data from American citizens, has been required to answer to its various oversight mechanisms in an effective manner. In response, President Obama directed the Privacy and Civil Liberties Oversight Board ("PCLOB") to conduct two reports about NSA intelligence gathering methods.[60] The PCLOB is an independent, bipartisan agency within the executive branch tasked with reviewing and analyzing executive branch actions taken in the name of national security to determine whether appropriate consideration has been afforded to civil liberties in the development and implementation of national anti-terrorism policy.[61] The recent PCLOB Report emphasizes that there is a:

> compelling danger . . . that the personal information collected by the government will be misused to harass, blackmail, or intimidate, or to single out for scrutiny particular individuals or groups . . . . while the danger of abuse may seem remote, given historical abuse of personal information by the government during the twentieth century, the risk is more than merely theoretical.[62]

The second report addressed more specifically Internet surveillance activities of the NSA—specifically those undertaken pursuant to Section 702.[63] These reports demonstrate that there is a serious risk of abuse of the data collected by the NSA, as well illustrating the failings of current governmental oversight of NSA data collection policies.

---

this is a candid statement by a member of Congress in an interview expressing uncertainty, rather than an official source. This seems to indicate that, despite all the information that members of Congress are privy to, members of the intelligence community are often as closed-lipped as possible unless the exact right question is asked in the exact right manner. *See id*.

59. *See id*.; Gellman & Soltani, *supra* note 2.

60. *See generally* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014) [hereinafter PCLOB REPORT I], *available at* https://www.eff.org/files/2014/01/23/final_report_1-23-14.pdf; PCLOB REPORT II, *supra* note 52.

61. PCLOB REPORT I, *supra* note 60, at 8; *About the Board*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., http://www.pclob.gov/about-us.

62. PCLOB REPORT I, *supra* note 60, at 12.

63. PCLOB REPORT II, *supra* note 52, at 2.

Moreover, according to some classified intelligence documents released by *The Washington Post* and other outlets, the NSA appears to be overwhelmed by the sheer amount of data it is has collected, which indicates that the mechanisms in place do not adequately help the NSA to focus its search. For instance, the NSA has begun to implement a program (SCISSORS) in order to focus on the portion of the data that is relevant amongst the mass of data collected.[64] This is because the NSA was collecting broad swaths of data with "little or no [foreign intelligence] information."[65] The first PCLOB report indicates that the NSA metadata collection program does not pass any semblance of relevancy standards to target the data to a specific question of national security; this is because the NSA does not have reason to suspect the owners of the metadata, unlike in other cases where the collection was lawful.[66]

Thus, the current oversight system suffers from some serious failings. First, it does not allow for a focused inquiry by the congressional committees. Additionally, the NSA can get around requirements imposed on it by FISA by conducting Internet surveillance abroad that nonetheless captures U.S. data flows, many of which traverse foreign networks. Moreover, the NSA has over-collected data with little value to the agency's national security mission, and therefore must sift through masses of data involving regular American citizens while fighting a public battle about how much information the agency collects.[67] This all suggests deficiencies in the NSA's oversight structure, as all preventive executive, legislative, and internal controls have not been effective.

B. Stronger oversight is also needed because the courts are ill-equipped to adequately review and oversee the NSA.

Further demonstrating that change in oversight is needed, federal courts, including the FISA Court, have shown themselves inadequately suited to oversee the NSA's activities. As discussed in the previous subsection, existing oversight mechanisms have not stopped the NSA from pursuing these aggressive and intrusive data collection policies.

---

64. Barton Gellman & Matt DeLong, *An Excerpt from the NSA's Wikipedia*, WASH. POST, Oct. 14, 2013, at 2 [hereinafter *Intellipedia*], *available at* http://apps.washingtonpost.com/g/page/world/an-excerpt-from-intellipedia/519/#document/p2/a126422. SCISSORS is a NSA system that helps parse electronic communications. *Id.*

65. *Id.* at 3.

66. PCLOB REPORT I, *supra* note 60, at 77–78 (citing Carrillo Huttel, LLP v. SEC, No. 11-65, 2011 WL 601369, at *1-2 (S.D. Cal. Feb. 11, 2011); *In re* Subpoena Duces Tecum, 228 F.3d 341, 345, 350–51 (4th Cir. 2000)). The first PCLOB Report indicates that the government collection of metadata would satisfy the relevancy criteria if the government's request was defined and limited by the concrete facts of a particular investigation, but there is no particularized inquiry in mass collection of data. PCLOB REPORT I, *supra* note 60, at 78.

67. *Intellipedia*, *supra* note 64, at 3.

Additionally, the courts too have a similar gap in reactive oversight. As such, some form of oversight is needed to bridge the gap between preventative oversight by congressional committees and reactive oversight by the FISA Court. This section first shows that the NSA defies judicial control, then discusses how the traditional appellate process is ineffective, before arguing that the FISA Court is ineffective at controlling the NSA's data collection policies.

The NSA is not effectively controlled by judicial mechanisms: the agency violated the orders of the FISA Court that set out the parameters of permissible surveillance. In 2009, the Department of Justice ("DOJ") discovered that the NSA had been operating an automated searching system contrary to FISA Court orders.[68] The NSA acknowledged that the Court's orders did not provide the agency with authority to employ the list of phone records in the manner in which it did.[69] Separately, it was also disclosed to the FISA Court that the NSA had violated the court's orders when thirty-one NSA analysts queried the telephone records database.[70] Moreover, traditional courts without security clearance have limited authority over the NSA.[71]

1. Traditional courts do not provide an adequate avenue of appeal.

The regular avenue of redress through trial and appellate courts does not provide an adequate avenue of appeal for citizens challenging NSA data collection. One primary drawback of the ordinary appellate process is its lack of uniformity. For instance, the U.S. District Court for the District of Columbia and the U.S. District Court for the Southern District of New York have reached wildly different conclusions while dealing with the same basic issue.[72] In particular, the United States District Court for the District of Columbia granted injunctive relief for citizens challenging NSA data collection policies, holding that the public interest weighed in favor of relief on constitutional grounds.[73] However, the District Court for the Southern

68. PCLOB REPORT I, *supra* note 60, at 47 (citing *In Re* Production of Tangible Things, No. BR 08-13 (Foreign Intelligence Surveillance Court Feb. 17, 2009)).

69. *Id*.

70. *Id.* at 50 (citing *In Re* Production of Tangible Things, No. BR 08-13 (Foreign Intelligence Surveillance Court Mar. 2, 2009)).

71. *See* Klayman v. Obama, 957 F. Supp. 2d. 1, 9 (D.D.C. 2013).

72. *Compare Klayman*, 957 F. Supp. 2d., *with* ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

73. *Klayman*, 957 F. Supp.2d at 42 (noting that it "is always in the public interest to prevent the violation of a party's constitutional rights") (quoting Am. Freedom Def. Initiative v. Wash. Metro. Area Transit Auth., 898 F. Supp. 2d 73, 84 (D.D.C. 2012) (quoting G & V Lounge, Inc. v. Mich. Liquor Control Comm'n, 23 F.3d 1071, 1079 (6th Cir.1994))). The court stayed its injunction in light of the significant national security interest at stake, pending appeal. *Id*. at 43-44.

District of New York found that, while the right to be free from searches and seizures is fundamental, it is not absolute, and thus held that NSA data collection practices were lawful.[74]

Moreover, while courts recently have not shied away from analyzing the constitutional issues involved,[75] these same opinions have indicated a healthy reluctance to overstep into issues where jurisdiction is more questionable due to national security concerns.[76] The regular appeals process generally cannot, or at least is often unable to, consider national security information.[77] Both this limitation and the lack of uniformity show that the courts are not a guaranteed avenue for citizens to seek redress from NSA data collection practices, nor do they provide one national voice to speak on such important topics that necessitate uniform and effective review.[78]

2. The FISA Court is not providing an adequate level of publicly available oversight.

Moreover, the FISA Court, a specialized judicial entity which is intended to provide direct oversight over data collection, is not providing an adequate level of publicly accountable oversight. Unlike regular courts, the FISA Court does not provide a mechanism for non-governmental parties to provide insight into the particulars of any given case via amicus briefs.[79] This characteristic of FISA Court proceedings means that the Court does not take adequate account of positions other than the government's, which in turn undermines the credibility and usefulness of the Court in cases involving

74. *Clapper*, 959 F. Supp. 2d at 756–57.

75. *See, e.g.*, *Klayman*, 957 F. Supp. 2d at 19 (finding that the court had the authority to review the constitutional claim raised); *Clapper*, 959 F. Supp. 2d at 742 (finding that the court had authority to review the constitutional claims raised).

76. *See, e.g.*, *Klayman*, 957 F. Supp. 2d at 19 (holding that the court was barred from reviewing the statutory claims based in the Administrative Procedure Act); *Clapper*, 959 F. Supp. 2d at 742 (noting that the claims based on statutory grounds were precluded and would likely fail even if they were not).

77. *Klayman*, 957 F. Supp. 2d at 19; *Clapper*, 959 F. Supp. 2d at 742. Indeed, the *Klayman* Court expressly noted that the government regused to avail itself of *in camera* review that would allow the Court to view sensitive information. *Klayman*, 957 F. Supp. 2d at 41 n.65.

78. For example, in debating the ultimate creation of the Court of Appeals for the Federal Circuit, the Senate acknowledged that the structure of the federal courts does not facilitate uniformity in circumstances of where a "promt, definitive answer to legal questions of nationwide significance" is required. S. Rep. 97-275 at 14 (noting that "the creation of the Court of Appeals for the Federal Circuit provides such a forum for appeals from throughout the country in areas of the law where Congress determines that there is *special need for national uniformity*." (emphasis added)). The challenge of providing effective oversight of the NSA's domestic surveillance activities is likewise such a circumstance, and triggers a similarly special need for national uniformity regarding the privacy rights and expectations of citizens.

79. PCLOB REPORT I, *supra* note 60, at 13–14. The PCLOB Report does, however, note that in one instance, the court accepted one amicus brief. *Id.*

metadata, as the court must rely solely on the assertions of the NSA.[80] The PCLOB noted that "[i]t is central to the integrity of the process that public has confidence in its impartiality and rigor," and the FISA Court proceedings lack this element by not allowing for outside comment.[81] Indeed, the FISA Court must rely on the assertions of the regulated parties, such as the NSA, and is unable to benefit from expertise of relevant parties, unlike regular courts, where outside parties are able to submit amicus briefs.[82] The public has a significant interest in privacy; this constitutional right is of central importance to the American people, and lack of public input is a serious failing of the process.[83]

Therefore, as the FISA Court must rely solely on the representations of the government, it is susceptible to misrepresentations. The recent declassified decision of the FISA Court revealed that "[c]ontrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using methods and terms that did not meet the standard for querying."[84] This confidential nature of FISA Court proceedings does not foster public confidence, as there has been public backlash to the fact that the primary opinion authorizing bulk metadata collection of U.S. citizens' records has taken this long to produce, even in redacted form.[85] This ruling shows that the FISA Court is not well-equipped to provide effective oversight of NSA operations because of the lack of public input in its proceedings, the possibility of misrepresentation, and the delays involved with providing decisions to the public.[86]

Moreover, while redaction is required to protect national security information, it does not inspire public confidence. The recent decision is necessarily heavily redacted due to the sensitive nature of the national

80. *Id.* at 14. .
81. *Id.*
82. *Id.*
83. *See id*.
84. Charlie Savage & Scott Shane, *Secret Court Rebuked N.S.A. on Surveillance*, N.Y. TIMES, Aug. 21, 2013, at A1, http://www.nytimes.com/2013/08/22/us/2011-ruling-found-an-nsa-program-unconstitutional.html?_r=0. Indeed, the FISA Court was "troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program." FISC Memorandum Opinion, *supra* note 23 at *16, n.14. Moreover, the FISA Court noted that "[C]ontrary to the government's repeated assurances, NSA had been routinely running queries of the metadata using querying terms that did not meet the required standard for querying." *Id.*
85. *See id.* (noting that while the opinion promoted openness and was not overly redacted, its delay was troubling).
86. *Id*. (quoting Mark Rumold of the Electronic Frontier Foundation as saying that "[t]his opinion illustrates that the way the court is structured now it cannot serve as an effective check on the N.S.A because it's wholly independent on the representations that the N.S.A makes to it . . . . [I]t has no ability to investigate. And it's clear that the NSA representations have not been entirely candid to the court."); *see* PCLOB REPORT I, *supra* note 60, at 13–14.

security information involved.[87] There is, however, a need for more transparent information proving that the NSA is not intruding too far into the privacy of American citizens with its world-wide programs[88] Moreover, recent judicial inquiries have focused on violations of the privacy of individuals one at a time, rather than large-scale violations, which are unlikely to stem the larger problem of continuing NSA surveillance.[89] Additionally, these judicial decisions, while setting conflicting precedents, are backward-looking, rather than forward-looking; courts cannot enjoin surveillance programs unless injured parties know they exist.[90] Moreover, as the discussion above has shown, the way the FISA Court oversight is structured works against promoting public confidence due to the necessary lack of disclosure and comment opportunities for the public. This illustrates the gap in oversight, as neither the appellate courts nor the FISA Court are able to foster public confidence in the government's ability to react to NSA privacy infringement, just as congressional and executive oversight cannot foster public confidence that the government can prevent privacy violations by intelligence agencies.

C. The FCC mission can be naturally expanded to protect privacy in relation to surveillance.

The FCC has a strong privacy background as well as a strong history of promoting openness and transparency on the Internet. First, this section shows the FCC has been extending many of its regulations to the Internet and adapting to changes in technology as it does so. Second, the FCC has a strong history of protecting the nation's communications infrastructure. The FCC has experience with accounting for the globalized nature of communications.[91] This section next argues that the FCC's background in these areas prepares the agency to step into a new role overseeing the NSA collection of data. Finally, this section discusses the benefits of tasking the FCC with this important oversight role.

87. *See generally* FISC Memorandum Opinion, *supra* note 23.

88. *See* PCLOB REPORT II, *supra* note 52, at 13.

89. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d. 1 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

90. *Compare Klayman*, 957 F. Supp. 2d. 1, *with Clapper*, 959 F. Supp. 2d 724. As discussed above, these recent judicial decisions regarding NSA data collection do not set a coherent precedent, and are in clear tension with one another.

91. *See, e.g.*, Comm'n Policies and Procedures Under Section 301(b)(4) of the Commc'ns Act, Foreign Investment in Broadcast Licenses, *Declaratory Ruling*, FCC 13-150, 28 FCC Rcd. 16244, 16247–48, paras. 6–8 (2013) (discussing globalization, growth, and innovation).

1. The FCC has strong a background and significant expertise that will allow the agency to provide oversight of the NSA.

Since the "advent of the Internet," the FCC has been involved in regulating this facet of the nation's communications infrastructure.[92] For instance, as early as 1980, the FCC considered the extent to which information processing (as involved in Internet services) required further or different regulation from other communications networks.[93] In 1980, the FCC began to recognize a distinction between basic and enhanced services, and applied this distinction until its codification in the Telecommunications Act of 1996.[94] Following codification, the FCC continued its use of this framework, but expanded its scope to include elements of Internet infrastructure, such as broadband connectivity.[95] However, the FCC remained willing to consider applying its regulatory framework to new technologies.[96] This flexibility has helped the agency adapt to new and changing technology as it influences the nation's communications infrastructure.

---

92. Verizon v. FCC, 740 F.3d 623, 629–30 (D.C. Cir. 2014) (noting that "[s]ince the advent of the Internet, the Commission has confronted the questions of whether and how it should regulate this communications network, which, generally speaking, falls comfortably within the Commission's jurisdiction over 'all interstate and foreign communications by wire or radio.'" (citing 47 U.S.C. § 152(a))).

93. *Id*. (discussing the Computer II "regime").

94. *Id*. (noting that the Telecommunications Act of 1996 tracks the Computer II distinction between basic and enhanced services in its distinction between telecommunications carries and information-service providers).

95. *Id.*

96. For instance, the FCC showed a willingness to expand and reinterpret existing regulations in its interpretation of cable broadband in Nat'l Cable & Telecom. Ass'n v. Brand X Internet Servs., 545, U.S. 967, 976–77 (2005). In *Brand X*, the FCC had changed its interpretation and concluded that cable broadband providers provide a single, integrated information service and were therefore entirely exempt from Title II regulation. *Id. Brand X* involved a prolonged legal battle regarding a declaratory ruling of the FCC classifying broadband cable modems as an information service rather than a telecommunications service, so as not to be subject to mandatory title II common carrier regulation. *Id.* at 967–68. There were many parties that petitioned for review and it was a long decision process that involved much uncertainty in what the FCC could do moving forward. *Id.* After the case, the FCC continued to "confront[] the challenge of protecting consumers, maintaining universal service and ensuring public safety in uncertain legal terrain." Statement of Comm'r Copps in Response to Supreme Court Decision in Brand X Internet Servs., WL 1523583 (FCC June 27, 2005), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-259623A1.pdf (noting that the *Brand X* decision "makes the climb much steeper. But this country just has to find ways to promote innovation, enhance competition, protect the openness of the Internet, and return the United States to a position of leadership in broadband penetration. The Commission needs to think anew and act anew to meet these challenges, and I look forward to working with my colleagues to do just that.").

Additionally, the FCC acknowledges the impact of privacy on the Internet. The recognition that "[c]onsumers' privacy needs are no less important when consumers communicate over and use broadband Internet access than when they rely on [telephone] services," has played a large part in FCC policy, as the agency has long supported protecting the privacy of broadband users.[97] The FCC further ensures that consumers have control over how their information is used, and that they are protected from "malicious third parties."[98] Moreover, there is a direct link between consumer confidence and the adoption of new technology, which the agency has taken into account as it formulates new policies. As former Chairman Genachowski explained, in the FCC's view, "[i]f consumers lose trust in the Internet, this will suppress broadband adoption and online commerce and communication, and all the benefits that come with it."[99] Moreover, the FCC has recognized that it can, and should, play a major role in protecting privacy and consumer confidence in the Internet, including working with industry members to provide best practices for security[100] and encouraging broadband adoption.[101] The next logical step is for Congress to authorize the FCC to further develop Internet privacy principles in the context of protecting consumers from NSA monitoring of their Internet communications and access of the Internet providers' infrastructure to do so.

2. FCC oversight of the NSA could confer significant benefits.

The lack of oversight indicates the need for a solution that is publically visible but would not undermine national security: due to its relevant expertise, the FCC is that solution. First, there are benefits specific to the FCC's area of expertise which make it well-suited to provide insight into the data collection regarding the public good and communications infrastructure. Second, the FCC's unique insights into the technological aspects of the Internet put the agency in a position to be uniquely helpful to congressional oversight committees. Moreover, the FCC is also particularly well-suited to

97. Framework For Broadband Internet Serv., *Notice of Inquiry*, FCC 10-114, 25 FCC Rcd. 7866, 7883–84, para. 39 (2010), *available at* https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-114A1_Rcd.pdf (citing Appropriate Framework for Broadband Access to the Internet over Wireline Facilities, *Report and Order and Notice of Proposed Rulemaking*, FCC 05-150, 20 FCC Rcd. 14853, 14930, para. 148 (2005)).

98. *Consumer Online Privacy: Hearing Before the S. Comm. on Commerce, Sci. & Transp.*, 111th Cong. 4 (2010) (statement of Hon. Julius Genachowski, Chairman, FCC).

99. *Id.*

100. *Id.* Chairman Genachowski noted that, "[a]s the nation's expert agency on communications, the FCC has a long history of engagement on network reliability and security, working with commercial communications providers, wired and wireless, to develop industry-based, voluntary best practices that improve security and reliability." *Id.*

101. *Id.*

provide oversight consistent with plans advocated by the PCLOB: for instance, specially providing the FISA Court with useful and insightful amicus curiae briefs.[102]

There are significant benefits to the FCC being the agency to provide insight into the NSA's monitoring activities. The NSA gets the information it collects from "major Internet switches" and depending on the type of surveillance, does not have to notify the companies from which it collects data.[103] However, the FCC could, with additional congressional authority, provide insight into basic statistics about the information collected by the NSA: for instance, volume, requiring the NSA to at least show patterns (i.e., the "relationship mapping" aspects).[104] This could be beneficial to the national security mission: by providing a volumetric, technical analysis, based on practices that can be described, the FCC could help focus the NSA's data collection, and thereby contribute to the effort to reduce overcollection, as well as provide a grounds for congressional monitoring and more effective court cases.[105] Moreover, the FCC routinely deals with sensitive information and collecting public comments.[106] For instance, the FCC often makes certain pieces of information confidential in its proceedings. Recently, the agency issued protective orders in its comment-seeking proceeding regarding the Technological Transition of the Nations Communications Infrastructure.[107] This experience would facilitate the FCC acting as a bridge between the NSA and its oversight mechanisms.

Additionally the PCLOB report calls for a similar oversight scheme.[108] The PCLOB, in its first report, calls for the government to work with Internet service providers and other companies that regularly receive FISA

---

102. It is important to note that this would not be the same as the FCC pursuing litigation on its own, rather than being overseen by the DOJ. *See* 28 U.S.C. § 516. The FCC would not be pursuing litigation on its own, but rather acting as an independent viewpoint to add context to the NSA's representations to the FISA Court. *See* PCLOB REPORT II, *supra* note 52, at 143.

103. Gellman & Soltani, *supra* note 2.

104. *See also* PCLOB REPORT II, *supra* note 52, at 146-47. Statistics such as those discussed by the PCLOB could be a template for FCC collection.

105. *See* PCLOB REPORT I, *supra* note 60, at 15. The PCLOB notes that "for the executive branch . . . disclosures about key national security programs that involve the collection, storage, dissemination of personal information . . . show that it is possible to describe practices and policies publicly, even those that have not otherwise been leaked, without damage to national security or operational effectiveness." *Id.*

106. *See e.g.*, AT&T Petition to Launch a Proceeding Concerning the TDM-to-IP Transition, *Second Protective Order*, DA 14-273, 29 FCC Rcd. 2022 (2014) [hereinafter *Second Technology Transitions Order*], *available at* https://apps.fcc.gov/edocs_public/attachmatch/DA-14-273A1_Rcd.pdf.

107. *Id.* The agency noted that "we expect to examine information provided by service providers, and others, that may be highly confidential. We anticipate that such information will be necessary to develop a more complete record on which to base the Commission's evaluation of the real-world applications of planned changes in technology that are likely to have tangible effects on consumers." *Id.*

108. PCLOB REPORT I, *supra* note 60, at 19.

production orders to develop rules permitting the companies to voluntarily disclose certain statistical information.[109] Additionally, the PCLOB recommends that the government publicly disclose detailed statistics to provide a more complete picture of government surveillance operations.[110] The PCLOB also recommends that independent experts as well as telecommunications service providers help assess at least one data collection technique.[111] The FCC regularly interacts with these companies in its own rulemaking proceedings, and would therefore be in a position to facilitate independent expertise being utilized in assessing the efficacy of the collection.[112] This is not only because the agency works with the companies and the infrastructure involved already,[113] but also because the FCC's general technical expertise places the agency in a position to consider what types of statistics would be helpful to the public. The need for expertise in determining the technical aspects of whether the data being collected is authorized is not limited to DOJ and NSA efforts, but extends to the FISA Court.

In its first report, the PCLOB calls for Congress to enact legislation enabling the FISA Court to hear independent views.[114] While a federal agency rather than an "independent" entity, the FCC would be particularly well-suited to bolster the outside input and provide the FISA Court with information regarding the impact on telecommunications, particularly the Internet, of NSA surveillance of the American public. The FCC would be a particularly helpful independent view to involve in the FISA Court proceedings because of its technical expertise. Furthermore, the FCC has significant experience dealing with sensitive information, such as trade secrets.[115] Both these traits make the agency particularly well-suited to provide helpful insights to the FISA Court.

---

109. *Id.* Indeed, telecommunications and tech companies are actively trying to be allowed to disclose such information. Ryan Gallagher, *Tech Giants Unite in Court Fight Against Government Surveillance Secrecy*, SLATE (Sept. 10, 2013, 5:26 PM), http://www.slate.com/blogs/future_tense/2013/09/10/yahoo_google_facebook_microsoft_fight_for_permission_to_release_data_about.html.

110. PCLOB REPORT I, *supra* note 60.

111. PCLOB REPORT II, *supra* note 52, at 143-44. The PLCOB expressly recognized there is an increased risk that the government will acquire wholly domestic communications during upstream collection. *Id*. at 143. As such, the PCLOB recommends the NSA, and the DOJ should, consult with telecommunications service providers and, when appropriate, utilize independent experts to periodically assess the efficacy of filtering techniques. *Id.*

112. *See Second Technology Transitions Order*, *supra* note 106; *see also* Telecommunications Act of 1996, Pub. L. No. 104-104, § 222, 110 Stat. 56 (codified as amended at 47 U.S.C. § 222) (directing telecommunications carriers to "protect the confidentiality of proprietary information of, and relating to . . . customers").

113. Indeed, the FCC deals both with telecommunications-specific information and companies on a constant basis. *See e.g.*, *Second Technology Transitions Order*, *supra* note 106.

114. PCLOB REPORT I, *supra* note 60, at 17–18.

115. *See e.g.*, *Second Technology Transitions Order*, *supra* note 106.

IV. HOW THE FCC SHOULD ADDRESS THE NSA SURVEILLANCE: IMPLEMENTING THE SOLUTION

Congress is equipped to enact legislation codifying FCC oversight of the NSA by virtue of both current law and the PCLOB's recommendations. First, the Telecommunications Act can serve as the basis for the FCC to take action to further develop its protection of consumers on the Internet, Moreover, there has been some movement in Congress calling on the FCC to take action regarding the NSA phone database, indicating the possibility of the FCC taking up an oversight role.[116] Further, Congress gave the FCC broad investigation, regulatory, and enforcement powers, as well as the privacy-focused directive of implementing Consumer Propriety Network Information protection.[117] Additionally, the first PCLOB Report calls for extensive changes in the NSA and FISA Court regime while the second report calls expressly for industry input and expertise: the FCC could facilitate some of the suggested changes through its subject matter expertise. Even as the FCC is set up to facilitate the PCLOB recommendations, Congress needs to codify the legal authority for the FCC to do this specifically. Granting express legal authority is key, as organic statutes of agencies determine what a given agency can and cannot do. Congressional authorization would be a logical outgrowth of both the FCC's regulatory interests and current legal recommendations regarding NSA oversight.

A. Congress should amend the organic statutes of the FCC and NSA and encourage participation in the FISA Court.

The lack of oversight of NSA data collection practices will continue to be problematic moving forward, as national security is an ongoing concern and technology is a large part of life in a modern society. There is need for effective and transparent oversight of the NSA's data collection. As such, Congress should act by amending the organic statutes of both the NSA and the FCC to provide the FCC with oversight authority over the NSA, and by allowing the FCC to participate as amicus curiae with the FISA Court.

116. *See* Press Release, Congressman Ed Markey, FCC Refuses to Investigate NSA Program, Predicting Likely Administration Road Blocks (May 23, 2006), *available at* http://votesmart.org/public-statement/175053/fcc-refuses-to-investigate-nsa-program-predicting-likely-administration-road-blocks; Chang, *supra* note 33, at 582.

117. *See* 47 U.S.C. § 222 (2012); *see also* Kris Anne Monteith, Chief, Enforcement Bureau, FCC, Written Statement Before the Subcommittee on Consumer Affairs, Product Safety, and Insurance on Protecting Consumers' Phone Records 2 (Sept. 29, 2006), *available at* http://www.commerce.senate.gov/pdf/monteith-020806.pdf.

1. Congress should amend the NSA organic statute to provide for collection of data by the FCC.

The NSA needs transparent and easily understood oversight. While it should not have to disclose national security information, the agency should be required to disclose basic statistics, such as how much information it is gathering, similar to Recommendation 9 in the second PCLOB Report.[118] This would at least illustrate to the public, via the FCC, that the NSA is targeting its surveillance at legitimate threats to national security—rather than performing blanket surveillance of all Internet users. Further, these reforms would comport with the PCLOB's enumerated Recommendations.[119] As of now, "lawmakers and the public do not have even a rough estimate of how many communications of U.S. persons are acquired under section 702."[120] Because the NSA is required to target foreign communications in order for its surveillance to be lawful,[121] an annual snapshot showing the volume of its surveillance will help foster some degree of transparency,[122] helping assure citizens that their privacy is not being intruded upon, without hampering legitimate national security efforts.[123]

This expanded role for the FCC in relation to the NSA should be codified by Congress. First, Congress should amend the NSA's organic statute to require the agency to comply with FCC requests for data. Additionally, while the FCC does not have the security clearance to review the substance of the surveillance, such clearance is not necessary on an agency-wide basis. Instead, Congress should require the NSA to provide targeting statistics that could be reasonably disclosed, or at least preliminary statistics that could focus the FCC's inquiry. This new legislation is all that is necessary to facilitate oversight on the NSA side, as the FCC will require most of the congressional authorization.

---

118. *See* PCLOB REPORT II, *supra* note 52, at 146. Recommendation 9, in particular, advocates the use of annual counting procedures to provide insight into the extent to which the NSA collects and utilizes communications of those located within the United States. *Id.*

119. *See* PCLOB REPORT I, *supra* note 60, at 19–20. The PCLOB recommends that the surveillance agencies work to develop rules disclosing statistical information provide a more complete picture of government surveillance operations. *Id.* In addition, the PCLOB does expressly acknowledge the usefulness of statistics to show the scope of NSA collection of communications of persons within the United States and United States citizens. PCLOB REPORT II, *supra* note 52, at 146.

120. PCLOB REPORT II, *supra* note 52, at 147.

121. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941, 59,947–48 (Dec. 4, 1981); PCLOB REPORT I, *supra* note 60, at 10.

122. *See* PCLOB REPORT I, *supra* note 60, at 19-20.

123. PCLOB REPORT I, *supra* note 60, at 15 (noting that "for the executive branch . . . disclosures about key national security programs that involve the collection, storage, dissemination of personal information . . . show that it is possible to describe practices and policies publicly, even those that have not otherwise been leaked, without damage to national security or operational effectiveness.").

2. The FCC's organic statute should be amended to allow the FCC authority over NSA data collection and participation in the FISA Court.

To enact a solution based on FCC oversight of NSA data collection, Congress should pass legislation allowing the FCC to collect information from the NSA, and to allow the FCC to submit its findings about this data to congressional oversight committees as well as the FISA Court. While novel, this solution is in keeping with the PCLOB recommendations, particularly the recommendation emphasizing the need for the NSA to publicly disclose the scope of its surveillance.[124] Moreover, it is not uncommon for agencies to have oversight authority over other agencies.[125] Thus, this type of inter-agency accountability could be codified to provide the FCC with oversight authority over NSA data collection.

Congress should first authorize the FCC to request certain types of data from the NSA. Similar to the PCLOB's recommendation,[126] this data, rather than being substantive, would be statistical; for instance, it might include data and the basic context surrounding how many communications providers from which the NSA is collecting metadata, or how many email contact lists the NSA is gathering.[127] This would thereby provide oversight over the relevancy problem, wherein the NSA collects information in such wide swaths so as not to be tied to any particularized inquiry.[128] The FCC would therefore be in a position to review the volume of information, while keeping it confidential.

The legislation should also include authorization for the FCC to interact with the other oversight bodies. Congress should give the FCC the authority to send any of the statistics that the agency finds problematic to the FISA Court and the relevant congressional committees, and should provide for the FCC to be informed of proceedings implicating data collection over which the FCC would be granted authority. Additionally, Congress should

---

124. *See id.* (noting that "for the executive branch…disclosures about key national security programs that involve the collection, storage, dissemination of personal information . . . show that it is possible to describe practices and policies publicly, even those that have not otherwise been leaked, without damage to national security or operational effectiveness.").

125. For instance, the EPA administers the National Environmental Policy Act ("NEPA") through which it requires federal agencies to incorporate environmental considerations in their planning and decision-making. *National Environmental Policy Act (NEPA)*, ENVTL. PROT. AGENCY, http://www.epa.gov/compliance/basics/nepa.html. Additionally, employment standards such as anti-discrimination policies and merit selection apply to all federal agencies. *See About EEOC*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, http://www.eeoc.gov/eeoc/; *Merit Systems Principles*, MERIT SYS. PROT. BD., http://www.mspb.gov/meritsystemsprinciples.htm.

126. *See* PCLOB REPORT II, *supra* note 52, at 146.

127. PCLOB REPORT II, *supra* note 52, at 146-47.

128. PCLOB REPORT I, *supra* note 60, at 77–78. The benefit may indeed also be in the fact that the NSA would have to think about the relevence of the large swaths of data collected.

provide a mechanism for the FCC to liaise with Congress on a regular basis *specifically* about the NSA data collection since it involves sensitive information: for instance, setting out regular reports or allowing Congress to send inquiries to the FCC as needed on the technical aspects of the NSA's methods of data collection. The language could also allow for public comment on NSA collection to some extent, modeled on the current FCC notice and comment procedures. The FCC could thereby ask for generalized comments without disclosing the exact nature of its inquiry. Thus, the FCC could solicit public comment on the underlying idea of NSA surveillance as it relates to the communications infrastructure and incorporate valid comments in its representations to the relevant oversight mechanisms. This would enable the FCC to incorporate comments by carriers and consumer interest groups into the oversight process and allow some degree of public participation without sacrificing national security.

Moreover, the legislation must include a mechanism for protecting national security information. The FCC has knowledge about the underlying infrastructure where the data is coming from as well as experience dealing with sensitive information.[129] However, there are valid concerns in disclosing *any* sort of information implicating national security. To that end, Congress may wish to consider adding a position in the FCC for an intelligence officer with clearance who can look into relevance when the amounts of data raise a red flag in the FCC's internal process for reviewing the data. Moreover, placement of a member of an NSA staffer in the FCC would facilitate inter-agency cooperation and dialogue about data collection.

For enforcement, in order to preserve national security, Congress should avoid providing the FCC any mechanism to call the NSA before it via hearing. However, the FCC would be able to report specially to the House and Senate committees, as well as petition the FISA Court as amicus curae. Additionally, if the PCLOB wants to stay involved and keep developing oversight, Congress should provide an avenue for the FCC to call forth another PCLOB investigation should the need arise.

3. Congress should allow outside parties to petition the FISA Court.

Congress should follow the PCLOB Recommendation to allow outside parties, to petition the FISA Court to put forth independent views. The PCLOB recommendation about FISA Court operations would allow for public comment.[130] While there are logistical problems with allowing other parties before the court, the PCLOB suggests that a Special Advocate could advise the FISA Court whether amicus participation would be helpful in a

129. *See Second Technology Transitions Order*, *supra* note 106.
130. *See* PCLOB REPORT I, *supra* note 60, at 17, 182.

given case.[131] Input from outside sources[132]—and, in particular, the FCC—would be useful in terms of providing technical insights into the impact of NSA surveillance on telecommunications. In particular, the FCC could be among the independent viewpoints incorporated in the continuing process of evaluating upstream and "about" collection.[133] Moreover, even if Congress decides to provide limited amicus participation, the FCC, providing volumetric data or technical expertise, could help act as a bridge between the public, parties in the communications field, and the court.

The FISA Court itself considers each and every surveillance application fastidiously, but the public needs to have the same confidence in the court's impartiality and rigor as those government actors who interact with or serve on the court.[134] While there is need for secrecy due to national security concerns, there is also the need for the court to take into account a greater range of views and legal arguments, as well as receive technical assistance and legal input from outside parties.[135] The PCLOB report indicates that, while there are difficulties in inviting amicus participation by parties lacking national security clearance, such as the FCC, the fact that it has been done in one instance indicates that it is possible to invite participation from outside parties without infringing upon national security.[136]

Moreover, as mentioned above, it may be useful for Congress to create a position at the FCC in which national security clearance is granted. Not only would this create a safeguard for the integrity of national security information, but this would provide for a person who can be called before the FISA Court who could be exposed to the facts of a given case, and using

131. *Id.* at 189.

132. *See id.*; PCLOB REPORT II, *supra* note 52, at 143-44. The PCLOB discusses the usefulness of outside experts; the FCC would be in a particular position to provide independent, industry-specific insights.

133. *See* PCLOB REPORT II, *supra* note 52, at 143-44. Upstream collection occurs with the compelled assitance of the owners of the "backbone" of telecommunications (in the words of the PCLOB, the owners of backbone over which telephone and Internet communications transit, rather than with the compelled assistance of ISPs or similar companies supplying particular modes of communication). *Id*. at 7. Upstream collection includes "about" communications, where the piece of data that marks a person as a target for collection (such as their email address) is present within the communication at issue, but that person is not a party to that particular communication; rather the communication is "about" the given targeted data. *Id*. Because upstream collection includes "about" communications, the two are often referred to together. *Id.* at 143 (using the phrase "[u]pstream and '[a]bout' [c]ollection").

134. *Id*. at 182. The PCLOB notes that it interviewed three judges who served on FISA Court, and that the Board had confidence that the judges, their staff, and the government lawyers who appear before the court all "operate with integrity and give fastidious attention and review to surveillance applications," but that this needs to be shown to the public as well. *Id.*

135. *Id.*

136. PCLOB REPORT I, *supra* note 60, at 189 (citing In Re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 13-185 (Foreign Intelligence Surveillance Court Dec. 18, 2013)).

the data that has been collected and/or analyzed by the FCC, could provide insight into a particular instance.

Therefore, Congress should encourage the FISA Court to use its ability to appoint technical experts as well as passing legislation to allow for more amicus participation by outside parties.[137] Congress should enact legislation following the PCLOB recommendations with an eye towards focusing on the FCC as an expert by enacting legislation for the FCC to participate as amicus curiae before the FISA Court.

V. CONCLUSION

The FCC is in a position to provide oversight and transparency to the NSA Internet monitoring scandal. As an agency tasked with regulating the technology and communications sectors, the FCC has been keeping up with the infrastructure and development of technology vis-à-vis the Internet as it pertains to its congressional mandate and its own regulations. Moreover, there would not be an intrusion onto national security efforts because only the volume of information collected would be disclosed. The current crisis in public confidence shows that there is a place for the FCC to be an integral part of the oversight process. The FCC would focus the inquiry of the congressional oversight committees and provide the FISA Court with much-needed outside perspective and technical assistance, while simultaneously giving the public some comfort and adding transparency to the process. This inter-agency monitoring could increase accountability and public confidence in a way that traditional oversight mechanisms cannot: thus, the FCC is in a unique position to add value to the oversight of the NSA and Congress should pursue codifying this solution.

137. PCLOB REPORT I, *supra* note 60, at 13–14.