PUSH IT TO THE (CONSTITUTIONAL) LIMIT: STRENGTHENING THE NATIONAL SECURITY AGENCY'S SECTION 702 SURVEILLANCE PROGRAM

JAMES PURCE*

* 2019 J.D./M.A. Candidate, American University Washington College of Law and American University School of International Service. This Comment would not have been possible without the support of family, the thoughtfulness and assistance from the Administrative Law Review, and the invaluable guidance from Professor Andrew F. Popper.

I. INTRODUCTION

The National Security Agency (NSA) has a history of conducting surveillance activities that toe the constitutional line.[1] At the time of this writing, the American public confronts the NSA's most recent controversy: Section 702 and the intentional collection of Americans' communications.[2] Section 702 of the Foreign Intelligence Surveillance Amendments Act (FAA) is a complex statute authorizing the Executive Branch to conduct warrantless, electronic surveillance of American citizens.[3] This Section is credited with thwarting three terrorist attacks on U.S. soil, producing more than twenty-five percent of all U.S. intelligence information, and is regarded as a core national security law.[4] However, Section 702's implementation has drawn

1. *See* Jonathan D. Forgang, "*The Right of the People": The NSA, the FISA Amendments Act of 2008, and Foreign Intelligence Surveillance of Americans Overseas*, 78 FORDHAM L. REV. 217, 237 (2009) (explaining Congress's push for Foreign Intelligence Surveillance Act (FISA) amendments following the Bush Administration's disclosure that the National Security Agency (NSA) engaged in unauthorized, warrantless surveillance of U.S. citizens).

2. *See, e.g.*, James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' Emails and Phone Calls*, GUARDIAN (Aug. 9, 2013, 12:08 PM), https://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls (publishing and analyzing leaked NSA documents revealing the NSA's constitutionally problematic collection of U.S. citizens' electronic communications under Section 702).

3. Section 702 enables the government to acquire international telephone and Internet communications content in pursuit of foreign intelligence. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 104 (2014) [hereinafter PCLOB REPORT]; *see also* 50 U.S.C. § 1802 (2012).

4. *See, e.g.*, John R. Parkinson, *NSA: 'Over 50' Terror Plots Foiled by Data Dragnets*, ABC NEWS (June 18, 2013), http://abcnews.go.com/Politics/nsa–director–50–potential–terrorist–attacks–thwarted–controversial/story?id=194281480 (reporting that Section 702 thwarted terrorist attacks on the New York Stock Exchange, the New York subway, and a Danish newspaper office in Chicago); *see also* PCLOB REPORT, *supra* note 3, at 10 (explaining that over a quarter of the NSA's reports concerning international terrorism include information that is based in whole or in part on Section 702 collection, and "this percentage

strong constitutional criticism[5] and has catalyzed civil lawsuits against the NSA.[6]

On April 28, 2017, the NSA addressed the intrusiveness of its Section 702 surveillance program when it eliminated a unique Section 702 surveillance technique—"About" communications collection.[7] While the NSA's announcement signaled a conscious effort to reduce privacy intrusions on *United States persons*'[8] communications, its decision simultaneously weakened the utility of the Section 702 surveillance program.[9] Given Section 702's

---

has increased every year since the statute was enacted"); Matt Olsen, *Necessary Surveillance: "Fixes" to FISA Could Severely Harm FBI National Security Investigations*, SLATE (Nov. 27, 2017, 4:25 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2017/11/_fixes_to_fisa_could_severely_harm_fbi_national_security_investigations.html (characterizing Section 702 as "[a] core national security law" allowing the government to collect intelligence information).

5. *See, e.g.*, Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 123 (2015) (asserting that certain practices instituted under Section 702 "fall outside acceptable Fourth Amendment bounds"); Kate Poorbaugh, *Security Protocol: A Procedural Analysis of the Foreign Intelligence Surveillance*, U. ILL. L. REV. 1363, 1395 (2015) (arguing that amending the procedures of the Foreign Intelligence Surveillance Court (FISC) is the best solution to reign in Section 702 intrusiveness).

6. *See* Wikimedia Found. v. Nat'l Sec. Agency, 857 F.3d 193, 211 (4th Cir. 2017) (finding that Wikimedia Foundation had standing to sue the NSA for Section 702 surveillance techniques infringing upon the company's Fourth Amendment privacy rights); *see, e.g.*, Jessica Conditt, *Wikimedia is Clear to Sue the NSA*, ENGADGET (May 23, 2017), https://www.engadget.com/2017/05/23/wikimedia-sue-nsa-appeals-court-rules (explaining that the Fourth Circuit's decision overturned a 2015 district court finding that Wikimedia had not proved the NSA was actually spying on Wikimedia communications through its Section 702 surveillance program); David Kravets, *Wikimedia Wins Small Victory in Challenge to NSA "Upstream" Spying*, ARS TECHINCA (May 23, 2016, 6:45 PM), https://arstechnica.com/tech–policy/2017/05/wikimedia–wins–small–victory–in–challenge–to–nsa–Upstream–spying (explaining that Wikimedia Foundation learned about the NSA's Section 702 surveillance program through Edward Snowden's 2013 security leak).

7. An "About" communication is one that includes a targeted email address in the text or body of an email, even though the email is between two persons who are not themselves targets. *See infra* Section II.B.1. "About" communications are acquired through a process called Upstream collection, which refers to the NSA's instantaneous interception of Internet communications as they transit the facilities of an "Internet backbone" carrier. *Id.*

8. See *infra* note 24 and accompanying text for the definition of *United States person*.

9. According to the NSA, the elimination of "About" communications reduces "the likelihood that the NSA will acquire communications of [United States] persons or others who are not in direct contact with one of the Agency's foreign intelligence targets." *See NSA Stops Certain Section 702 "Upstream" Activities*, NAT'L SECURITY AGENCY (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml [hereinafter NSA Press Release]. The NSA announced the elimination of "About"

utility as a bona fide national security apparatus during the ongoing "war on terror," this Comment posits that the NSA should reintroduce "About" communications collection in the interest of U.S. national security.[10]

Part II provides an overview of the NSA's authority to conduct Section 702 surveillance, noting the constitutional and statutory requirements provided in Section 702 of the FAA.[11] Part III examines the NSA's implementation of its Section 702 compliance procedures as applied to "About" communications collection. Part III also demonstrates that the NSA's implementation of its Section 702 compliance procedures uncomfortably toes the line of constitutional reasonableness. Part IV recommends procedural steps that the NSA should take to reintroduce "About" communications. Finally, Part V concludes by proposing procedural enhancements that will draw the NSA's Section 702 compliance procedures more comfortably within the lines of constitutional reasonableness.

II. BACKGROUND

A. Schematic of Statutory Regulation on Electronic Foreign Surveillance

1. The Past and Current Authority of the NSA on Electronic Foreign Surveillance

In 1975, the American public learned, through the reports of an American journalist, that the Executive Branch abused American civil liberties through government sanctioned surveillance activities.[12] In response to the reports, Congress took a fresh look at the practices of U.S. intelligence

communications collection after learning that its analysts unlawfully searched "About" communications belonging to *United States persons*. *See infra* Section II.B.1.

10. "[O]ver a quarter of NSA's reports concerning international terrorism include information that is based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted." *See* PCLOB REPORT, *supra* note 3, at 10. Due to the manner in which the NSA collects "About" communications, the NSA cannot eliminate "About" communications without also eliminating a significant portion of other communications it seeks under Section 702. *Id.* at 123. For a chronological and analytical discussion of the "war on terror," *see* Kimberly Amadeo, *War on Terror Facts, Costs, and Timeline*, BALANCE (Oct. 9, 2017), https://www.thebalance.com/war-on-terror-facts-costs-timeline-3306300.

11. *See, e.g.*, 50 U.S.C. § 1801 (2012).

12. *See* Forgang, *supra* note 1, at 234 (explaining that Seymour M. Hersh revealed that the Central Intelligence Agency (CIA) conducted illegal surveillance on thousands of American citizens supporting the antiwar movement under the Nixon Administration); *see also* Seymour M. Hersh, *Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22, 1974, at A1.

agencies.[13] Congressional investigation confirmed that U.S. intelligence agents and Executive Branch members had "ignored the statutory checks" prohibiting surveillances of American citizens.[14] As a result, Congress enacted the Foreign Intelligence Surveillance Act (FISA) of 1978 for the purpose of reigning presidentially ordered surveillances back within constitutional limits.[15] The Act also established the Foreign Intelligence Surveillance Court (FISC), which continues to serve as the judicial check on the U.S. government's authority to surveil American citizens' electronic communications in the interest of national security.[16]

Today, FISA exists in a revamped form. In 2007, the intelligence community addressed a letter to Congress asking that FISA be amended to ease

---

13. *See* Forgang, *supra* note 1, at 234 (explaining that after years of abstention, Congress decided to address "the need for balance between national security interests and civil liberties protections with FISA").

14. *See id.* Between 1975–1976, Senator Frank Church led a Congressional inquiry into U.S. domestic spying. *See* Stephanie Cooper Blum, *What Really Is at Stake with the FISA Amendments Act of 2008 and Ideas for Future*, 18 B.U. PUB. INT. L.J. 269, 275 (2009) (citing Loch K. Johnson, *NSA Spying Erodes Rule of Law, in* INTELLIGENCE AND NATIONAL SECURITY, THE SECRET WORLD OF SPIES 411 (Loch K. Johnson & James Wirtz, eds., 2008)). The inquiry revealed:

> (1) [T]he FBI had conducted 500,000 investigations into alleged subversives from 1960–1974; . . . (2) the CIA had engaged in widespread mail–openings in the United States; (3) that Army intelligence operatives had conducted secret inquiries against 100,000 U.S. citizens opposed to the Vietnam War; (4) that the NSA monitored every cable sent overseas or received by Americans from 1947 to 1975; and (5) that the NSA conducted surveillance of telephone conversations of an additional 1680 citizens.

Id.

15. *See* Blum, *supra* note 14, at 275 (explaining that FISA served as the U.S. government's first statutory framework for conducting electronic surveillance pursuant to a foreign intelligence purpose).

16. The FISC maintains the authority to approve warrant requests to electronically surveil American citizens so long as it finds the following statutory requirements:

> (1) probable cause that the target is an agent of a foreign power or a foreign power . . . ; (2) probable cause that the target is using or about to use the "facility" to be monitored; (3) applicable "minimization procedures" designed to minimize the acquisition and retention, and to prevent the dissemination, of information concerning U.S. persons that is unrelated to foreign intelligence; (4) a certification that the information sought "cannot reasonably be obtained by normal investigative techniques;" (5) the Attorney General must approve the application and a high-ranking intelligence official must certify that a "significant purpose" of the surveillance is to gain foreign intelligence information.

Id. at 277; *see also* 50 U.S.C. § 1805(a)(2012).

the Executive Branch's ability to target U.S. interests abroad.[17] In 2008, Congress acquiesced to the intelligence community's request by enacting Section 702 of the FAA.[18] Through Section 702's enactment, Congress loosened the procedural restrictions governing how the NSA collects electronic communications pursuant to a foreign intelligence purpose.[19] For the purposes of this Comment, it is necessary to hone in on Section 702 and the procedural requirements imposed on the NSA.

2. Section 702 and the Procedural Compliance Framework

Section 702 permits the intelligence agencies to conduct electronic foreign intelligence surveillance so long as the FISC approves annual certifications, targeting procedures, and minimization procedures submitted by the Attorney General (AG) and the Director of National Intelligence (DNI).[20] The annual certifications specify categories of foreign intelligence information that the government is authorized to acquire under Section 702.[21] However, the targeting and minimization procedures establish the procedural and constitutional processes the NSA must follow when conducting Section 702 surveillance activities.[22] Additionally, whereas the minimization procedures outline the oversight and compliance procedures governing post-foreign surveillance acquisition, the NSA targeting procedures outline

17. *See* Donohue, *supra* note 5, at 135–36 (explaining that the Director of National Intelligence, J.M. McConnell, submitted a proposal to Congress to amend the FISA to make it easier for the Executive Branch to target U.S. interests abroad).

18. *See* PCLOB REPORT, *supra* note 3, at 5.

19. Section 702 regulates the acquisition of electronic communications pursuant to a foreign intelligence purpose. *See* 50 U.S.C. § 1881(a)(i)(2)(2012); *see also* Blum, *supra* note 14, at 279 n.64, 297–98 (explaining that the original FISA "call[s] for different treatment based on the kind of technology employed in acquiring the foreign intelligence," whereas Section 702 loosens the restrictions on the type kind of technology that must be used).

20. *See* 50 U.S.C. § 1881a(i) (explaining that the FISC is statutorily charged with reviewing and approving the Attorney General (AG) and Director of National Intelligence (DNI) certifications).

21. The specific categories for which the annual certifications authorize remain redacted. *See* NAT'L SEC. AGENCY/CENT. SEC. SERV., OFFICE OF THE INSPECTOR GEN., ST-14-0002, IMPLEMENTATION OF § 215 OF THE USA PATRIOT ACT AND § 702 OF THE FISA AMENDMENTS ACT OF 2008 70 (2015) [hereinafter IMPLEMENTATION OF § 702 REPORT] (explaining that through the annual certifications, the AG and the DNI certify that the respective intelligence agencies will abide by the accompanied targeting and minimization procedures if approved by the FISC).

22. *See id.* (explaining that the minimization procedures establish controls over the acquisition, retention, and dissemination of non-public *United States person* information, whereas the targeting procedures establish the controls for the manner in which the NSA determines that a person targeted is a non-*United States person* not located in the United States).

oversight and compliance procedures governing pre-foreign surveillance acquisition.[23] Ultimately the combined effect of the certifications, targeting procedures, and minimization procedures is to substantially reduce the risk that the NSA will use or disseminate information concerning *United States persons* who are not approved targets.[24]

In reviewing the AG and the DNI targeting procedures, the FISC determines: (1) whether the certifications contain all of the statutorily required elements;[25] (2) whether the targeting and minimization procedures are consistent with the statutorily prescribed requirements;[26] and (3) whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment.[27] Section 702 does not require the NSA to submit individual surveillance applications for a specific target.[28] Rather, Section 702 establishes a warrant approval system that allows for blanket surveillance approvals in the interest of national security.[29]

---

23. *See, e.g.*, *The FISA Amendment Act: Q & A*, OFF. OF THE DIRECTOR OF NAT'L INTELLIGENCE 1 (Apr. 18, 2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

24. A "*United States person*" includes U.S. citizens, legal permanent residents, unincorporated associations with a substantial number of U.S. citizens or legal permanent residents as members, and corporations incorporated in the United States. *See* 50 U.S.C. § 1801(i). It does not include associations or corporations that qualify as a "foreign power." *Id*; *see also* Memorandum Opinion & Order, No. [Redacted], at *39 (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf [hereinafter 2015 FISC Memorandum Opinion & Order] (analyzing the FISC's prior review of the NSA targeting and minimization procedures).

25. *See* 50 U.S.C. § 1881a(i)(2)(A).

26. *See id.* § 1881a(i)(2)(B) (stating that the targeting procedures must be "reasonably designed . . . to prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States"); *see also id.* § 1881a(i)(2)(C) (articulating that the minimization procedures meet the definition of minimization procedures under 50 U.S.C. § 1801(h) or § 1821(4)).

27. The FISC's approval of the AG and DNI submitted certifications is contingent on whether the targeting and minimization procedures are consistent with the requirements of the Fourth Amendment. *See id.* § 1881a(i)(3)(A).

28. Section 702 of the Foreign Intelligence Surveillance Amendments Act (FAA) "removed previous FISA requirements that required intelligence agencies to submit detailed information about the nature of the information sought and describing the person or place targeted in order to receive a warrant for that specific surveillance." Forgang, *supra* note 1, at 238 (citing 50 U.S.C. § 1804(a) (2006)).

29. *Id.* at 246 (explaining that the Section 702 blanket surveillance approvals rely on the good faith of the Executive Branch).

B. Section 702 and the Uniqueness of Upstream Internet Collection

1. The Functionality of Upstream Internet Collection

Under the Section 702 targeting and minimization procedures, the NSA is authorized to collect Internet communications through two programs: Downstream collection and Upstream collection.[30] Downstream collection requires the NSA to ask Internet Service Providers (ISPs) to provide communications sent or received by a *targeted selector*.[31] Upstream collection, on the other hand, refers to the NSA's interception of Internet communications as they transit the facilities of an "Internet backbone" carrier.[32] Under Upstream collection, the NSA first identifies a target's selector or identifier, such as an email address.[33] Next, the NSA sends that email address to a U.S. Electronic Communications Service Provider who controls an Internet backbone.[34] Then, the U.S. Electronic Communication Service Provider assists the NSA in acquiring all Internet communications associated with the selected target's email address.[35] Finally, the communications sent *to, from*, or *about* the target's email address are filtered into the NSA's Section 702 database.[36]

---

30. *See* PCLOB REPORT, *supra* note 3, at 82–86 (juxtaposing the collection methods used in Upstream and Downstream collection).

31. A "targeted selector" is a specific communications facility that is "assessed to be used by the target, such as the target's email address or telephone number." *See id.* at 32. The government provides an Internet Service Provider (ISP) with the target "selector" and "the provider is compelled to give the communications sent to or from that selector to the government." *Id.* at 7.

32. The term "Internet backbone" refers to communications transiting through circuits that are used to facilitate Internet communications. *See id.* at 36–37. Upstream communication involves the compelled assistance of telecommunications providers that control the "Internet backbone" over which telephone and Internet communications transit. *Id.* at 7; *see also* [Redacted], 2011 WL 10945618, at *26 (FISA Ct. Oct. 3, 2011).

33. *See* PCLOB REPORT, *supra* note 3, at 36 (explaining that selectors tasked for Upstream Internet transaction collection must be specific selectors, such as an email address of the targeted individual).

34. *Id.* at 37 (explaining that U.S. service providers are compelled to assist the government in acquiring communications across the Internet backbone).

35. Upstream collection occurs as communications flow "Upstream" between communication services providers, whereas Downstream collection occurs as the local telephone company or email provider provides the communication with whom the target interacts. *See id.* at 35.

36. To identify and acquire Internet transactions associated with the Section 702–tasked selectors on the Internet backbone, Internet transactions are first filtered to eliminate potential domestic transactions, and then are screened to capture only transactions containing a tasked selector. *See id.* at 37. Internet communications are not ingested into govern-

While Upstream and Downstream collection methods are similar in that they both involve the interception of communications *to* or *from* a selected target, Upstream collection is distinguishable in that it also captures any Internet communications containing mere references to the target's email address.[37] For example, if the NSA were using a name "John Smith" as a target identifier, under the Upstream collection program, the NSA would collect foreign intelligence-related communications in which that name appeared in the body of the communication.[38] Consider that two known terrorists are communicating via e-mail,[39] and one terrorist says to the other: "We should recruit Smith."[40] That e-mail is subject to Upstream collection and would be classified as an "About" communication because the email is *about* "John Smith."[41] Conversely, under Downstream collection, the NSA would not collect the terrorist's email mentioning "John Smith" because Downstream only collects e-mails *to* and *from* "John Smith," but not *about* "John Smith."[42]

Unlike Downstream collection, Upstream collection incidentally acquires additional communications that are not *to*, *from*, or *about* a specific target.[43] For example, if two known terrorists exchange ten emails where one email references "John Smith," Upstream's "About" communications technique permits the NSA to collect not only the discrete communication about "John Smith," but also the other nine emails in the terrorists' email chain.[44] Accordingly, "About" communications makes Upstream collection more likely to collect information that may contain no foreign intelligence val-

---

ment databases unless the communications pass both screens. *Id.*

37. *Id.* at 7 (explaining that "an 'About' communication is one in which the selector of a targeted person (such as that person's email address) is contained within the communication but the targeted person is not a participant in the communication").

38. For a helpful illustration regarding "About" communication collection, *see* Paul Rosenzweig et al., *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, HERITAGE (May 13, 2016), http://www.heritage.org/defense/report/maintaining–americas–ability–collect–foreign–intelligence–the–section–702–program.

39. *Id.*

40. *Id.*

41. *Id.*

42. *Id.*

43. *See* NAT'L SEC. AGENCY/CENT. SEC. SERV., OFFICE OF INSPECTOR GEN., ST-11-0009, REP. ON THE SPECIAL STUDY: ASSESSMENT OF MANAGEMENT CONTROLS OVER FAA § 702 8 (2013) [hereinafter OIG SPECIAL STUDY] (explaining that Upstream Internet collection acquires the discrete communication where the target is referenced, but also acquires the entire email chain, including communications where the selected target is not the sender, receiver, or mentioned in the communication).

44. *Id.*

ue.[45] As a result, Upstream collection is more likely than Downstream collection to acquire communications that may contain no foreign intelligence value.[46]

2. The NSA's Unnecessary Abandonment of "About" Communications

On October 24, 2016, the NSA revealed that it had erroneously infringed on an undisclosed number of *United States persons'* privacy interests.[47] The NSA reported that its analysts erroneously used known *United States person* identifiers to query Upstream acquired information.[48] Specifically, the NSA revealed that it had erroneously used *United States person* email addresses, telephone numbers, and other key words and phrases to search Section 702 Upstream Internet data.[49] The NSA's report proved problematic considering that the NSA was explicitly prohibited from querying Upstream information using *United States person* identifiers and that the purpose of that prohibition was to protect the individual privacy interests of *United States persons*.[50] Following internal reviews, the NSA ultimately attributed the Up-

45. *Id.*

46. *Id.*

47. *See, e.g.*, Jordan Brunner et al., *Foreign Intelligence Surveillance Court Approves New Targeting and Minimization Procedures: A Summary*, LAWFARE (May 15, 2017, 12:13 PM), https://lawfareblog.com/foreign-intelligence-surveillance-court-approves-new-targeting-and-minimization-procedures-summary (summarizing the FISC's findings regarding the 2017 NSA targeting and minimization procedures); *see also* Memorandum Opinion & Order, No. [Redacted], at *4 (FISA Ct. Apr. 26, 2017), https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf [hereinafter 2017 FISC Memorandum Opinion & Order] (explaining that the NSA's reported querying errors raise a serious Fourth Amendment issue).

48. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *19–23 (explaining the timeline for which the NSA reported its querying issues to the FISC); *see also* PCLOB REPORT, *supra* note 3, at 55 ("[A] 'query' refers to any instance where data is searched using a specific term or terms for the purpose of discovering or retrieving . . . Section 702–acquired data.").

49. *See* PCLOB REPORT, *supra* note 3, at 55.

50. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *81 (explaining that the NSA Minimization Procedures, Section 3(b)(5), explicitly prohibit NSA analysts from using *United States person* identifiers to query Section 702 Upstream information); *see also* [Redacted], 2011 WL 10945618, at *26 (FISA Ct. Oct. 3, 2011) (explaining that queries using *United States person* identifiers of Upstream information exceed the constitutional bounds of the Fourth Amendment because they unreasonably intrude on non-target *United States persons'* privacy interests); NAT'L SEC. AGENCY, EXHIBIT B: MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 3(b)(5) [hereinafter 2016 NSA MINIMIZATION

stream querying issues to human error and system design issues.[51] As a result, the NSA proposed eliminating its "About" communications collection to remedy its unauthorized querying violations.[52]

On April 26, 2017, the FISC released an opinion where it reviewed the NSA's proposal to eliminate "About" communications, as well as the constitutionality of the NSA's implementation procedures.[53] The court found that the NSA had conducted an alarming number of unauthorized queries and that the NSA had failed to promptly report the noncompliant queries per statutory requirements.[54] Nevertheless, the court concluded that the NSA's internal minimization procedures were sufficiently designed to alleviate NSA querying errors as required under the Fourth Amendment.[55] The FISC also concluded that the NSA's proposal to cease Upstream communications collection adequately remedied the noncompliant querying issues.[56]

III. ARGUMENT

A. The NSA's Weak Implementation of Post-Collection Compliance Procedures

1. Internal Procedures Designed to Prevent Unauthorized United States Person Queries

While eliminating "About" communications effectively remedied the NSA's Section 702 querying issues, abandoning "About" communications

---

PROCEDURES], https://assets.documentcloud.org/documents/3718787/ 2016-NSA-Section-702-Minimization-Procedures-Sep.pdf (stating that the NSA is prohibited from using *United States person* identifiers to query Upstream Internet information).

51. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *19–20 (explaining that the NSA informed the FISC, through a January 3 Notice, that the primary factor for the noncompliant queries was human error and system design issues).

52. *Id.* at *27–28 (explaining that NSA proposed to eliminate its Upstream "About" collection method in exchange for the ability to query all *to* and *from* Section 702 Upstream information using *United States person* identifiers).

53. The constitutional analysis focused on the NSA's implementation of its targeting and minimization procedures. *See id.* at *67.

54. The court ultimately reasoned, however, that the "extensive oversight" efforts conducted within the appropriate NSA oversight bodies "generally identified and remedied compliance issues in a timely and appropriate fashion." *Id.* at *67–68.

55. *Id.* at *66 (asserting that the FISC "evaluates the reasonableness of 'the program as a whole,'" rather than individual actions and that "the controlling norms are ones of reasonableness and perfection").

56. *Id.* at *28 (asserting the Court's agreement that the removal of "About" communications eliminates the types of communications presenting the Court with the "greatest level of constitutional and statutory concern").

collection was not constitutionally or statutorily necessary.[57] The NSA has implemented procedures designed to provide reasonable assurance of compliance with Section 702 of the FAA *after* the collection of "About" communications.[58] These internal procedures and controls include training, access control, multiple levels of review, and oversight.[59] For example, the NSA implemented courses on Section 702, which include training on how to properly use *United States person* identifiers to query Section 702 data.[60] The NSA's procedures restrict analysts from querying or receiving Section 702 information unless the analysts have successfully completed the training program.[61] NSA analysts that have successfully completed the training are then granted authorization to query Section 702 data.[62]

Authorization allows NSA analysts to conduct two types of queries using *United States person* identifiers: metadata and content queries.[63] For metadata queries, the NSA analyst is required to document the basis for their metadata query prior to conducting it.[64] NSA analysts are not required, however, to obtain approval prior to running the metadata query.[65] Con-

57. The FISC did not instruct the NSA to abandon "About" communications, nor did it find that the NSA's "About" communication minimization procedures violated the Constitution. *See id.* at *29, *67.

58. *See* OIG Special Study, *supra* note 43, at iii (explaining that pursuant to the NSA targeting and minimization procedures, the NSA has established internal protocols designed to detect and prevent NSA analysts' queries using *United States person* identifiers).

59. *Id.* at 3–4.

60. The training procedures inform NSA analysts that: (1) queries of Upstream Internet collection using *United States person* terms are prohibited; (2) queries of metadata are not subject to preapproval, but the query and foreign intelligence justification must be documented; (3) content queries using *United States person* terms follow request and documentation procedures and are subject to preapproval by the NSA Oversight and Compliance Office, and (4) that the NSA Oversight and Compliance Office maintains records of all queries using *United States person* identifiers for its query review. *See* IMPLEMENTATION OF § 702 REPORT, *supra* note 21, at 107–10.

61. Prior to completing the requisite training, the NSA limits access to whole databases by "tagging" "each acquired communication with the legal authority under which it was acquired, and then . . . [implements] systems that [prevent] an analyst from accessing or querying data acquired under a legal authority for which the analyst does not have the requisite training . . . ." *See* PCLOB REPORT, *supra* note 3, at 55–56.

62. *Id.* at 55–56 (noting that after successful completion of the Section 702 training program, NSA analysts are granted access to Section 702 databases and are given the authority to query Section 702 for "foreign intelligence information").

63. *Id.* at 129 (clarifying that content queries involve a search of the content, whereas metadata queries involve information associated with the communications).

64. *Id.* at 57.

65. *Id.* at 130 (explaining that NSA analysts, alternatively, "must supply a written justification for the query and all queries are recorded and subject to audit").

versely, for content queries, NSA analysts must request and document foreign intelligence justifications for using a *United States person* identifier and await preapproval from NSA oversight bodies before running the query.[66] Once approval is granted for the content query, the analyst is free to use that *United States person* identifier to query the Section 702 database.[67] "Although metadata queries are not subject to preapproval, the query and [the] foreign intelligence justification must be recorded to support external oversight."[68] Content queries using *United States person* identifiers, on the other hand, are subject to preapproval by the NSA compliance offices.[69]

While the training program and authorization procedures restrict who can access Section 702 Upstream data, the NSA procedures do not effectively prevent NSA analysts from conducting unauthorized Upstream queries.[70] Currently, the NSA does not possess technology that can distinguish between Upstream and Downstream collected data, so inquiry collections are not separated into two distinct repositories.[71] Because there is no technological solution for separating Section 702 data into distinct repositories, the NSA relies heavily on its analysts' ability to craft queries that will only return authorized non-Upstream information.[72] Consequently, if a trained NSA analyst uses a *United States person* identifier that inadvertently returns Upstream information, nothing will stop that query from occurring.[73]

---

66. *Id.* at 57.

67. *Id.*

68. *See* IMPLEMENTATION OF § 702 REPORT, *supra* note 21, at 110–11 (explaining that the CIA and Federal Bureau of Investigation (FBI) submit requests tasking prospective targets and that the NSA reviews and approves the foreignness information and the foreignness justification for the prospective target).

69. *Id.* at 110 (asserting that the NSA's Signals Intelligence Directorate office is charged with approving content queries using *United States person* identifiers).

70. NSA analysts are trained to craft complex Section 702 queries that are "reasonably likely to return foreign intelligence information." *See* PCLOB REPORT, *supra* note 3, at 56. While NSA analysts are educated on the prohibited use of *United States person* identifiers, no technological procedures prevent an NSA analyst from using a *United States person* identifier to return unauthorized Upstream information. *See id.* at 56–57.

71. The NSA "houses" all Section 702 data, both Upstream and Downstream in one repository system. *Id.* at 55. The government has not been able to design a technological filter that can segregate *to* and *from* Upstream communications from "About" Upstream communications. *Id.* at 85.

72. The NSA trains its analysts on how to craft queries that limit the return of unauthorized data, but has not implemented technological barriers preventing an ill-crafted query from returning unauthorized Upstream information. *See id.* at 56–57.

73. NSA analysts are verbally prohibited from using unapproved *United States person* identifiers when querying Upstream data but are not technologically or physically prohibited from using unapproved *United States person* identifiers when querying Upstream data. *See id.*

The NSA has instituted an auditing system as an additional safeguard against unauthorized *United States person* queries.[74] Auditors first examine queries to determine whether the queries have a "valid foreign intelligence purpose."[75] Auditors then evaluate whether queries were constructed to avoid obtaining information on *United States persons*.[76] While the NSA requires that all *United States person* identifier queries be recorded and subjected to audits, the audit does not proactively or retroactively identify whether unapproved *United States person* queries have been used to query Upstream Internet data.[77] Rather, the audit system merely allows auditors to review whether NSA analysts have provided the proper justifications for using a *United States person* identifier to query general Section 702 data.[78] As a result, NSA auditors, analysts, and additional oversight personnel can only be apprised of unauthorized *United States person* queries if the NSA analyst possesses the competency to identify and self-report when a query has returned unauthorized information.

The reality is clear: the NSA has no way to prevent inadvertent, unauthorized queries, technologically or physically, through its implemented procedures.[79] The procedures are neither perfect nor reasonable in minimizing Section 702 queries using *United States person* identifiers that return unauthorized Upstream information.[80] Moreover, there is no guarantee that an NSA analyst will identify that he crafted a query that is unauthorized or that he will properly identify and report that event as a noncompliant incident.[81] There is also no guarantee that the auditors will be able to detect the unauthorized query, thus limiting the NSA's ability to accurately and efficiently report noncompliance incidents to the proper oversight channels.[82] Considering the NSA's lack of safeguards designed to reasona-

---

at 57; *see also* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *81–82 (explaining that violations resulted from NSA "analysts not recognizing the need to avoid querying datasets for which querying requirements were not satisfied or not understanding how to formulate queries to exclude such datasets.").

74. *See* IMPLEMENTATION OF § 702 REPORT, *supra* note 21, at 108–09 (explaining that queries using approved *United States person* identifiers are subject to review by an auditor).

75. *Id.* at 108 (asserting that all queries must be "driven by a foreign intelligence purpose").

76. *Id.* (explaining that "[t]he review is intended to balance the pursuit of foreign intelligence and protection of [*United States persons'*] Fourth Amendment rights.").

77. *See* PCLOB REPORT, *supra* note 3, at 56 (asserting that the NSA is required to record all queries of Section 702 acquired data and that these records are subject to audit).

78. *Id.* at 26.

79. *See supra* notes 58–78 and accompanying text.

80. *Id.*

81. *See supra* note 73 and accompanying text.

82. The NSA auditing procedures are designed to detect *United States person* identifiers

bly prevent unauthorized *United States person* queries, it follows that the NSA's current procedures lack strength in minimizing privacy intrusions incurred through unauthorized Section 702 Upstream queries.

2. Toeing the Constitutional Line of Reasonableness

Under Section 702, the NSA is obligated to report directly to the FISC immediately after it learns Upstream Internet data has been queried using a *United States person* identifier.[83] Under the approved Section 702 procedures, any Upstream query using a *United States person* identifier constitutes a compliance incident.[84] Whether that incident constitutes an illegal search, however, depends on whether the NSA's implementation procedures are reasonable under the Fourth Amendment.[85] The Supreme Court holds that the touchstone of the Fourth Amendment is reasonableness.[86] Courts adjudicating the reasonableness of a particular governmental action must weigh the action's intrusion upon an individual's privacy against the need for that action to promote legitimate government interests.[87] When the relevant government interest is national security, it is of the highest magnitude.[88] Accordingly, courts are unlikely to find a particular national security action unconstitutional unless the protections in place for individual privacy interests are insufficient to alleviate the risks of government error and abuse.[89]

---

approved for use, but no audit system exists for Section 702 queries using unapproved *United States person* identifiers. *See* IMPLEMENTATION OF § 702 REPORT, *supra* note 21, at 108–09; *see also* 2015 FISC Memorandum Opinion & Order, *supra* note 24, at *25–26 n.22 (explaining that the Department of Justice (DOJ) and the Office of the Director of National Intelligence (ODNI) review all *United States person* identifiers approved for use in querying contents of Section 702 communications, but that no such review exists for unapproved *United States person* identifiers).

83. *See* IMPLEMENTATION OF § 702 REPORT, *supra* note 21, at 89–90 (explaining the procedures regarding reportable NSA compliance incidents).

84. *See* 2016 NSA MINIMIZATION PROCEDURES, *supra* note 50, at § 3(b)(5).

85. *See* PCLOB REPORT, *supra* note 3, at 96.

86. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2482 (2014) (explaining that the reasonableness of the Fourth Amendment affords citizens the right to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures); *see also* U.S. CONST. amend. IV.

87. *See, e.g.*, Wyoming v. Houghton, 526 U.S. 295, 300 (1999).

88. *See* In re Directives, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008); *see also* Haig v. Agee, 453 U.S. 280, 307 (1981) (explaining that it is "obvious and unarguable" that no governmental interest is more compelling than the security of the nation).

89. *Id.*; *see In re Directives*, 551 F.3d at 1012 (determining that in balancing privacy interests and national security governmental activities, the constitutional scales will tilt in favor of upholding the government's actions so long as the protections in place for individual privacy

In assessing the constitutionality of Section 702 minimization procedures, the FISC must examine how the procedures will be implemented.[90] Next, the FISC must consider steps taken pursuant to the minimization procedures to limit the *United States person* queries of acquired Section 702 data.[91] If the internal minimization procedures cannot be conducted in a manner consistent with the Fourth Amendment, the FISC is required to determine that the implementing agency's actions do not satisfy the reasonableness requirement of the Fourth Amendment.[92]

Conversely, even if the core of the Section 702 program falls within the constitutional limits of the Fourth Amendment, the program as a whole can be pushed beyond the threshold of reasonableness if "a particular feature of the program or any particular combination of features do not reasonably minimize intrusions on a person's privacy."[93] For example, in 2011 the FISC considered whether the NSA's targeting and minimization procedures, as applied to Upstream collection, satisfied the requirements of the Fourth Amendment.[94] In finding that the NSA's minimization procedures maximized rather than minimized the retention of non-target *United States person* information, the FISC concluded that the proposed NSA targeting and minimization procedures were inconsistent with the requirements of the Fourth Amendment.[95] The FISC's opinion echoed the principle that protections built into the system at the back-end to limit the acquisition, use, dissemination, and retention of *United States persons'* communications are

---

interests are sufficient in light of the governmental interest at stake).

90. *See* 50 U.S.C. § 1881a(i)(3)(A) (2012); *see also* 2015 FISC Memorandum Opinion & Order, *supra* note 24, at *10 (noting that FISC's review of the targeting and minimization procedures under Section 702 are not confined to the procedures as written; instead the court examines how the procedures will be implemented).

91. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *63–64 (explaining that revised NSA procedures must subject the NSA's use of *United States person* identifiers "to the same limitations and requirements that apply to its use of such identifiers to query information acquired by other forms of Section 702 collection").

92. *See* 50 U.S.C. § 1881a(b)(5) (mandating that the NSA minimization procedures cannot be conducted in a manner that is inconsistent with the Fourth Amendment of the Constitution).

93. *See* PCLOB REPORT, *supra* note 3, at 96–97 (stating that "at the very least, too much expansion in the collection of [United States] persons' communications or the uses to which those communications are" deployed may push Section 702 over the constitutional line).

94. *See* [Redacted], 2011 WL 10945618, at *5 (FISA Ct. Oct. 3, 2011).

95. *Id.* at *27 (explaining that because of the limited review of "About" communications, as well as the difficulty of identifying protected information within "About" communications, the NSA's ability to query Upstream information using *United States person* identifiers seems "to enhance, rather than reduce, the risk of error, overretention, and dissemination of non-target information").

significant when adjudicating the constitutionality of NSA implementation procedures.[96]

It is undisputed that the NSA's Upstream Internet queries using *United States person* identifiers constitute a Section 702 noncompliance incident.[97] Nor is there a dispute that the government, on behalf of the NSA, toed the line of constitutional reasonableness when it made materially inaccurate representations to the FISC.[98] Nevertheless, the most relevant issue is one the FISC did not substantively address: whether the NSA implemented its internal oversight framework to reasonably identify and report unauthorized Section 702 Upstream queries of non-targets using *United States person* identifiers.[99]

While the NSA's implementation of Section 702 is a complex endeavor for which the minimization procedures impose "detailed rules concerning retention, use and dissemination," the NSA's weak querying procedures push Section 702 close to the line of constitutional unreasonableness.[100] Drawing the NSA's querying procedures more comfortably within the sphere of constitutional reasonableness requires enhanced internal procedures that can reasonably minimize *United States person* identifier queries that return unauthorized Section 702 Upstream information.[101] Any enhanced querying procedures regarding Section 702 "About" collection need not be perfect; rather, they merely need to be reasonable.[102]

---

96. *See* Donohue, *supra* note 5, at 205 (asserting that the totality of the circumstances test must take into account the scanning of content for information in "About" selectors/targets); *see also* PCLOB REPORT, *supra* note 3, at 96 (applying a holistic inquiry to the Section 702 program "requires examining a web of factors bearing on the collection, use, dissemination, and retention of the communications of [United States] persons under the program").

97. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *66–67; *see also [Redacted]*, 2011 WL 10945618, at *26.

98. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *19 (asserting that the NSA's failure to report the frequency in which NSA analysts had been conducting unauthorized Upstream surveillance raised a "serious Fourth amendment issue").

99. *See id.* at *67–68 (concluding that it "appears" compliance issues are "generally identified and remedied" and declining to substantively address the NSA's implementation of its procedures).

100. *See id.* at *67.

101. The NSA is required to ensure Section 702 Upstream acquisition is conducted in a manner designed, to the greatest extent feasible, to minimize the acquisition of information not relevant to the authorized purpose of the acquisition. *See generally* OIG Special Study § 702, *supra* note 43, at 41.

102. *See* 2015 FISC Memorandum Opinion & Order, *supra* note 24, at *45 (explaining that for Section 702 constitutional examination "the controlling norms are ones of reasonableness, not perfection" under both Section 702 and the Fourth Amendment).

IV. RECOMMENDATION

A. Reintroducing "About" Communications

1. Clearing the Five Congressional Hurdles

On January 18, 2018, Congress reauthorized Section 702 of the FAA and provided a roadmap to reintroduce "About" communications collection.[103] According to Congress's 2018 Reauthorization Bill, "About" communications collection may only be reintroduced if the AG and the DNI obtain authorization directly from Congress.[104] On a macro level, the AG and DNI must: (1) submit a written notice of intent to the Senate and House Select Committees on Intelligence,[105] and (2) wait a thirty-day period for the Senate and House Select Committees to conduct a review of the written notice.[106] On a micro level, the written notice must include: (1) a copy of any certification submitted to the FISC that authorizes the intentional acquisition of "About" "communications;[107] (2) the decision, order, or opinion of the FISC approving such certification;[108] (3) a summary of the protections for detecting material breaches;"[109] (4) any data demonstrating that the "About" communication acquisition method will be in accordance with FISA;[110] and (5) a statement indicating that no intentional Section 702

103. *See* 50 U.S.C. § 1881a (2012), *amended by* FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018).

104. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118 § 103(b)(2)(A)–(C), 132 Stat. 3, 10-12 (explaining that the AG and ODNI may not implement the authorization of the intentional acquisition of "About" communications before the end of a thirty-day congressional review period).

105. The AG and the DNI must submit to the Committee on the Judiciary and the Select Committee on Intelligence of the Senate and the Committee on the Judiciary and the Permanent Select Committee on Intelligence of the House of Representatives a written notice of the intent to authorize "About" communication acquisition, as well as supporting materials in accordance with the subsection. *Id.* § 103(b)(2)(A).

106. During the thirty-day period beginning on the date written notice is submitted, the Senate and House committees will "hold hearings and briefings and otherwise obtain information in order to fully review the written notice." *Id.* § 103(b)(2)(B).

107. *Id.* § 103(b)(3)(A) (explaining that a copy of any certification submitted to the FISC must include "all affidavits, procedures, exhibits, and attachments").

108. *Id.* § 103(b)(3)(B).

109. *Id.* § 103(b)(3)(C); *see also id.* § 103(b)(1)(B) (defining material breach as "significant noncompliance with applicable law or an order of the Foreign Intelligence Surveillance Court concerning any acquisition of abouts communications").

110. Such data must be provided if the "data or other results . . . exist at the time the written notice is submitted and were provided to the Foreign Intelligence Surveillance Court." *Id.* § 103(b)(3)(D).

"About" collection will occur until after the review period.[111]

The Reauthorization Bill affords the AG and DNI flexibility to present past or future FISC certifications authorizing "About" communications collection.[112] The NSA's easiest route to reintroducing "About" communications is to present the 2015 certifications because it instantly satisfies four of the five written notice requirements.[113] The first hurdle is cleared because the 2015 certifications authorized the intentional acquisition of "About" communications and were submitted to the FISC.[114] The second hurdle is cleared because the 2015 certifications are accompanied by a FISC order approving the certifications.[115] The third hurdle is cleared because all 2015 NSA acquisition methods involving the *intentional* acquisition of "About" communications were in accordance with FISA.[116] Finally, the fifth hurdle is easily overcome because the NSA need only provide a statement that no acquisition authorized under any FISC certifications shall include the intentional acquisition of an "About" communication until after the end of the thirty-day review period.[117] With four of the five requirements satisfied, the

111. *See id.* § 103(b)(2)(C). This provision provides an exception for Emergency Acquisitions. *Id.* § 103(b)(4) (outlining requirements for emergency acquisitions of "About" communications).

112. *See id.* § 103(b)(3)(A).

113. *See supra* notes 106–112; *infra* notes 114–115 and accompanying text.

114. On July 15, 2015, the AG and DNI submitted its "2015 certifications" to the FISC. *See* 2015 FISC Memorandum Opinion & Order, *supra* note 24, at *2. The "2015 certifications" collectively refer to the certifications themselves, as well as the accompanied affidavits, targeting procedures, and minimization procedures. *Id.* The "2015 certifications" included the NSA minimization procedures authorizing the use of intentionally acquired "About" communications. *See* NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (2015), https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf [hereinafter 2015 NSA MINIMIZATION PROCEDURES].

115. *See* 2015 FISC Memorandum Opinion & Order, *supra* note 24, at *77 (issuing an order approving the use of the 2015 NSA minimization procedures); *see also* 2015 NSA MINIMIZATION PROCEDURES, *supra* note 114, § 3(b)(4) (authorizing the use of intentionally acquired "About" communications).

116. *See* 2015 FISC Memorandum Opinion & Order, *supra* note 24, at *77 (concluding that the 2015 certifications "to be implemented" comply with applicable FISA provisions); *see also* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *82 (reviewing data regarding noncompliant queries authorized under the 2015 certifications, and finding that there is no reason to believe that the 2015 certifications period coincided with "an unusually high error rate").

117. This provision is satisfied regardless of the 2015 FISC certification used. *See* FISA Amendments Reauthorization Act of 2017 § 103(b)(3)(E).

NSA will only have to provide a summary of the protections in place to detect any material breach.[118]

For the sake of argument, if the NSA decided to present Congress with a newly approved FISC certification, the path to "About" communication reintroduction would be less expedient. Unlike providing a previously authorized 2015 certification, providing a new FISC certification would leave the NSA with zero of the five written notice requirements satisfied. The NSA would have to submit new certifications, affidavits, procedures, exhibits, and attachments for the FISC's approval; and would have to wait until a FISC opinion approved that certification.[119] Even though a clear advantage of presenting all new certifications and documents is building Congressional confidence in the new procedures, that same confidence can arguably be obtained by providing new and effective protections to detect material breaches. Given the extra hurdles that would need to be cleared through this option, it follows that presenting the 2015 FISC certification is the most efficient option.

2. Protections to Detect a Material Breach

With four of the five hurdles cleared under the 2015 FISC certification package, the NSA need only provide a "summary of protections in place to detect material breaches."[120] Before addressing the protections the NSA must proffer, it is important to highlight the major player responsible for the proffer. The Office of the Director of Compliance (ODOC) is the NSA's primary vehicle for developing, directing, and executing compliance strategies and activities.[121] ODOC has the authority to develop, implement, and monitor a comprehensive mission compliance program for the agency, and it provides documentation for review by the Department of Justice and Office of the Director of National Intelligence.[122] Accordingly, ODOC will most likely lead the charge in producing "the summary of protections to detect material breaches," if the NSA opts to restore "About" communications.[123]

Under the 2018 Reauthorization Bill, a material breach is defined as "significant noncompliance with applicable law or an order of the [FISC]

118. *See id.* § 103(b)(3)(C).

119. *See supra* notes 106–111 and accompanying text.

120. FISA Amendments Reauthorization Act of 2017 § 103(b)(3)(C).

121. The Office of Director of Compliance's (ODOC's) focus is on protecting *United States persons'* privacy during the conduct of authorized NSA missions. *See* IMPLEMENTATION OF § 702 REPORT, *supra* note 21, at 128.

122. *Id.* at 127–28.

123. *See* FISA Amendments Reauthorization Act of 2017 § 103(b)(3)(C).

concerning any acquisition of ["About"] communications."[124] A major advantage in using the 2015 certifications for the written notice package is that the NSA can demonstrate that it has learned from past mistakes. The original 2016 certifications submitted to the FISC are identical to the 2015 certifications.[125] However, while the FISC approved "About" communications collection in its 2015 opinion, the FISC did not approve "About" communications in its 2016 opinion.[126] Fortunately for the NSA, the FISC clearly stated its reservations regarding the NSA's inability to prevent unauthorized queries, which are borne from the "NSA's failure to adhere fully to those [rigorous] safeguards."[127] Accordingly, any proposal to reintroduce "About" communications should address the NSA's past inability to fully adhere to "rigorous safeguards" preventing unauthorized queries.[128]

Under § 103(b)(3)(C) of the FISA Amendments Reauthorization Act, the NSA need only demonstrate that its new protections can detect "significant" noncompliance.[129] The new procedures do not need to be perfect, but rather, preventative. As evidenced above, the NSA's inability to prevent significant querying issues stemmed from the lack of proactive procedures.[130] Therefore, any proposal to bring back "About" communications should be accompanied by procedures that do what the former system could not: (1) proactively prohibit an NSA analyst from querying Section 702 Upstream information, and (2) proactively inform NSA auditors of whether a *United States person* identifier query has returned unauthorized Upstream information.[131]

B. Alternative Remedies for Minimizing Section 702 United States Person Queries

According to a leaked budget report, the NSA is afforded ten billion dol-

---

124. *See id.* § 103(b)(1)(B).

125. *See e.g.*, 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *2–3, n.1–2 (asserting that the provisions in the government's 2016 certifications mirrored the FISC-approved 2015 certifications).

126. The government's original 2016 certifications were amended and eventually approved as the 2017 certifications after the NSA revealed its inability to prevent erroneous querying errors regarding "About" communications. *Id.* at *5.

127. *Id.* at *30, n.34.

128. *See id.*

129. *See* FISA Amendments Reauthorization Act of 2017 § 103(b)(3)(C); *see also id.* § 103(b)(1)(B).

130. *See supra* Section III.A.0.

131. The NSA's safeguards are inefficient in proactively prohibiting an NSA analyst from querying Section 702 Upstream data, nor do they proactively inform NSA auditors whether a query using an unapproved *United States person* identifier returned unauthorized Upstream information. *Id.*

lars annually for its operations.[132] As of 2013, the majority of that budget was spent on "data collection, data analysis, management, facilities and support and data processing and exploitation."[133] Despite the classified nature of the NSA's current operating budget, past allocation suggests that the NSA's budget would hover around ten billion dollars for the 2017 fiscal year.[134] Operating on the assumption that similar priorities exist in 2017, it follows that the development of new Section 702 procedures is exactly what the NSA's budget is designed to fund. Accordingly, the ODOC should develop safeguards evidencing an NSA analyst's intent when crafting queries.

The proposed safeguards should demonstrate an intention to obtain non-Upstream information, while also demonstrating an intention not to retain unauthorized Upstream information. To evidence intent, NSA analysts must be required to acknowledge whether the *United States person* query is intended for non-Upstream data on the front-end, while also requiring NSA analysts to acknowledge that Upstream information has not been returned on the back-end. Evidencing intent can be achieved through an acknowledgment system that is technologically incorporated as a pop-up window. The pop-up window should appear before the analyst clicks "search," followed by another pop-up window appearing after the query returns information. For example, if the NSA analyst determines that only non-Upstream information had been returned pursuant to the *United States person* query, the NSA analyst should be required to confirm through the pop-up window and move on. If an NSA analyst discovers that unauthorized Upstream information had been returned pursuant to his query, the NSA analyst should be required to acknowledge this occurrence, close the query session, and construct a new query that does not return the unauthorized data. By requiring NSA analysts to assess queries as they are happening in real time, the NSA can show that it implemented strengthened and effective procedures designed to identify and prevent its analysts from utilizing Section 702 information that is acquired through unauthorized, statutorily prohibited queries.

Furthermore, the additional procedures should not stop at the time of the query. Utilizing its current audit system, the NSA should subject all *United States person* queries to audits that track an NSA analysts' acknowl-

---

132. Wilson Andrews & Todd Linderman, *The Black Budget: Top Secret U.S. Intelligence Funding*, WASH. POST (Aug. 29, 2013), http://www.washingtonpost.com/wp-srv/special/national/black-budget/ (providing an overview of the secret budget that is allocated to the CIA, NSA, and National Reconnaissance Office).

133. *Id.* (asserting that data collection, data analysis, management, facilities and support and data processing and exploitation comprise the four main spending categories).

134. *See id.* (asserting that the NSA's budget has steadily increased since 2004, and has hovered around ten billion dollars per year from 2010–2013).

edgment as to whether the *United States person* query returned non-Upstream results or unauthorized Upstream results.[135] For example, if the NSA analyst (1) determines that the *United States person* query returned unauthorized Upstream information, (2) closes out that search, and (3) constructs a new search, then the audit system should track that action as a compliant query.[136] On the other hand, if the NSA analyst (1) determines the *United States person* query returned non-Upstream results, (2) acknowledges that the query returned non-Upstream results, and (3) on review, the auditor later discovers the query actually returned unauthorized Upstream results, then that occurrence should be recorded and reported as a noncompliant incident. While the proposed procedure does not guarantee that all queries using *United States person* identifiers will be prevented on the front-end, this procedure allows NSA auditors to monitor and identify the frequency of which NSA analysts construct queries that return unauthorized information. The benefit of this process is that the NSA can determine which analysts are properly crafting queries, which analysts are unknowingly crafting unauthorized queries, and whether any unauthorized queries are the result of incompetence or intention.

Implementing these procedures is realistically feasible considering that the NSA already utilizes a system with similar functionality.[137] The current system requires NSA analysts to "opt-out" of querying Section 702 information when simultaneously querying multiple databases.[138] This Comment's recommended safeguard is similar in that it serves as a warning banner, but specifically for Section 702 Upstream queries using *United States person* identifiers. In this light, the acknowledgment recommendation has the potential to increase ownership and accountability on the part of the NSA analyst crafting the query and demonstrate to Congress that the NSA proactively combats unauthorized queries. Admittedly, the cost of implementing these procedures is difficult to determine given the classified nature of the NSA's technology. However, given the NSA's presumed ten-billion-dollar annual budget, coupled with the NSA's focus on data processing exploitation, it follows that the NSA has the funds to implement the above procedures.[139]

---

135. *See supra* text accompanying notes 74–80.

136. *See* PCLOB REPORT, *supra* note 3, at 130 (explaining that the current audit system tracks every *United States person* query of Section 702 information but does not specifically track Upstream queries).

137. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *21 (asserting that the NSA has utilized systems that require analysts to "opt–out" of querying Section 702 Upstream Internet data, and that such systems are "more conducive to compliance").

138. *Id.*

139. *See* Andrews & Lindeman, *supra* note 132.

Although the proposed procedures make subtle changes to the NSA's implementation procedures, such changes can go a long way in strengthening the protections that alleviate privacy risks incurred by NSA Upstream querying errors.[140] By proactively prohibiting its analysts from using *United States person* identifiers to query unauthorized information, the NSA can demonstrate a constitutionally and statutorily sufficient effort to minimize the privacy intrusions that can occur from querying Upstream data.[141] Under the proposed procedures, the NSA can support its written notice to Congress with feasible and proactive protections to detect Section 702 material breaches.

V. CONCLUSION

The revelation that the NSA had been conducting unauthorized surveillance on American citizens is likely to form the basis of future lawsuits for alleged Fourth Amendment violations.[142] However, and as seen in prior case law, the government is afforded considerable deference when carrying out national security interests that toe the line of constitutional reasonableness.[143] This Comment introduces procedural enhancements that will draw the NSA's Section 702 "About" communications technique comfortably within the lines of constitutional reasonableness. By recommending procedural enhancements, this Comment argues that the NSA can reinstate its "About" communications technique while also ensuring that American individual privacy risks are proactively minimized. Accordingly, the NSA should stop handicapping its beneficial Upstream surveillance tool, while also ensuring that the tool does not unconstitutionally infringe on the privacy interests of *United States persons*.[144]

---

140. *See* 2017 FISC Memorandum Opinion & Order, *supra* note 47, at *83 (explaining that the NSA introduced a "banner" presented to users to emphasize that *United States person* identifiers should never be used for a designated type of query, and that this implementation demonstrated increased compliance).

141. *See supra* note 105 and accompanying text.

142. *See, e.g.*, Wikimedia Found. vs. Nat'l Sec. Agency, 857 F.3d 193, 207 (4th Cir. 2017).

143. *See, e.g.*, [Redacted], 2011 WL 10945618, at *26 (FISA Ct. Oct. 3, 2011) (accepting the government's representations that NSA's Upstream collection is "uniquely capable of acquiring certain types of targeted communications containing valuable foreign intelligence information").

144. *See* NSA Press Release, *supra* note 9.