2016

Reauthorizing the FISA Amendments Act: A Blueprint for Enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities

Peter Margulies
Roger Williams University School of Law

PETER MARGULIES*

Reauthorizing the FISA Amendments Act: A Blueprint for Enhancing Privacy Protections and Preserving Foreign Intelligence Capabilities

INTRODUCTION

The reauthorization of § 702 of the FISA Amendments Act (FAA)[1] in 2017[2] will trigger a vigorous legislative debate. Under the current statute, the government

* Professor of Law, Roger Williams University School of Law; B.A., Colgate, 1978; J.D., Columbia Law School, 1981.

1. 50 U.S.C. § 1881a (2012) (amended 2015); *see* United States v. Hasbajrami, No. 11-CR-623, 2016 WL 1029500, at *4–13 (E.D.N.Y. Mar. 8, 2016) (holding that § 702 was consistent with the Fourth Amendment of the United States Constitution); United States v. Mohamud, No. 3:10–CR–00475–KI–1, 2014 WL 2866749, at *7–9, *12–27 (D. Or. June 24, 2014) (holding that § 702 was consistent with the Fourth Amendment of the United States Constitution); [Name Redacted by Court], at 36–77 (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (holding that § 702 was consistent with Fourth Amendment of the United States Constitution); *cf. In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008) (holding that the Protect America Act of 2007, a predecessor of § 702, was consistent with the Constitution). For a sampling of the extensive commentary on the FAA, compare Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings*, HOOVER WORKING GROUP ON NATIONAL SECURITY, TECHNOLOGY, AND LAW, no. 1604, Apr. 27, 2016, at 2–4, 15–19, https://www.lawfareblog.com/defense-faa-section-702-examination-its-justification-operational-employment-and-legal-underpinnings (discussing origins of the program and current legal constraints), and David R. Shedd, Paul Rosenzweig & Charles D. Stimson, *Maintaining America's Ability to Collect Foreign Intelligence: The Section 702 Program*, HERITAGE FOUND. BACKGROUNDER, May 13, 2016, at 4–7, http://www.heritage.org/research/reports/2016/05/maintaining-americas-ability-to-collect-foreign-intelligence-the-section-702-program (noting § 702's efficacy and downplaying privacy concerns), with LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE, 68–72 (Oxford Univ. Press 2016) (arguing that the FAA is a threat to privacy that has not received sustained public scrutiny because of its secrecy). *See also* Mieke Eoyang, *Beyond Privacy & Security: The Role of the Telecommunications Industry in Electronic Surveillance*, HOOVER WORKING GROUP ON NATIONAL SECURITY, TECHNOLOGY, AND LAW, no. 1603, Apr. 8, 2016, at 13–18, https://www.lawfareblog.com/beyond-privacy-security-role-telecommunications-industry-electronic-surveillance-0 (discussing proposals for reform, including requiring that upstream collection and filtering for selectors be performed by private sector firms, which will turn over to government only those communications that match particular selectors); David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, HOOVER WORKING GROUP ON NATIONAL SECURITY, TECHNOLOGY, AND LAW, No. 1601, Feb. 24, 2016, at 8–27, https://www.lawfareblog.com/trends-and-predictions-foreign-intelligence-surveillance-faa-and-beyond (discussing future issues relevant to FAA reauthorization); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1103–08 (2016) (discussing the framework for implementing § 702 and suggesting that the administrative law model is the best paradigm for protecting privacy while ensuring effectiveness of program).

must obtain approval annually from the Foreign Intelligence Surveillance Court (FISC) of a certification describing procedures for collection of communications likely to produce foreign intelligence information, in which one party is reasonably believed to be located abroad.[3] Some legislators, joined by privacy and civil liberties advocates and former government officials, want to substantially limit the government's power under the statute.[4] Others, convinced that the statute plays a vital role in identifying terrorist and other national security threats, wish to reauthorize the statute with virtually no changes.[5] This Article argues that changes to § 702 should strengthen technological safeguards for privacy, enhance transparency, and expand the public voice at the FISC, but stop short of surveillance critics' principal goal: requiring a court order for *all* queries of U.S. person data incidentally collected under the statute.

Even without taking that step, which would unduly hamper the collection of valuable foreign intelligence information, there is plenty to do in reforming § 702. First, consider the role of technology. Congress should expressly mandate that the National Security Administration (NSA) use (1) the best feasible technology to limit the incidental collection of U.S. person data, particularly through so-called "upstream" collection at internet hubs, (2) scientific validation of all of its search techniques, and (3) due diligence to determine the status of a target and whether that individual is in the United States. However, as it moves to limit undue collection of irrelevant data, Congress should recognize that dangerous gaps in relevant data might grow as technology evolves. For that reason, Congress should permit the NSA to collect data for the purpose of determining whether legitimate

2. *See* 50 U.S.C. § 1881a note (amended 2015) (setting sunset date of statute as Dec. 31, 2017).

3. *Id.* at § 1881a.

4. *See Hearing on Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties Before the S. Comm. on the Judiciary*, 114th Cong. (2016) [hereinafter *Senate Judiciary Committee May 2016 § 702 Hearing*] (statement of Elizabeth Goitein, Co-Director of Liberty & National Security Program, Brennan Center for Justice at New York University School of Law) (suggesting that Congress should require that the government seek a court order for each specific query of information on U.S. citizens, lawful residents, or persons physically located in the U.S. that is incidentally collected under the statute); *id.* (statement of Sen. Patrick Leahy) (suggesting that Congress should require that government seek a court order for each specific query of information on U.S. citizens, lawful residents, or persons physically located in the U.S. that is incidentally collected under the statute); *see also* Elizabeth Goitein & Faiza Patel, *What Went Wrong with the FISA Court*, BRENNAN CENTER FOR JUSTICE, Mar. 18, 2015, at 45–49, https://www.brennancenter.org/publication/what-went-wrong-fisa-court (setting out proposed reforms); *cf. Senate Judiciary Committee May 2016 § 702 Hearing* (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board) (recounting testimony by then Chair of the Privacy and Civil Liberties Oversight Board) (same).

5. *See* Inglis & Kosseff, *supra* note 1, at 2; *Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4 (statement of Kenneth Wainstein); *id.* (statement of Rachel Brand, member of Privacy and Civil Liberties Oversight Board) (suggesting that any changes to the program can be made without amending the statute).

surveillance targets outside the U.S. are using Virtual Private Networks (VPNs) to spoof U.S. IP addresses and thereby thwart surveillance.[6]

Congress should also mandate greater transparency. Transparency serves several purposes.[7] First, it allows Congress, the FISC, and the public to accurately assess the size, scope, and nature of intelligence collection involving U.S. person data.[8] Second, transparency also has a useful *ex ante* prophylactic effect.[9] The prospect of public exposure helps concentrate the bureaucratic mind, ensuring that officials only advance and implement programs that they can defend. Congress should require specific disclosure to the legislature of any and all instances in which the FISC concludes that the NSA has overstepped statutory bounds or that the government's lawyers have been insufficiently candid in their filings with the FISC.[10] However, transparency does increase the risk of disclosing intelligence sources and methods.[11] Furthermore, some information can be difficult to quantify and may not appreciably add to public knowledge of intelligence programs.[12] Accordingly, Congress should resist calls to require the NSA to disclose the number of U.S. person communications that it incidentally collects.[13]

In the area of judicial review, tailored reform should distinguish between two different kinds of incidental collection of U.S. person data. Upstream collection at internet hubs should be more closely regulated, as it is under rulings of the FISC and current administrative rules.[14] That regulation, which should include requiring a court order for U.S. person queries, is necessary since upstream collection is more likely to include U.S. person data that is wholly unrelated to foreign intelligence.[15] In contrast, downstream collection is *already* tailored to foreign intelligence targeting criteria;[16] as a result, the U.S. person information incidentally collected is

6. *See* Kris, *supra* note 1, at 22–24.

7. *See Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4 (statement of Elizabeth Goitein, Co-Director of Liberty & National Security Program, Brennan Center for Justice at New York University School of Law); DONOHUE, *supra* note 1, at 149–50; Goitein & Patel, *supra* note 4, at 46; Rachel Brand, *Transparency in the Intelligence Community*, LAWFARE (Nov. 2, 2015, 10:21 AM), https://www.lawfareblog.com/transparency-intelligence-community#.

8. *See infra* notes 136–37 and accompanying text.

9. *See infra* notes 138–41 and accompanying text.

10. *See infra* notes 161–70 and accompanying text.

11. *See infra* notes 145–47 and accompanying text; *see also* Brand, *Transparency*, *supra* note 7.

12. *See infra* notes 178–84 and accompanying text.

13. *See id.*

14. *See, e.g.*, *Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4 (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board); DONOHUE, *supra* note 1, at 151–52.

15. *See, e.g.*, *Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4 (statement of Elizabeth Goitein, Co-Director of Liberty & National Security Program, Brennan Center for Justice at New York University School of Law); DONOHUE, *supra* note 1, at 151–52.

16. *See* [Name Redacted by Court], at 34 (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf; *Senate Judiciary Committee May 2016 § 702*

more likely to be related to foreign intelligence information.[17] With respect to downstream U.S. person data, this Article will demonstrate that requiring a court order could hinder the timely acquisition of foreign intelligence information.[18]

In addition, FISC review of government certifications under § 702 would benefit from the presence of a robust public advocate.[19] Currently, the FISC has statutory power to appoint amici curiae to assist in its deliberations and must explain in writing why it has failed to do so.[20] An amicus curiae pushes the government toward greater clarity in its filings and prompts more precise and refined reflection by the FISC. However, the FISC's record on appointing amici continues to be spotty. A November, 2015 opinion by Judge Hogan on § 702 benefited immeasurably from the probing and diligent arguments made by amicus, Amy Jeffress, a prominent Washington D.C. lawyer with substantial national security experience.[21] However, a December, 2015, FISC opinion by Judge Hogan of the

---

Hearing, supra note 4 (statement of Rachel Brand, member of Privacy and Civil Liberties Oversight Board); PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, 93 (2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB § 702 REPORT 2014].

17. *See* [Name Redacted by Court], at 34 (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf; *Senate Judiciary Committee May 2016 § 702 Hearing, supra* note 4 (statement of Rachel Brand, member of Privacy and Civil Liberties Oversight Board); PCLOB § 702 REPORT 2014, *supra* note 16 *passim*.

18. For a contrary view from former Vice President Walter Mondale, who as Vice President regarded the original Foreign Intelligence Surveillance Act of 1978 (FISA) as a dangerous expansion of government power beyond traditional warrants to investigate criminal activity, see Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 MINN. L. REV. 2251, 2298–2301 (2016).

19. In that respect, this Article shares the views of § 702's critics and other commentators. *See* DONOHUE, *supra* note 1, at 145–46; Mondale, et al., *supra* note 18, at 2297–98; Stephen I. Vladeck, *The FISA Court and Article III*, 72 WASH. & LEE L. REV. 1161, 1176–77 (2015).

20. *See* 50 U.S.C. § 1803(i)(2) (amended 2015); *see also* [Name Redacted by Court], at 5 (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf; *In re* Application of the FBI for Orders Requiring the Production of Call Detail Records, No. [Redacted], at 24 (FISA Ct. Dec. 31, 2015),
https://www.dni.gov/files/documents/12312015BR_Memo_Opinion_for_Public_Release.pdf.

21. *See* [Name Redacted by Court], *passim* (FISA Ct. Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf; *see also* Peter Margulies, *Madison at Fort Meade: Checks, Balances, and the NSA*, LAWFARE (May 10, 2016, 12:45 PM), https://www.lawfareblog.com/madison-fort-meade-checks-balances-and-nsa# (discussing importance of Jeffress's work as amicus curiae). Another prominent lawyer, Marc Zwillinger, served as amicus curiae in a recently disclosed opinion by the Foreign Intelligence Surveillance Court of Review (FISCR), which reviews FISC decisions. *See In re* Certified Question of Law, No. FISCR 16-01, at 1 (FISA Ct. Rev. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf (holding that when court-authorized pen register device that targets metadata, such as telephone numbers, results in incidental collection of post-cut-through-digits (PCTD) – numbers, such as passwords, entered *after* placing a telephone call – such incidental collection does not violate federal statutes or the Fourth Amendment if agency rules limit use of PCTD when they constitute content, not merely call record information); *cf.* Orin Kerr, *Relative vs. Absolute Approaches to*

FISC was unduly dismissive of the need to appoint an amicus.[22] This inconsistency does not serve the court in the longer term. It also disserves Congress, the public, and the intelligence community, all of which benefit from the fullest feasible airing of different perspectives at the FISC. A broader public advocate empowered to participate in a larger range of FISC matters would enhance the FISC's deliberations.

The Article is in four Parts. Part I discusses the history of the FAA, and describes the manner in which the government collects and uses data under the statute. Part II urges legislative changes that would enhance technological safeguards for privacy in foreign intelligence collection and use. Part III discusses judicial review and other regulation of agency action under the FAA, arguing against requiring a warrant for querying U.S. person information currently collected "downstream" through internet service providers (ISPs). According to this Part, requiring a court order to query downstream collection would hamper efforts to "connect the dots" in counterterrorism efforts. Moreover, limiting FBI access to FAA data in ongoing investigations would needlessly stifle the FBI's efforts to find patterns in terrorist activity. However, to make the FISC an even more robust monitor of best practices in surveillance, this Part also argues that a more robust public advocate is vital for FISC proceedings. Finally, Part IV suggests features that would enhance the transparency of intelligence community (IC) practices for Congress, the FISC, and the public. Overall, these changes will ensure that the § 702 program remains effective, while providing greater privacy, legitimacy, and accountability.

I. THE FAA: HISTORY AND CURRENT PRACTICE

Congress enacted the FAA as a way to both enhance lawful intelligence collection and subject it to meaningful constraints.[23] Momentum for enactment of the statute started with revelations in late 2005 that the Bush administration in the wake of the 9/11 attacks had unilaterally allowed the NSA and other agencies, collaborating with the private sector, to collect both certain content information from communications made or received by U.S. persons, and metadata such as the numbers called.[24] This broad surveillance effort, conducted outside any statutory framework, was called the Terrorist Surveillance Program (TSP).[25] After a post-

the Content/Metadata Line, LAWFARE (Aug. 25, 2016), https://lawfareblog.com/relative-vs-absolute-approaches-contentmetadata-line (discussing FISCR decision).

22. *In re* Application of the FBI for Orders Requiring the Production of Call Detail Records, No. [Redacted], at 23–24 (FISA Ct. Dec. 31, 2015), https://www.dni.gov/files/documents/12312015BR_Memo_Opinion_for_Public_Release.pdf.

23. *See* Inglis & Kosseff, *supra* note 1, at 4–8.

24. *See* Kris, *supra* note 1, at 3; Shedd et al., *supra* note 1, at 2.

25. William C. Banks, *Programmatic Surveillance and FISA: Of Needles and Haystacks*, 88 TEX. L. REV. 1633, 1641–43 (2010).

disclosure interlude in which the FISC permitted a modified form of the TSP, at least one FISC judge declined to reauthorize the program, highlighting the importance of a legislative fix.[26] Congress, in a bipartisan effort including then-senator Barack Obama, first passed the Protect America Act in 2007, and followed that with the FAA in 2008.[27]

Under § 702 of the FAA,[28] the government may engage in surveillance that targets the contents of communications of non-U.S. persons reasonably believed to be located abroad when the surveillance will result in the collection of foreign intelligence information.[29] Under § 702, the government submits a certification to the FISC describing its targeting protocols, as well as minimization rules that diminish the probability that analysts will use or retain purely domestic communications or irrelevant information about U.S. persons.[30] The FISC reviews these targeting and minimization protocols, although the FISC does not approve in advance individual targets of surveillance.[31]

In addition, under § 702, foreign intelligence information that the government may acquire includes data related to national security, such as information concerning an "actual or potential attack" or "other grave hostile acts [by a] foreign power or an agent of a foreign power."[32] Foreign intelligence information also comprises information relating to possible sabotage[33] and clandestine foreign "intelligence activities."[34] Another prong of the definition is broader, encompassing information relating to the "the conduct of the foreign affairs of the United States."[35]

Commentators have often acknowledged the effectiveness of the § 702 program. For example, the Privacy and Civil Liberties Oversight Board (PCLOB), which had access to classified information in the course of its review of the program,

26. *Id.* at 1643.

27. *Id.* at 1644.

28. 50 U.S.C. § 1881a (2012) (amended 2015).

29. *Id.* at § 1881a(a). For further discussion of this subsection, see Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137, 2140 (2014); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1, 17 (2014) [hereinafter Margulies, *Dynamic Surveillance*].

30. *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD, 135–36 (Dec. 12, 2013) [hereinafter PRESIDENT'S REVIEW GROUP]. This Article defines U.S. persons as U.S. citizens and lawful permanent residents, as well as persons physically located within the U.S.

31. *Id.* at 135–36, 152–53.

32. 50 U.S.C. § 1801(e)(1)(A) (2012).

33. *Id.* at § 1801(e)(1)(B).

34. *Id.* at § 1801(e)(1)(C).

35. *Id.* at § 1801(e)(2)(B). *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990) (holding that the Fourth Amendment's Warrant Clause does not protect non-U.S. persons located outside the territorial U.S.).

recognized § 702 had consistently produced helpful information about the structure, operation, and plans of terrorist groups.[36] The President's Review Group rendered a similar opinion.[37] However, a balanced assessment of § 702 must also weigh its costs to privacy[38] and consider approaches for minimizing those costs.[39]

II. TECHNOLOGY IN THE SERVICE OF PRIVACY

Technology is a double-edged sword. Much has been written on how technology constitutes a threat to privacy.[40] Pursuant to § 702, the NSA makes use of cutting-edge technology to collect foreign intelligence information.[41] Technology can be intrusive if its uses are not controlled. However, technology can also *enhance* privacy, enabling more effective constraints on government surveillance.[42] When intelligence collection with new technology risks heightened intrusions, Congress should also insist that government use the best feasible technology to *protect* privacy.

One example of this is described in the November, 2015 FISC opinion by Judge Thomas Hogan. A recurrent theme in Judge Hogan's opinion is the use of search filters by law enforcement agencies such as the FBI to ensure that only trained

36. PCLOB § 702 REPORT 2014, *supra* note 16; *accord* Peter Swire, *U.S. Surveillance Law, Safe Harbor, and Reforms Since 2013* 10 (Ga. Tech. Scheller Coll. of Bus., Research Paper No. 36, Dec. 18, 2015); Shedd et al., *supra* note 1, at 4 (noting the PCLOB's finding "that the Section 702 program has indeed helped in the fight against terrorism."); Inglis & Kosseff, *supra* note 1, at 19–20.

37. *See* PRESIDENT'S REVIEW GROUP, *supra* note 30, at 144–45 (noting that in great majority of counterterrorism investigations since 2007 that "resulted in the prevention of terrorist attacks ... information obtained under section 702 contributed ... to the success of the investigation"). *But see* DONOHUE, *supra* note 1 (taking a more skeptical view of intelligence programs' effectiveness).

38. *See* DONOHUE, *supra* note 1, at 68–72 (noting privacy issues with § 702); *cf.* Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015) (suggesting U.S. policymakers do not adequately incorporate the costs to civil liberties in the overall assessment of program values); Rachel Brand, *What Does Effective Intelligence Oversight Look Like?*, LAWFARE (May 3, 2016), https://www.lawfareblog.com/what-does-effective-intelligence-oversight-look (stating that agencies should ask "whether they *should* engage in particular intelligence activities even if they *can* as a matter of law.").

39. *See* Ashley Deeks, *Intelligence Services, Peer Constraints, and the Law*, 7 HARV. NAT'L SEC. J 1, 2 (2015) (discussing constraining influence on U.S. of other states' intelligence services); Shirin Sinnar, *Institutionalising Rights in the National Security Executive*, 50 HARV. C.R.-C.L. L. REV. 289, 294–98 (2015) (discussing the merits of establishing units in the U.S. executive branch to foster compliance with civil and human rights).

40. *See* FRANK PASQUALE, THE BLACK BOX SOCIETY 46–47 (Harvard Univ. Press 2015); Lior Jacob Strahilevitz, *Toward a Positive Theory of Privacy Law*, 126 HARV. L. REV. 2010, 2021–22 (2013).

41. PCLOB § 702 REPORT 2014, *supra* note 16, at 117.

42. *See* John DeLong, *Aligning the Compasses: A Journey through Compliance and Technology*, IEEE SECURITY AND PRIVACY, 85–86 (July-Aug. 2014) (discussing technology that enhances compliance with legal rules); *see also* Ribert S. Litt, *The Fourth Amendment in the Digital Age*, 126 YALE L.J.F. 8, 18 (2016) (asserting that "technology can play an important role ... in protecting privacy while enabling lawful collection of information by the government.").

personnel have access to the § 702 database.[43] As Judge Hogan noted, when FBI personnel enter a query that results in a "hit" on data that those employees are not cleared to see, a search filter blocks that data, although the querying employee does receive notice that the search terms have resulted in a positive match.[44] Agencies can and do equip their software with the capability of sending alerts to supervisory personnel when an employee attempts to gain access to data without authorization.[45]

This software also facilitates audits that analyze unauthorized queries and find patterns in such incidents.[46] Improving alert and audit technology is vital to enhancing compliance with legal rules. The FISC should receive updates on the implementation of this technology as part of the certification process. In reauthorizing § 702, Congress should require that the NSA and law enforcement agencies implement the best feasible technology to perform these alert and audit functions.

Another valuable example highlighted by former PCLOB Chair David Medine is requiring the best feasible technology to reduce the incidental collection under § 702 of U.S. person information and minimize its use.[47] The NSA collects § 702 data in two forms: through specific requests to ISPs and telecommunications companies (the PRISM or downstream program) and through scanning the contents of international internet transmissions at hubs that comprise the Internet's backbone (the upstream program).[48] Upstream scanning raises the risk of acquiring purely domestic communications that the government can intentionally obtain only with a traditional warrant.[49] Without careful regulation, therefore, the scanning of upstream communications could allow the government to circumvent a large part of the Fourth Amendment's privacy protections.

The potential to collect purely domestic content arises due to the Internet's architecture and current limits on the NSA's own technological prowess.[50] The

43. *See* [Name Redacted by Court], at 28 (FISA Ct. Nov. 6, 2015) (noting that technological safeguards applicable to FBI queries of § 702 data will deny access to query information for an official who has not received proper training or is otherwise not authorized to obtain access).

44. *Id.*

45. For further discussion of the importance of use restrictions reinforced by technological controls, see Jane Bambauer, *Other People's Papers*, 94 TEX. L. REV. 205 (2015) (discussing the importance of use restrictions reinforced by technological controls).

46. *See* Litt, *supra* note 42, at 18.

47. For further discussion of the importance of using the best feasible technology, see *Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4, at 10 (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board).

48. PCLOB § 702 REPORT 2014, *supra* note 16, at 7 ("There are two types of Section 702 acquisition: what has been referred to as 'PRISM' collection and 'upstream' collection.").

49. *Id.* at 36–38.

50. *See* Margulies, *Dynamic Surveillance*, *supra* note 29.

Internet divides and combines individual communications into packets.[51] Devices such as routers that manage packet transmission will take the most efficient path available.[52] Sometimes the most efficient path for a particular packet of domestic communications lies through equipment typically used by foreign nationals located abroad.[53] An NSA device monitoring hubs used by foreign nationals overseas will then pick up this domestic communication.[54] An ISP may also change protocols in a fashion that makes it more likely that some of the user's communications will run through such equipment.[55]

In upstream collection, the interaction of internet architecture and limited technology yields an additional risk that the NSA will collect purely domestic communications.[56] Because upstream collection occurs at the Internet backbone, the NSA obtains data in the form of communications "transactions."[57] A transaction is any set of data traversing the Internet that a device aggregates or divides to facilitate transmission. Internet transactions are two-fold.[58] The first is a single communication.[59] The second, called a multiple communications transaction (MCT), contains many individual communications.[60] For example, at the internet backbone hubs where the NSA, in partnership with ISPs, scans for upstream collection, emails are often "bundled together within a single Internet transmission."[61]

As of April, 2016, public reports confirm that the NSA has been unable to design and implement a filter that reliably and uniformly collects only those specific emails in an MCT that are responsive to specific search requests.[62] To collect the email that meets its search criteria, the NSA must sometimes collect entire MCTs, analogous to pages of personal emails.[63] As with anyone's email account, an entire page will include numerous messages on varying subjects from a spectrum of senders.[64]

---

51. PCLOB § 702 REPORT 2014, *supra* note 16, at 38; *In re* Government's ex parte Submission of Reauthorization Certification for 702 Program, 2011 U.S. Dist. Lexis 157706, at 39–41 (FISA Ct. Oct. 3, 2011) (Bates, J.).

52. *See* DONOHUE, *supra* note 1, at 56.

53. *Id.* at 56–57.

54. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 38.

55. *Id.* at 40.

56. *Id.* at 40–41.

57. *Id.* at 39.

58. *Id.* at 41.

59. *Id.*

60. PCLOB § 702 REPORT 2014, *supra* note 16, at 41.

61. *See* PRESIDENT'S REVIEW GROUP, *supra* note 30, at 141 n.137–38.

62. *See* Inglis & Kosseff, *supra* note 1, at 12.

63. *Id.*

64. *Id.*

Some MCTs include messages sent between persons located in the U.S. – i.e., purely domestic communications.[65]

While today's technological limits oblige the NSA to collect MCTs, those limits might ease tomorrow.[66] For example, the NSA or private firms might develop a scanning methodology that can reliably identify, isolate, and extract individual selector-based emails within a larger packet, thus obviating the MCT issue.[67] Congress and the FISC are not well-situated to determine what that technology is, and when it will arrive. However, Congress *can* mandate that the NSA regularly assess and update its methods to ensure that it uses the best feasible technology to collect data upstream.[68] Moreover, Congress can mandate that the government include a representation to this effect in its certification for the FISC pursuant to § 702, and that the FISC review the government's representation.[69] Congress can also require the Inspector General for the NSA to report to Congress on progress in this area.[70]

This "best feasible technology" approach is flexible enough to give the NSA the room it needs to innovate.[71] The best feasible technology standard will not lock the NSA into a particular method that is not practicable or scalable, or may be obsolete the day after tomorrow.[72] By the same token, the standard will oblige the NSA to devote part of its technological prowess to technology that protects privacy.[73] Given the intrusions on privacy that are necessary in the NSA's work,[74] that seems like a fair bargain.

Congress should also expressly require the NSA to use the best feasible technology to evaluate its searches. Right now, anecdotal evidence suggests that the

65. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 41.

66. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, RECOMMENDATIONS ASSESSMENT REPORT, 21 (2016), https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf (discussing Recommendation No. 6).

67. *Id.*

68. *See Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4, at 10–11 (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board) (recommending that Congress mandate that the NSA update its technology and report to Congress regularly on its progress).

69. *See id.* at 10–11 (recommending that the government be required to evaluate the effectiveness of existing technology and investigate improvements).

70. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 75.

71. *See id.* at 144 (suggesting that there should be an ongoing dialogue between the government, telecommunications providers, and independent experts to ensure that the best technology is being used, and that the determination should be continually revisited).

72. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 143–45.

73. *Id.*

74. *See* Jonathan Mayer et al., *Evaluating the Privacy Properties of Telephone Metadata* 5536 (Cynthia Dwok ed., PROCEEDINGS NAT'L ACAD. SCI. vol. 113 no. 20, 2016) (utilizing digital research and probabilistic analysis to show that collection of metadata such as call records can impose serious privacy consequences).

NSA lacks a uniform approach for evaluating the accuracy of its searches.[75] In any case, its governing statutes do not mandate development or implementation of such a methodology.[76] Although the NSA's self-evaluation protocols are not publicly available, it seems reasonable to assume that, overall, the agency follows what I'll call an individual expert judgment approach: in other words, it hires experts in cryptology, computers, and the Internet, and creates an environment in which these experts can develop their expertise in the service of the NSA's multiple missions.[77] That individual expert judgment approach presumably figures in NSA's work under § 702.[78] There is one major problem with the unadulterated reliance on expert judgment: expert judgment is not always what it is cracked up to be.[79] Sometimes, it is neither particularly expert nor the exercise of judgment.[80] Left to its own devices, expert judgment can run aground because of biases and other flaws in human inference.[81] Studies of doctors, for example, show that medical decisions

75. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 86.

76. *See NSA Reports to the President's Oversight Intelligence Board (IOB)*, NSA (May 3, 2016), https://www.nsa.gov/news-features/declassified-documents/intelligence-oversight-board/index.shtml (suggesting that rules may vary but they contain the same hallmarks).

77. DeLong, *supra* note 42, at 85–86 (suggesting that technology may be the best way to support oversight and compliance).

78. It seems logical to assume that the NSA periodically reviews its work for evaluation purposes. Many of those evaluations are useful for showing when the NSA is on the right track and when it must make additional improvements. *See id.* (discussing the importance of workplace culture of inquiry and commitment to evolving best practices). However, public reports do not indicate that the NSA has developed a systematic approach to *evaluating its evaluative methodology*, to ensure that it consistently and comprehensively uses the most advanced approaches that are feasible. *Cf.* PCLOB § 702 REPORT 2014, *supra* note 16. Congress should require this and periodic reports on progress toward that goal. If, for security reasons, any of this information must be presented in a closed session or hearing, Congress has authority to conduct proceedings in that fashion.

79. *See* Geir Kirkebøen, *Decision Behaviour – Improving Expert Judgement*, *in* MAKING ESSENTIAL CHOICES WITH SCANT INFORMATION: FRONT-END DECISION MAKING IN MAJOR PROJECTS 169, 179–90 (Terry Williams, Knut Samset & Kjell Sunnevåg eds., Palgrave-Macmillan 2009) (discussing how professional judgment is inferior to simple statistical models and subject to emotional and motivational biases). *See generally* Stephen C. Hora, *Expert Judgment in Risk Analysis*, Create Homeland Security Center 1, 1–11 (2009), http://create.usc.edu/sites/default/files/publications/expertjudgmentinriskanalysis_0.pdf (discussing what constitutes expert judgement).

80. *See* Hora, *supra* note 79. *See also* Colin F. Camerer & Eric J. Johnson, *The Process-Performance Paradox in Expert Judgment: Why do Experts Know so Much and Predict so Badly?*, *in* TOWARD A GENERAL THEORY OF EXPERTISE: PROSPECTS AND LIMITS 195, 202–11 (K. Anders Ericsson & Jacqui Smith eds., Cambridge Univ. Press 1991) (arguing that while experts are good at generating hypotheses and complex decision rules, those attributes have little impact on their performance).

81. *See* Eric S. Janus & Robert A. Prentky, *Forensic Use of Actuarial Risk Assessment with Sex Offenders: Accuracy, Admissibility, and Accountability*, 40 AM. CRIM. L. REV. 1443, 1444 (2003) ("Our thesis is straightforward: actuarial methods have proven equal or superior to clinical judgments."); Michelle M. Mello & David M. Studdert, *Deconstructing Negligence: The Role of Individual and System Factors in Causing Medical Injuries*, 96 GEO. L.J. 599, 605 (2008) (finding that doctors' judgement errors were the most prevalent cause of injury claims); Christopher Slobogin, *Risk Assessment and Risk Management in Juvenile Justice*, A.B.A. CRIM.

determined by an expert's judgment are often wrong, failing to take into account patients' medical histories and responses to medications.[82] All experts, including those specializing in surveillance algorithms, are subject to these errors.[83]

Wrong calls at the NSA can have serious consequences. Those wrong calls can result in two types of errors: false positives, in which the agency conducts surveillance on people who have no relation to terrorism or any other national security threat, and false negatives, in which the agency *fails* to detect threats.[84] Some of the NSA's searches may create excessive numbers in at least one of these categories.[85] However, these errors are not inevitable.[86] Technology and methodical human review can identify these errors, diagnose their cause, and point the way toward better practices in the future.[87] Congress should mandate the best feasible technology to accomplish that result.

JUST. MAG., Winter 2013, at 10, 12–13 (observing that actuarial techniques for predicting recidivism among offenders that rely on a common list of factors are more accurate than unstructured clinical assessments).

82. For a sobering discussion of the incidence and range of medication administration errors by trained nurses, see Steven D. Williams, et al., *Causes of Medication Administration Errors in Hospitals: A Systematic Review of Quantitative and Qualitative Evidence*, DRUG SAFETY: INT'L J. MED. TOXICOLOGY & DRUG EXPERIENCE, 1045, 1063–64 (2013).

83. Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 810–15 (2015) (arguing for application of *Daubert* test on scientific evidence for validation of computer search techniques).

84. False positives have drawn particular attention in the context of no-fly lists. *See* Latif v. Holder, 28 F. Supp. 3d 1134, 1153–54 (D. Or. 2014) (holding that the low evidentiary standard for placement on the No-Fly list combined with a lack of meaningful opportunity to be removed from the No-Fly list risks deprivation of constitutionally protected liberty interests); *see also* Ibrahim v. Dep't of Homeland Sec., 62 F. Supp. 3d 909, 928–29 (N.D. Cal. 2014) (holding that the government's conceded error in placing plaintiff on a No-Fly list violated plaintiff's constitutional rights); Irina D. Manta & Cassandra Burke Robertson, *Secret Jurisdiction*, 65 EMORY L.J. 1313, 1318–19, 1346–47, 1351–53 (2016) (finding that the federal government's process of putting someone on the No-Fly list is unconstitutional and does not improve airline security); *cf.* Abdelfattah v. United States Dep't of Homeland Sec., 787 F.3d 524, 529–31, 534 (D.C. Cir. 2015) (describing plaintiff's frustration over repeated security checks possibly triggered by information in government databases and holding that plaintiff could seek a remedy under both Privacy Act and U.S. Constitution, but denying relief on grounds that the plaintiff had not established facts to support relief sought).

85. *See* Peter Margulies, *Surveillance by Algorithm: The NSA, Computerized Intelligence Collection, and Human Rights*, 68 FLA. L. REV. (forthcoming 2016), http://ssrn.com/abstract=2657619.

86. *Id.*

87. *See* DeLong, *supra* note 42, at 88 (noting that "[t]he best way to achieve the benefits of technology in a compliance program, while minimizing as many of the risks as possible, is to have frequent, meaningful, and documented interactions among people, across all functional areas in an organization."). Medical data analysts have made substantial progress in this area. *Cf.* Ruben Amarasingham et al., *An Automated Model to Identify Heart Failure Patients at Risk for a 30-Day Readmission or Death Using Electronic Record Data*, 48 MED. CARE 981–82, 986–87 (2010) (describing and evaluating a model that performed well in identifying heart patients who, upon discharge from the hospital, were at great risk of imminent death or readmission; the model facilitated the provision of services that would reduce these risks).

An additional technological problem under § 702 is the uncertainty of using Internet Protocol addresses as proof of the location of a target of surveillance. Under § 702, the NSA can only target communications where one party to the communication is a non-U.S. person "reasonably believed to be located outside the United States."[88] However, IP addresses can be inaccurate. An IP address that appears to be in Germany, Pakistan, or Hong Kong may actually belong to a user in the United States, or may appear as a foreign "hit" in an NSA search because a domestic user has accessed common, innocuous websites based abroad or domestic sites containing links to overseas sites.[89] Without additional information, NSA collection may yield many false positives – people whose communications are targeted even though these individuals are actually located in the United States where the FAA precludes targeting by agencies such as the NSA.[90] The PCLOB has stated that the NSA already deals with the false positive problem by using due diligence to ascertain a target's U.S. person status and current location.[91] That exercise of due diligence can entail checking "multiple sources."[92] In reauthorizing § 702, Congress should write the due diligence standard into the law.

In expressly requiring due diligence to ferret out false positives, Congress should also address the problem of false negatives, particularly those concerning VPNs.[93] An individual can use a VPN to mask or "spoof" her IP address.[94] While the address might otherwise be readily recognized as being located outside the U.S., using a VPN allows such individuals to communicate with an apparent IP address that matches the VPN server's location.[95] As a result, an individual in Pakistan using a VPN could communicate using an apparent IP address from the United States. An Al Qaeda or ISIS member could use such a method to avoid surveillance under § 702. Congress should expressly permit the NSA to use multiple sources to ascertain that a putative U.S. IP address is actually being used by a U.S. person or an individual located here. The reauthorized statute should include a narrow provision that permits the NSA to acquire information on U.S. IP addresses that

88. 50 U.S.C. § 1881a(a) (2012) (amended 2015).

89. *See* Letter from Jonathan Mayer, Stanford Univ. Sec. Lab., to Review Grp. on Intelligence and Commc'ns Techs., Office of the U.S. Dir. of Nat'l Intelligence 2 (Oct. 3, 2013) (noting the frequency of "[i]nstances where an American reasonably expects to interact with a domestic website – and is, in fact, interacting with a domestic website – where his or her browsing activity may nevertheless flow across international boundaries."). The domestic site may be as harmless and generic as a site run by the U.S. government itself, which features web apps sourced from abroad. *Id.* at 2–4.

90. 50 U.S.C. § 1881a(b) (2012) (amended 2015).

91. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 43–44; Kris, *supra* note 1, at 22–24 (discussing how the NSA analyst must look at the totality of the circumstances when making a determination if the target is in the United States).

92. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 43–44; Kris, *supra* note 1, at 23–24.

93. *See* Kris, *supra* note 1, at 22 (discussing how VPNs operate in the context of location-spoofing).

94. *Id.*

95. *Id.*

appear to be linked to tasked selectors. The NSA should be allowed to engage in this acquisition for the purpose of detecting spoofed U.S. VPNs, subject to appropriate minimization procedures.[96]

III. THE FISC AND OTHER SAFEGUARDS: QUERYING U.S. PERSON DATA, ESTABLISHING A PUBLIC ADVOCATE, AND CREATING A "COLLECTION AVOIDANCE" EXCEPTION TO MINIMIZATION REQUIREMENTS

One central issue in § 702 reauthorization is whether Congress should require that officials obtain a court order before querying incidentally collected U.S. person § 702 data. While some argue that any query for U.S. person information should require a specific court order specifying the subject of the query,[97] this approach paints with too broad a brush. Instead, the requirement of a court order should hinge – as it does under current NSA practice – on whether the NSA has collected the data upstream or downstream.[98] This section elaborates on this point. It also urges that Congress establish a more robust public advocate for FISC proceedings. The section then briefly addresses minimization requirements, arguing for an express exception for data that aids the NSA in *avoiding* collection on targets who have traveled to the United States.[99]

---

96. *See also infra* notes 126–32 and accompanying text (discussing the implied exception to U.S. person or locational collection for assessing when an overseas subject has traveled to the U.S., thereby requiring cessation of collection, and suggesting that Congress make this implied exception express).

97. DONOHUE, *supra* note 1, at 143; *Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4 (comments by Sen. Leahy and testimony of Elizabeth Goitein of the Brennan Center for Justice).

98. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 56–57 (discussing the limitations on NSA analysts when using a U.S. person identifier in both upstream and downstream collections).

99. This Article does not take a position on whether Congress should amend the *substantive* provisions of the FAA, such as the subsection that defines the foreign intelligence information that the government can target for collection as including data "with respect to a foreign power or foreign territory" relating to the "the conduct of the foreign affairs of the United States." 50 U.S.C. § 1801(e)(2)(B) (2012). Some insightful commentators have argued that this provision appears overbroad, particularly to Europeans and tribunals such as the Court of Justice of the European Union (CJEU). *See* Timothy Edgar, *Focusing PRISM: An Answer to European Privacy Concerns?*, LAWFARE (Oct. 10, 2015, 5:20 PM), https://lawfareblog.com/focusing-prism-answer-european-privacy-concerns; *cf.* Faiza Patel, *Safe Harbor and Reforming Section 702*, JUST SECURITY (Oct. 22, 2015, 11:25 AM), https://www.justsecurity.org/27009/safe-harbor-reforming-section-702/ (discussing concerns of both CJEU and U.S. privacy advocates). I agree that the U.S. needs to do more to convey to European stakeholders that activity authorized by this provision does not result in the indiscriminate collection, storage, or retention of the personal data of private citizens in Europe or elsewhere. *See* Peter Margulies, *Transatlantic Setback or Invitation to Dialogue?: EU Data Regulators' Verdict on Privacy Shield*, LAWFARE (Apr. 15, 2016, 9:52 AM), https://www.lawfareblog.com/transatlantic-setback-or-invitation-dialogue-eu-data-regulators-verdict-privacy-shield. Perhaps Congress can add a preamble to the FAA to this effect. The language of any such preamble should avoid undue specificity about the collection authorized by the "foreign affairs" provision, such as collection on any foreign government officials who may collude with foreign entities to violate international trade agreements or other norms. Undue specificity could be counterproductive, complicating U.S. diplomatic efforts and leaving the U.S. with fewer options in the complex arena of foreign

A. Distinguishing Queries: Upstream v. Downstream

In considering whether to require a court order for querying incidentally collected U.S. person data, Congress should distinguish between upstream and downstream collection. Analyzing collection through this prism will produce tailored limits that do not compromise an analyst's ability to connect the dots. In contrast, ignoring the differences between these two modes of collection could lead to dangerous gaps in the data on future threats.

Importantly, the NSA, the Justice Department, and the FISC already understand this distinction. The NSA has barred analysts from querying the upstream collection dataset with U.S. person identifiers.[100] Moreover, according to Judge Hogan of the FISC, the FBI does not receive any unminimized information obtained through upstream collection.[101] According to Judge Hogan, this limitation is crucial since upstream collection involves acquisition of MCTs. It therefore collects a significant volume of information unrelated to tasked selectors.[102] As a result, the upstream program is "more likely" than other programs to include U.S. person communications with no foreign intelligence value.[103] Congress should expressly bar both FBI receipt of unminimized upstream data and any U.S. person queries by the NSA on communications incidentally collected under the upstream program, or any other program that scans communications as they pass through international Internet hubs.

Downstream collection presents a different calculus. In downstream collection, an ISP aggregates the content of communications involving a U.S. citizen or lawful resident (or another individual located in the U.S.) and a tasked selector linked to an individual reasonably believed to be located outside the United States.[104] Because of these parameters, downstream collection is far more tailored than upstream collection.[105] Downstream collection does not entail obtaining MCTs, which can include purely U.S. person content unrelated to a selector.[106] Moreover, this information may have foreign intelligence value that requiring a court order would vitiate. Suppose the government wished to know if a known ISIS operative in Syria or Iraq had emailed, telephoned, or described U.S. persons who have traveled overseas to fight on ISIS's behalf or might wish to do so. Further suppose that the

---

relations. *See* Peter Margulies, *Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy*, 72 WASH. & LEE L. REV. 1283, 1285–86 (2015) [hereinafter Margulies, *Defining "Foreign Affairs"*].

100. PCLOB § 702 REPORT 2014, *supra* note 16, at 56.

101. [Name Redacted by Court], at 43 (FISA Ct. Nov. 6, 2015).

102. *Id.* at 43–44.

103. *Id.* at 44.

104. *Id.* at 33–34.

105. *Id.*

106. *Id.*

NSA or the FBI had a list of persons in the U.S. whom it suspected were forming such plans, but lacked sufficient evidence to obtain a warrant. The plans of a terrorist recruit can change quickly, and a U.S. person planning to go abroad would probably not give the NSA or the FBI an engraved invitation to the airport gate. Even if the NSA or the FBI received some fresh information suggesting travel abroad was imminent, drafting a request for a warrant and waiting for a judge's approval might consume too much time to stop the ISIS recruit.[107] In this context, requiring a court order prior to a U.S. person query would clash with U.S. national security and foreign relations.[108]

The statute should continue to give law enforcement the flexibility to design queries that yield useful information, whether or not those queries expressly focus on foreign intelligence information. Judge Hogan of the FISC observed in his November, 2015 opinion that the posing of "queries designed to elicit evidence of ordinary crimes is not entirely unconnected to foreign intelligence."[109] Those links are more likely since § 702 collection targets are persons reasonably believed to "possess, receive, or communicate" foreign intelligence information.[110] Given that limited sample population of targets, contacts of the targets may also have such links. As Judge Hogan hinted, it is far more likely within the tailored downstream data set that a criminal scheme, involving identity theft, selling of contraband, money laundering, or kidnapping, would be linked to international terrorism or another foreign source.[111] Judge Hogan was correct to assert that such links might be rare, but would nevertheless be of "substantial" intelligence value when law enforcement officials discovered them.[112]

Proposals to provide an exception from the court order requirement under exigent circumstances[113] do not grant the government sufficient flexibility. Indeed, an exigent circumstances test would place the government in a Catch-22 dilemma. In the needles-in-haystacks world of foreign intelligence, meeting an exigent circumstances test requires access to data.[114] Without data, the government is engaging in speculation, not addressing exigent circumstances. However, without

107. *Cf. In re* Directives Pursuant to Section 105B of FISA, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008) (noting that there is a "high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information.").

108. *See id.* (observing that requiring a warrant would "impede the vital national security interests ... at stake.").

109. *See* [Name Redacted by Court], at 42 (FISA Ct. Nov. 6, 2015).

110. *Id.*

111. *Id.*

112. *Id.*

113. *See Senate Judiciary Committee May 2016 § 702 Hearing, supra* note 4, at 8 (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board).

114. *Cf.* NAT'L RESEARCH COUNCIL OF THE NAT'L ACAD., PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS, 77 (2008) (noting risks and potential benefits of counterterrorism data analysis).

the ability to query incidentally collected U.S. person downstream data, the government may not obtain the data it needs to *discover* exigent circumstances. For example, without the ability to craft specific queries involving U.S. person contacts of individuals abroad, officials might not learn in a timely fashion that a suspected ISIS recruit's travel abroad was imminent. Without that information, officials would be unable to show exigent circumstances. Placing the government in this bind sacrifices national security and foreign relations goals for marginal increases in privacy.

B. Preserving the FBI's Flexibility

For similar reasons, Congress should not limit the occasions that permit FBI querying of the downstream § 702 database. Some surveillance critics have argued that the FBI should be able to query downstream § 702 data only when the query figures in a current investigation.[115] The FBI's current practice, which permits queries in a range of circumstances, gives the FBI the agility it needs.[116] Suppose that monitoring of a known terrorist chat-room provides a lead that the FBI wishes to check out by querying § 702 data. Encouraging that initiative will allow the FBI to most efficiently "connect the dots." Restricting the ability to query § 702 data to a particular phase of an investigation stifles the FBI agents' initiative and risks leads falling through the cracks. That cabined mindset was disastrous in the run-up to 9/11.[117] Reintroducing that rigid perspective would put a crimp in the FBI's ability to adapt to an ever-changing threat environment.

C. Build in a Robust Public Advocate

Rather than stifle the FBI agents' initiative, Congress should institutionalize the role of a public advocate at the FISC. A heartening element of the Hogan opinion is its thoughtful response to the vigorous advocacy of amicus curiae Amy Jeffress.[118] As a number of commentators have noted, the addition of a public voice can only improve decision-making.[119] Indeed, despite modest cavils, the 2015 FISC opinion

115. *Cf.* Robert Loeb & Helen Klein Murillo, *A Comprehensive Look at the FISC Order Legal Analysis*, LAWFARE (Apr. 28, 2016), https://www.lawfareblog.com/comprehensive-look-fisc-order-legal-analysis (criticizing the November, 2015 FISC opinion and urging greater limits on FBI queries of § 702 data); Marcy Wheeler, *Former Top Holder Aide Says Back Door Searches Violate Fourth Amendment; FISC Judge Thomas Hogan Doesn't Care*, EMPTYWHEEL (Apr. 22, 2016), https://www.emptywheel.net/2016/04/22/former-top-holder-aide-says-back-door-searches-violate-fourth-amendment-fisc-judge-thomas-hogan-doesnt-care/.

116. *See* [Name Redacted by Court], at 29 n.27 (FISA Ct. Nov. 6, 2015).

117. *See* Nathan Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEX. L. REV. 1795, 1795–96 (2010).

118. *See* [Name Redacted by Court], at 5–6 (FISA Ct. Nov. 6, 2015).

119. *See* Wheeler, *supra* note 115 (praising Jeffress's work as an amicus curiae); *see also* Margulies, *Dynamic Surveillance*, *supra* note 29, at 51–55 (noting the benefits of a public advocate in FISC decisions); Vladeck, *supra* note 19, at 1176–77 (emphasizing that "adversarial participation" in the FISC process would alleviate any

has the qualities of deliberation one would expect of a decision by an Article III court: the opinion considers alternative arguments and reasons carefully to a conclusion – attributes that Alexander Hamilton extolled in Federalist No. 78,[120] an essay long considered the fount of wisdom on the virtues of judicial review.

Congress, in reauthorizing § 702, should enhance the public voice by moving beyond the discretionary authority to appoint amici curiae established in the USA Freedom Act to a more thoroughly institutionalized public advocate.[121] That advocate would be authorized to view a representative sample of § 702 selectors and queries, including U.S. person queries.[122] The public advocate would also be empowered to petition the FISC if those queries or selectors appeared overbroad.[123]

One possible objection is that a public advocate with such expansive responsibilities would also present greater security challenges. However, this concern is less serious than it appears. A public advocate would have to be chosen from the ranks of lawyers with wide experience in the executive branch. Such lawyers would have a strong reputational interest in maintaining their credibility with the intelligence community, Congress, and the courts.[124] A lawyer with this interest would be exceptionally diligent in maintaining secrets, protecting sources of methods, and safeguarding other information vital to national security.[125]

D. Collection Avoidance and Minimization

While minimization of data entails healthy limits on officials' access to irrelevant information, current NSA practice acknowledges that in certain situations an exception to minimization can enhance privacy. The FISC has recognized an implicit exception to minimization rules when information is useful in collection avoidance, i.e., in stopping collection in a timely manner when an overseas target's travel to the U.S. renders continued surveillance illegal.[126] Congress should codify this exception.

Article III problems); Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* JUSTSECURITY (Nov. 4, 2013, 1:34pm), https://www.justsecurity.org/2873/fisa-special-advocate-constitution/ (indicating that there is no harm in having an extra lawyer participate in the decision-making process).

120. THE FEDERALIST No. 78, at 489–94 (Alexander Hamilton) (Benjamin F. Wright ed., 1961).

121. Emily Berman, *The Two Faces of the Foreign Surveillance Court*, 91 IND. L.J. 1191, 1241 (2016) (emphasizing the importance of the adversarial process in FISA Court proceedings).

122. *Id.*

123. *Id.*

124. *Cf.* Ronald J. Gilson & Robert H. Mnookin, *Disputing Through Agents: Cooperation and Conflict Between Lawyers in Litigation*, 94 COLUM. L. REV. 509, 509–13 (1994) (noting that lawyers, as "repeat-players" in litigation, often choose strategies that protect their reputations with other stakeholders in the process).

125. Both Congress and the FISC obviously took this view of the role of the amici curiae. Congress would not have provided for a panel of amici, and the FISC would not consider appointing them, if security were a concern.

126. *See* [Name Redacted by Court], at 66–68 (FISA Ct. Nov. 6, 2015).

Minimization is a requirement pursuant to the statute to ensure that agencies do not retain personal data for a longer period than necessary.[127] Under the statutory framework governing § 702 foreign intelligence collection, this is a major concern regarding U.S. person information.[128] Agencies must typically purge this information within a specific period of time (five years or less) unless it is relevant to a foreign intelligence purpose or is evidence of a crime.[129]

However, the NSA informed the FISC in 2015 that for a number of years it had retained information longer for collection avoidance reasons.[130] Consider information collected when a surveillance target abroad entered the U.S. (in NSA parlance, became a "roamer") and then used personal information linked to a U.S. person during that U.S. visit. A "roamer" (who could be a terrorist, arms trafficker, diplomat, etc.) could use an email address that the NSA had tasked as a "selector" for collection purposes, but send those emails from an IP address associated with a U.S. person with whom the target was staying during the target's visit to this country. The NSA loads such data into a technological tool it uses to evaluate "alerts" it receives when a target may have entered the U.S.[131] This use may be outside of any express statutory exception, but the NSA has described it as an *implicit exception*, since the information is retained not for collection or querying, but instead only for the limited purpose of determining when collection should *cease*.[132] Judge Hogan of the FISC ultimately found that such an implicit exception was appropriate.[133]

Congress should make this implicit exception express. Eliminating the exception would hinder the NSA in determining when a target had entered the United States. It would therefore force the agency to be even more intrusive, not less. To resolve the problem, Congress should include language that expressly authorizes the NSA to retain data used strictly for collection avoidance.

127. *See* 50 U.S.C. § 1801(h)(1) (2012) (amended 2015) (requiring that agencies adopt "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information"); *cf.* PCLOB § 702 REPORT 2014, *supra* note 16, at 50–51 (explaining minimization under the statute).

128. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 50–51.

129. *Id.* at 60.

130. *See* [Name Redacted by Court] at 66–68 (FISC Ct. Nov. 6 2015) (noting that the NSA did not comply with requirements to age off communications collected in conjunction with the FBI within a fivc year period).

131. *Id.* at 67–68 (explaining the process used to resolve alerts).

132. *See id.* (noting that the Government has modified procedures to justify when communication collection is kept for longer than five years).

133. *Id.* at 70–71. The FISC concluded that the NSA Minimization Procedures do not prohibit the NSA from keeping data for longer periods of time in an effort to ensure homeland safety. *Id.*

IV. TRANSPARENCY

Transparency is another vital factor in § 702 reauthorization. The Office of the Director of National Intelligence (ODNI) has provided unprecedented transparency in the wake of Edward Snowden's revelations.[134] Moreover, the USA Freedom Act has introduced further openness.[135] However, more needs to be done.

A. Transparency's Virtues and Risks

Transparency has several virtues in democratic governance. First, it allows Congress, the FISC, and the public to accurately assess the size, scope, and nature of intelligence collection involving U.S. person data.[136] Transparency also allows these stakeholders to understand how the branches of government work together to review and oversee intelligence collection.[137] With the benefit of transparency, stakeholders can see if the FISC has been unduly deferential to the government or if it has made intelligence collection needlessly cumbersome.

Second, transparency has a useful *ex ante* effect. The prospect of public exposure helps concentrate the bureaucratic mind, ensuring that officials only advance and implement programs that they can defend.[138] In a system that lacks express transparency requirements, officials may overreach, with groupthink encouraging the illusion that unduly expansive interpretations of legal authorities will never be subject to public scrutiny.[139] That heedless mindset is a collective illusion, since leaks from disgruntled personnel like Snowden will eventually result in public disclosure.[140] An up-front transparency requirement rids officials of that illusion of opacity, forcing them to formulate and implement programs with an eye toward the

134. For an insightful analysis of transparency's risks and benefits, see Brand, *Transparency*, *supra* note 7; *see also* Carrie Cordero, *The DNI's New Transparency Implementation Plan*, LAWFARE (Oct. 27, 2015, 2:00 PM), https://www.lawfareblog.com/dnis-new-transparency-implementation-plan (describing transparency principles announced by Director of National Intelligence James Clapper).

135. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 292 (2015).

136. *See* DONOHUE, *supra* note 1, at 149 (discussing the vital function that transparency plays in a democratic state).

137. *Id.*

138. *See* Jack Goldsmith, *A Partial Defense of the Front-Page Rule*, HOOVER INST.: THE BRIEFING (Jan. 29, 2014), http://www.hoover.org/research/partial-defense-front-page-rule (noting that disclosures have forced the intelligence community to justify itself and address tradeoffs that it could ignore when its activities remained secret).

139. *See* Robert M. Chesney, *National Security Fact Deference*, 95 VA. L. REV. 1361, 1415–16 (2009) (discussing causes and effects of groupthink); Jon D. Michaels, *The (Willingly) Fettered Executive: Presidential Spinoffs in National Security Domains and Beyond*, 97 VA. L. REV. 801, 871–73 (2011) (analyzing the impact of groupthink on the functionality of executive agencies).

140. *See* Goldsmith, *supra* note 138.

best public justifications they can present. In a democracy, that early focus on public justifications is generally the best default position for government.[141]

Transparency also buttresses the legitimacy of government programs. Perceptions of legitimacy rise if the current rules work and government is actually following those rules.[142] Transparency can rebut surveillance critics who claim that overreaching is the norm.

However, decreeing transparency as a universal default position can also trigger a negative effect on decision-making. Lawmakers and the public intuitively understand that in areas such as attorney-client privilege, the law requires confidentiality to avoid chilling communication.[143] The same concerns affect the formation and implementation of public policy. The Framers recognized that sometimes a fishbowl is not the ideal venue for complex decisions involving national security and foreign affairs.[144] In some contexts, disclosure of policies will limit policymakers' options and undermine a decision's implementation.[145] For example, the Obama administration decided to make overtures to Iran that ultimately resulted in the U.S.-Iran nuclear accord.[146] Early disclosure of those overtures might have scuttled negotiations with Iran, locking the administration into a hostile stance. In the domain of surveillance, undue transparency can tip off adversaries and encourage them to modify their tactics to evade detection.[147]

B. Current Examples of Transparency

U.S. intelligence has made extraordinary strides toward greater transparency after Snowden's disclosures. Brief discussion of those innovations provides concrete evidence of transparency's virtues and also helps identify areas for further reforms.

---

141. *See* DONOHUE, *supra* note 1, at 149–50 (noting that the public discussion of the necessity for transparency in surveillance gathering has surfaced since the Snowden leaks).

142. *Id.*

143. *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) (attorney-client privilege "encourages full and frank communication between attorneys and their clients and thereby promotes broad public interests in the observe of law and the administration of justice").

144. *See* Margulies, *Defining "Foreign Affairs," supra* note 99, at 1284, 1295 (noting that while the Framers believed in the value of transparency, they understood the utility of secrecy at times).

145. *See id.* at 1295–96 (noting that the Framers recognized that premature disclosure could adversely affect certain policy options' effectiveness).

146. *Cf.* Asli U. Bali, *Negotiating Nonproliferation: International Law and Delegation in the Iranian Nuclear Crisis*, 61 UCLA L. REV. 232, 269 (2014) (discussing that overtures of Obama resulted from the first high-level bilateral meeting between America and Iran in thirty years).

147. *Cf.* Margulies, *Dynamic Surveillance, supra* note 29, at 28 (noting that detailed government disclosure can impair surveillance and limit the choices available to decision makers).

After Snowden's leaks, the ODNI began to release important FISC opinions.[148] The USA Freedom Act mandated continuation of this process.[149] The result has been two-fold. First, disclosure of FISC opinions has made clear that the court's judges wrestle with the difficult problems of intelligence collection. For example, Judge Reggie Walton expressed deep concern for wayward NSA practices that led to the use of identifiers under § 215 of the USA Patriot Act [now USAF] for which the agency lacked reasonable and articulable suspicion (RAS) of links to terrorism.[150] Judge Walton ordered the Justice Department for a period of almost one year to submit all proposed identifiers to the FISC for advance approval.[151] The court permitted continuation of the program only when the Justice Department had conclusively demonstrated that it had overhauled its collection protocols to eliminate the problem of non-RAS-approved identifiers.[152]

In the realm of ongoing NSA collection, Congress has already sought transparency in the USA Freedom Act, particularly the Act's requirement that the NSA disclose the number of U.S. persons, specifically U.S. citizens or lawful permanent residents (LPRs) who have been subject to queries of data incidentally collected under § 702.[153] On an annual basis, the NSA must publish a "transparency report" that discloses this and similar information about the impact of § 702 surveillance on U.S. persons.[154]

This report is useful. For example, the 2015 report revealed that the NSA obtained under 5,000 court orders for querying the § 702 dataset regarding the content of U.S. persons' communications.[155] Armed with that number, Congress, the FISC, and the public – including privacy and civil liberties advocates – can assess how the NSA uses incidental collection. Moreover, these stakeholders can see trends in the numbers. If the NSA is collecting markedly more content in a given year, compared to the previous year, stakeholders can ask why. Perhaps there are more terrorists among U.S. persons (including youths recruited to join ISIS in Syria and Iraq). Or perhaps the NSA is becoming too eager to conduct surveillance and

148. For a recent sampling, see Cody M. Poplin, *ODNI Releases Three FISC Opinions*, LAWFARE (Apr. 20, 2016, 1:25 PM), https://www.lawfareblog.com/odni-releases-three-fisc-opinions.

149. USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 292 (2015).

150. *See In re* Production of Tangible Things, BR 08-13, at 4–5 (FISC Ct. Mar. 2, 2009).

151. *Id.*

152. *Id.*; *see also* John DeLong & Susan Hennessey, *Understanding Footnote 14: NSA Lawyering, Oversight, and Compliance*, LAWFARE (Oct. 7, 2016), https://www.lawfareblog.com/understanding-footnote-14-nsa-lawyering-oversight-and-compliance (discussing this episode).

153. USA FREEDOM Act of 2015, 129 Stat. at 292–93 (providing mandatory reporting requirements regarding United States persons).

154. *Id.*

155. *See generally* Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, IC ON THE RECORD (May 2, 2016), https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

collection. The answer may be the first alternative, the second, or a mix of the two. Obliging the NSA to report this information allows stakeholders to ask the crucial questions. It also obliges the NSA to monitor *its own* practices in the anticipation of such stakeholder inquiries. That complementarity between transparency and internal constraints is a vital asset that Congress should enhance in the FAA's reauthorization.

For example, the NSA has agreed with the PCLOB's recommendation that the NSA provide the FISC with a sample of queries and selectors used by the agency.[156] That is a helpful development, as Judge Hogan indicated in his November, 2015 opinion.[157] Congress should provide expressly that the NSA will furnish such samples periodically to the FISC. However, more is needed.

C. The FISC and Transparency

Congress should do more to mandate that Congress and the public know more about the procedures followed by the FISC. Independent reviews have indicated that the FISC is not a rubber stamp.[158] Nonetheless, this Article has argued that an institutionalized public advocate would refine the FISC's deliberations. With or without a full-time public advocate, however, more transparency about the FISC's proceedings would benefit both Congress and the public.

Congress should do more to facilitate public awareness of the give-and-take at the FISC. For example, Congress should mandate that the Justice Department publicly disclose on an annual basis the number of times that the FISC requires *additional information* from government attorneys before approving querying of U.S. person information.[159] Those statistics would, like the statistics on the total number of court orders approving U.S. person queries, provide a baseline for future analysis. If the rate of FISC requests for further information increased markedly in a given year, that might indicate that the government was becoming too broad in its initial requests. Legislators and privacy advocates could use that information to push for greater precision in initial applications. Perhaps this inference was unfounded; if so, the intelligence community could push back and convince the doubters. This dialectic would not entail disclosure of intelligence sources or methods; it might merely involve a more open discussion of intelligence agencies' guiding philosophy, supplemented as needed by closed legislative hearings to drill

156. *See* [Name Redacted by Court], at 46–47 n.36 (FISC Ct. Nov. 6, 2015).

157. *Id.*

158. *See* PCLOB § 702 REPORT 2014, *supra* note 16, at 29 (noting that the FISC's review of § 702 certifications "is not limited to the four corners of [agency] documents. The FISC also takes into consideration additional filings by the government to supplement or clarify the record, responses to FISC order to supplement the record, and the sworn testimony of witnesses at hearings.") (citations omitted).

159. A publicly disclosed net figure would not need to include identifying information about the subject of each query.

down into the details. That conversation, like many of the public conversations about intelligence policy that took place in the wake of Edward Snowden's disclosures, would be healthy for democracy.[160]

Furthermore, Congress should require that the government disclose all occasions in which the FISC has commented adversely on the candor of government lawyers, or expressed the view that those lawyers had needlessly delayed in disclosing episodes of compliance. For example, in his November, 2015 opinion, Judge Hogan remonstrated with government attorneys, asserting that they had not been sufficiently forthcoming in explaining implementation of a policy that was several years old and retained U.S. person data when that data was helpful in "collection avoidance."[161] As explained earlier, the government argued that the minimization requirements had an "implicit exception" for collection avoidance.[162] That exception entailed certain U.S. person information that was helpful in flagging entry into the U.S. by certain overseas targets (roamers) who, by virtue of entry into the U.S., were no longer appropriate subjects for warrantless collection.[163] Since the government should cease such collection as soon as possible, information that would flag the U.S. entry of targets is useful for compliance with both statutory and constitutional obligations.[164] However, according to Judge Hogan, the NSA had interpreted the implicit exception too broadly, retaining records that it should have purged.[165] The government argued that it had informed the FISC; however, the FISC indicated in its opinion that this disclosure had not been sufficiently clear.[166]

160. If the number stayed steady, stakeholders would have greater assurance of continuity in the NSA's stance. Either way, the result would be greater legitimacy for the agency.

161. *See* [Name Redacted by Court], at 58–59 (FISA Ct. Nov. 6, 2015); *id.* at 66–68 (observing that the court was "extremely concerned about the NSA's failure to comply" with its own minimization procedures).

162. *See supra* notes 132–33 and accompanying text.

163. [Name Redacted by Court], at 66–68 (FISA Ct. Nov. 6, 2015).

164. *Id.*

165. *Id.* at 57–58.

166. *See id.* at 58 (criticizing the the government's "failure to convey . . . explicitly" to the court that the agency had continued to retain certain information otherwise subject to purge); *see also id.* at 59 (accepting the government's explanation that some incomplete purges had resulted from technical errors that the agency was working to correct). For a valuable account of an NSA compliance issue that involved an interpretation of authority to collect domestic metadata, *see* DeLong & Hennessey, *supra* note 152 (discussing the FISC's disagreement with interpretation by NSA counsel regarding whether search terms used to query daily stream of new call records had to comply with standard of "reasonable and articulable suspicion" of links to terrorism that FISC had imposed on querying of "archived data"). The FISC's concerns about candor do not mean that government lawyers were acting in bad faith. Many of these disputes – perhaps all – involved good faith disagreements. My only point here is that the FISC's perceptions matter more than any single lawyer's subjective intent. Because of the importance of the FISC's perceptions, the agency should highlight to Congress any concerns on this score that the court has advanced.

Candor is even more vital in *ex parte* proceedings like those under § 702, where there is no other party to bring to light inaccurate or incomplete assertions.[167]

Any incidents perceived by the FISC as reflecting a lack of candor by the government's lawyers also have a corrosive effect on the intelligence community's legitimacy. Repeat players in adjudications or transactions know that their reputation is key to their success.[168] Based on the trial lawyer's familiar maxim, "false in one thing, false in all,"[169] shortfalls in candor in one matter will injure an agency's reputation, ultimately calling into question the accuracy of *all* agency positions.[170] Any episode that leads the FISC to question the government's candor should be brought to Congress' attention so that Congress can determine for itself whether the government was sufficiently forthcoming and take appropriate action if Congress determines that greater candor was needed. Ideally, even the prospect of such congressional inquiries will spur the government to bend over backwards in the name of candor. That would be an entirely salutary development; the government should aim to be comprehensive in its disclosures to the FISC, since otherwise the framework simply cannot work as Congress intended.

D. Properly Recording FBI Queries

Reform is also needed in the way that the FBI records queries that yield outputs from the § 702 database. Currently, the FBI does not classify as a query a database search done by FBI personnel not authorized to view § 702 data.[171] That approach seems to stand transparency principles on their head: surveillance stakeholders have a legitimate interest in discovering the volume of search requests made by personnel not eligible to see the results of those requests. A high volume of requests of this sort would indicate that the FBI is either wasting its agents' time or seeking to access information in violation of internal rules. Either development should trigger outside scrutiny. To address this issue, the FBI's protocol requires revision.

Here is what the FBI currently does, per Judge Hogan's November FISC opinion.[172] Suppose that an FBI employee who does not have clearance under FBI rules to access the § 702 dataset inputs a search request. Because of automatic

167. [Name Redacted by Court], at 59 (FISA Ct. Nov. 6, 2015) (describing the "heightened duty of candor in *ex parte* proceedings"); *see also* MODEL CODE OF PROF'L CONDUCT r. 3.3(d) (AM. BAR ASS'N 2016) (providing that in an *ex parte* proceeding, a lawyer "shall inform the tribunal of all material facts known to the lawyer that will enable the tribunal to make an informed decision"); James E. Pfander & Daniel D. Birk, *Article III Judicial Power, the Adverse-Party Requirement, and Non-Contentious Jurisdiction*, 124 YALE L.J. 1346, 1446–47, 1464–65 (2015) (discussing centrality of candor in *ex parte* proceedings).

168. *See* Gilson & Mnookin, *supra* note 124.

169. *Falsus In Uno Doctrine*, BLACK'S LAW DICTIONARY (10th ed. 2014).

170. The key factor under the FAA framework is the view of the FISC, not whether, on some construction of the law or facts, the government's position might be justifiable.

171. *See* [Name Redacted by Court], at 28 (FISA Ct. Nov. 6, 2015).

172. *Id.* at 28–29.

controls, that employee will not be able to view the results of that search.[173] However, the employee will receive a notice of a "hit" if the search does turn up information that fits the search terms.[174] In this situation, the employee's supervisor or a higher-ranking national security employee at the FBI may authorize the employee who conducted the original search to access the material, but only if the search output "reasonably appears" to be foreign intelligence information, to be "necessary to understand foreign intelligence information, or to be evidence of a crime."[175] If it is unclear, the original employee can gain access to the search result "solely" to discern whether the result meets this test.[176] However, the FBI does not count such searches as queries.[177] Congress should require that the FBI change its approach.

A search request is a "query," in common parlance. It should be classified and recorded as such. Failing to count such a request as a query relies on a strained and counterintuitive definition of the term, "query." In the post-Snowden era, officials should avoid these strained definitions. In the transparency context, treating even a frustrated search as a query is the only way to properly align incentives for FBI employees who lack access to § 702 data; otherwise, those employees always have a work-around available, even if they formulate a search that they know is likely to obtain such data. Recording search requests as queries when they uncover § 702 data promotes stakeholder review, without unduly chilling agents' initiative.

E. Transparency's Limits: The Chimera of Quantifying Total Incidental Collection

However, some proposals for transparency in surveillance are either risky or irrelevant to the core concerns that should drive § 702's reauthorization. For example, some commentators have requested that the NSA provide an estimate of the number of U.S. persons whose data is incidentally collected pursuant to § 702.[178] As the following paragraphs demonstrate, this proposal for quantification of incidental collection is impracticable and could potentially undermine both national security *and* privacy.

The key to impracticability of the quantification proposal is its failure to acknowledge a vital aspect of § 702 highlighted in this Article: the difference between upstream and downstream collection.[179] Providing an estimate of incidentally collected U.S. person data in the upstream program is exceptionally

173. *Id.* at 28.

174. *Id.*

175. *Id.* at 29.

176. *Id.*

177. *See* [Name Redacted by Court], at 28 (FISA Ct. Nov. 6, 2015).

178. *See Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4, at 11–12 (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board).

179. *See supra* notes 63–81 and accompanying text.

difficult since the upstream program's stationing at internet hubs means that the number may fluctuate wildly with routers' search for the most efficient pathways for transmitting messages.[180] Moreover, the MCTs unavoidably collected (given current technology) under the upstream program will also fluctuate with respect to U.S. person content – some MCTs will have higher content, others less, depending on technical details of internet transmission that have no relationship to the government's targeting criteria.[181] In the upstream context, therefore, providing a specific number will be technically difficult and not particularly illuminating about the factors governing collection or use of § 702 data. The better course is to take steps outlined earlier in this Article: limits on the querying of upstream U.S. person data, which the FISC and the NSA have already imposed and Congress should codify in § 702's reauthorization, and requiring that the NSA use the best feasible technology to limit incidental upstream collection of MCTs.

In the downstream context, requiring that the NSA provide a precise figure for incidentally collected U.S. person data will pose another risk: supplying information to our adversaries that will enable them to adjust their tradecraft to avoid detection. In the tailored downstream program, disclosing the volume of incidentally collected U.S. person data would provide important clues to our adversaries about the scope of our intelligence capabilities. U.S. intelligence agencies may collect content and metadata on virtually all of the contacts in the U.S. of tasked selectors.[182] Intelligence analysts cast this wide net because they cannot know in advance which contacts are significant and which are trivial or innocuous.[183] Widespread publication of a number that specifically indicates that U.S. intelligence agencies cast a wide net may alert adversaries, encouraging them to adopt means to hinder surveillance such as encryption or spoofed U.S. VPNs.[184] The gain to public deliberation supplied by such disclosures is outweighed by these adverse intelligence consequences.

Finally, as a proponent of the quantification proposal concedes,[185] the proposal could undermine privacy. For MCTs collected upstream, the NSA can readily

180. *See* DONOHUE, *supra* note 1, at 56.

181. *Id.*

182. *FISA Amendments Act Oversight/Reauthorization: Senate Judiciary Committee-Hearing*, 114th Cong. (2015) (testimony of Matthew Olsen, Director, National Counterterrorism Center) (last visited Sept. 11, 2016) (explaining value of tracing possible U.S. contacts through hypothetical example involving two foreign targets in Syria who share a U.S. person's passport photo).

183. *See id.* (observing that sharing a U.S. passport photo could be "innocent" but might signal a more troubling link and would be of interest to the FBI).

184. *See* Kris, *supra* note 1, at 22–24 (pointing to the fact that that ISIL has provided guidance to its members and affiliates on the use of encryption and that this could extend to their use of TOR, VPNs or similar services).

185. *See Senate Judiciary Committee May 2016 § 702 Hearing*, *supra* note 4, at 10 (statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board).

detect that the message does not match a tasked selector. However, the agency may need to review substantially more of the transmission records and content of the communication to determine if it involves U.S. persons. This inquiry will be intrusive, perhaps involving human inspection. That human review of communications might be necessary to classify a communication as involving U.S. persons, even when the communication would not be flagged in any query of incidentally collected information and therefore might not come to any analyst's attention. In other words, the quantification task might require human review of information that would otherwise not trigger human review prior to purging the information. Quantification therefore poses a gratuitous risk of privacy intrusions that Congress should avoid, not embrace.

V. CONCLUSION

In reauthorizing § 702, Congress faces fateful choices. One salient task is reinforcing the strides in transparency and accountability that the intelligence community made after Edward Snowden's disclosures and that Congress codified in the USA Freedom Act.[186] However, a rigid approach would rob intelligence analysts of the agility they need to protect the public against dynamic threats.[187] This Article strives to reach a middle ground that combines effective foreign intelligence collection with a concern for civil liberties.

Congress should do more to encourage the NSA to use technology as a tool to enhance privacy. The NSA and the FBI already use technology to filter out certain data that is irrelevant and prevent unauthorized access to databases.[188] Congress should build on these efforts without stifling innovation within the intelligence community. To achieve these goals, Congress should mandate that the NSA use the best feasible technology to limit incidental collection of U.S. person data.

On requirements for querying U.S. person data, Congress should expressly recognize that collection under § 702 is a tale of two programs: the upstream program that collects foreign intelligence at internet hubs, and the more tailored downstream program, in which ISPs acquire only those communications that match tasked selectors tied to terrorism, espionage, weapons proliferation, or other national security and foreign affairs concerns. Currently, both the FISC and the IC

186. Brand, *Transparency*, *supra* note 7 (commenting on National Intelligence's plan to implement new transparency principles as showing a new habit of transparency); *see also* Cordero, *supra* note 134 (describing transparency principles announced by Director of National Intelligence James Clapper).

187. [Name Redacted by Court], at 29 n.27 (FISA Ct. Nov. 6, 2015) (arguing the FBI's current practice which disallows downstream queries nonetheless gives the FBI the agility it needs).

188. *See id.* at 28 (noting that technological safeguards applicable to FBI queries of § 702 data will deny access to data if official posing query has not received proper training or is otherwise not authorized to obtain access); *see also* Inglis & Kosseff, *supra* note 1, at 12 (explaining that although NSA has been unable to design and implement a filter that reliably and uniformly collects only those specific emails in an MCT that are responsive to specific search requests, the agency nonetheless filters emails in other contexts).

rightly subject upstream collection to tighter regulation, because incidental collection of irrelevant U.S. person communications is more likely in this space.[189] Congress should codify these upstream constraints, requiring a court order for querying of incidentally collected upstream communications.

In the downstream space, however, requiring a court order would be inappropriate.[190] Downstream collection is already far more tailored, and U.S. person communications are more likely here than in the upstream context to reflect national security or other foreign intelligence concerns.[191] Requiring a court order to query such information would make it more difficult for intelligence analysts to connect the dots, without concomitant benefits for privacy.[192]

While rejecting an unduly rigid approach to intelligence collection, reauthorization should enhance the FISC's deliberations with a more institutionalized public advocate. The system put in place by the USA Freedom Act, in which the FISC can seek help from a panel of amici curiae, should be supplemented by a public advocate who can push back against the government in a wider range of cases. This opposing voice will help keep the government honest and ensure that the FISC gets the range of views it needs for sound decisions.[193]

Transparency is also a part of this process. Here, too, Congress should enhance the FISC's deliberations, but legislate with a clear understanding of the nature of both upstream and downstream collection. Surveillance critics' call for an estimate of the total number of incidentally collected U.S. person communications is unworkable in the upstream program, where the shifting nature of efficient internet transmissions and the NSA's unavoidable collection of MCTs make a precise number impossible to obtain.[194] In the downstream program, an estimate would be imprudent since it would publicize too much about the NSA's capabilities.[195]

However, Congress should insist on greater transparency regarding the government's interactions with the FISC. For example, Congress should require that the government disclose to both Congress and the public (using redactions

189. *See* [Name Redacted by Court], at 44 (FISA Ct. Nov. 6, 2015).

190. *In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008) (citing the "high degree of probability that requiring a warrant would hinder the government's ability to collect time-sensitive information").

191. [Name Redacted by Court], at 43–44 (FISA Ct. Nov. 6, 2015).

192. *See In re* Directives, 551 F.3d at 1011–12 (observing that requiring a warrant would "impede the vital national security interests . . . at stake").

193. *See* Mondale, et al., *supra* note 18, at 2297–98 (arguing that as long as FISC proceedings don't resemble traditional warrant proceedings, there must be adverse positions presented); *see also* Vladeck, *supra* note 19, at 1176-77 (positing that one of the more common themes of calls for post-Snowden reforms to United States surveillance law is to provide for more adversarial participation before the FISC).

194. *See* DONOHUE, *supra* note 1, at 56–57.

195. *See* Kris, *supra* note 1, at 22–24 (observing that alerting enemies of the NSA's downstream capabilities may encourage them to adopt encryption or VPNs).

when necessary) when the FISC expresses any concern about the candor of government attorneys. That candor is central to the FISC's work, especially when the government makes *ex parte* requests.[196] Candor serves as a bridge between the government and the court, ensuring that the latter has the information it needs.[197] Gaps in that bridge call for urgent maintenance. The prospect of expressly flagging such gaps for Congress may have a useful *ex ante* effect, diminishing the incidence of such episodes.[198]

In sum, ISIS's rise makes reauthorization of § 702 an urgent priority. Fears of terrorism should not disable the movement toward greater NSA transparency and accountability. However, a nuanced view of the statute that distinguishes between upstream and downstream collection is necessary to preserve the United States' foreign intelligence capabilities. This Article has aimed to provide a blueprint for that delicate balance.

196. Goitein & Patel, *supra* note 4, at 46–47.

197. [Name Redacted by Court], at 59 (FISA Ct. Nov. 6, 2015) (describing the "heightened duty of candor in *ex parte* proceedings" and the overall importance of candor in general).

198. *See supra* Section IV (discussing the risks and benefits of transparency in this context); *see also* Gilson & Mnookin, *supra* note 124, at 513 (hypothesizing that repeat litigators must protect their relationship with the court and their reputation is key to success).