Washington and Lee Law Review

Volume 72 | Issue 3 Article 8

Summer 6-1-2015

Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy

Peter Margulies
Roger Williams University School of Law

Follow this and additional works at: https://scholarlycommons.law.wlu.edu/wlulr

 Part of the Privacy Law Commons

Recommended Citation
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 (2015), https://scholarlycommons.law.wlu.edu/wlulr/vol72/iss3/8

This Article is brought to you for free and open access by the Washington and Lee Law Review at Washington & Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington & Lee University School of Law Scholarly Commons. For more information, please contact lawref@wlu.edu.

Defining "Foreign Affairs" in Section 702 of the FISA Amendments Act: The Virtues and Deficits of Post-Snowden Dialogue on U.S. Surveillance Policy

Peter Margulies*

I. Introduction

The revelations of Edward Snowden about government intelligence collection and surveillance have spurred a national conversation about surveillance.[1] Both government and civil

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

1. *See* David Cole, *Can Privacy Be Saved?*, N.Y. REV. BOOKS, Mar. 6, 2014, at 23 (discussing concerns about privacy). *See generally* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015) (cautioning about risks of foreign surveillance); Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014) (warning about risks of domestic surveillance); Shayana Kadidal, *NSA Surveillance: The Implications for Civil Liberties*, 10 ISJLP 433 (2014) (same). *Cf.* Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1 (2014) [hereinafter *Dynamic Surveillance*] (arguing that pre-Snowden domestic and foreign intelligence collection were consistent with both U.S. statutes and the Constitution, while arguing for reforms to enhance legitimacy of such efforts); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291 (2015) (arguing for procedural norms); Peter Margulies, *The NSA in Global Perspective: Surveillance, Human Rights, and International Counterterrorism*, 82 FORDHAM L. REV. 2137 (2014) [hereinafter *NSA in Global Perspective*] (arguing that U.S. surveillance and intelligence collection policy is consistent with international human rights law, and that reforms would buttress this argument); Peter Margulies, *Rage Against the Machine?: Automated Surveillance and Human Rights*, (Roger Williams Univ. L. Stud. Paper No. 164, 2015), *available at* http://ssrn.com/abstract=2657619 (urging safeguards such as independent review of transnational surveillance).

For case law on various surveillance programs, see *In re* Directives Pursuant to Section 105b of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1006 (FISA Ct. Rev. 2008) (upholding predecessor to FAA as constitutional); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *1, *9–27 (D.

liberties advocates, although they differ on the cost of Snowden's disclosures, agree that this conversation has in some respects been beneficial. In this brief essay, I examine the virtues and limits of that conversation, with respect to a particular statutory provision: the definition of "foreign intelligence information" in § 702 of the FISA Amendments Act of 2008 (FAA) as including information with "respect to a foreign power" relating to the "conduct of the foreign affairs" of the United States.[2] The exact parameters of the surveillance authorized by this language are admittedly unclear. However, privacy advocates—despite their sincerity—have not advanced the conversation in their approach to this issue.[3] A more nuanced dialogue is necessary; this essay seeks to further that process.

While critics have argued that § 702's "foreign affairs" provision is a roving license for open-ended intelligence collection, that position fails to acknowledge the Framers' view that secrecy is necessary for deliberation.[4] Premature public disclosure of lawful surveillance and intelligence collection can sour negotiations and embarrass allies.[5] The Framers, who had practiced diplomacy from the American Revolution through the Founding Era, prized secrecy as one of the virtues of statecraft.[6] Aware that they were pursuing a new legal and political order,

---

Or. June 24, 2014) (upholding surveillance under § 702); *see also* Klayman v. Obama, 2015 U.S. App. Lexis 15189 at *1, *6 (D.C. Cir. Aug. 28, 2015) (vacating preliminary injunction against § 215 program that had been issued by district court). *But see* ACLU v. Clapper, 785 F.3d 787, 813–16 (2d Cir. 2015) (holding that § 215 program exceeded statutory authority).

2. 50 U.S.C. § 1801(e)(2)(B) (2012).

3. For a useful and dispassionate source of analysis and information on § 702 surveillance, see PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 93 (2014) [hereinafter PCLOB § 702 REPORT], https://www.pclob.gov/library/702-Report.pdf.

4. *See* Margulies, *Dynamic Surveillance*, *supra* note 1, at 30–33 (discussing Framers' views); *cf.* David E. Pozen, *Deep Secrecy*, 63 STAN. L. REV. 257, 278, 282–83, 287 (2010) (noting secrecy's risks and benefits).

5. *See* STANLEY ELKINS & ERIC MCKITRICK, THE AGE OF FEDERALISM 348–61 (1993) (discussing reaction of Jefferson and Hamilton during neutrality crisis with France to tactics of French minister Edmond Genet); JOHN LAMBERTON HARPER, AMERICAN MACHIAVELLI: ALEXANDER HAMILTON AND THE ORIGINS OF U.S. FOREIGN POLICY 115–23 (2004) (recounting neutrality crisis).

6. *See* Margulies, *Dynamic Surveillance*, *supra* note 1, at 30–33 (discussing secrecy in American law).

they were also determined to revive virtues from the humanist political tradition that the warring monarchies of Europe had submerged. Moreover, the Framers understood diplomacy's place in international law. The criticism that Founding Era officials such as Hamilton and Madison, despite their differences, directed at the French minister Edmond Genet during the Neutrality Crisis demonstrated their understanding of secrecy's utility for diplomacy.[7]

Properly understood as limited to state conduct, the "foreign affairs" prong of "foreign intelligence information" under § 702 deals largely with matters ancillary to diplomacy, including foreign officials' taking of bribes from private companies, aid to individuals and entities in the theft of U.S. intellectual property, and attitudes toward sanctions on rogue states such as Iran.[8] The "foreign affairs" language, understood as its language and intent suggest, is not a residual clause authorizing *all* the collection and surveillance precluded by other definitions in the statute. It simply allows the United States to gather information relating to other states' compliance with norms and the prospects for international cooperation on enforcement. This U.S. monitoring may occur clandestinely. As with other forms of information-gathering, undue disclosure of the means and subject of the collection may undermine the purpose of the investigation or jeopardize other U.S. foreign policy goals, such as cooperation with states that the United States has targeted for investigation.

Privacy advocates who criticize the breadth of the "foreign affairs" provision in the FAA have generally not recognized its importance for U.S. diplomacy. This failure to acknowledge the diplomatic issues addressed by the "foreign affairs" provision has adversely affected the public debate about surveillance and intelligence collection. To grapple with the issues raised by the "foreign affairs" provision, privacy advocates should have acknowledged the government's interests. They then should have argued that those interests are less important than the government contends or that the government can vindicate those

---

7. *See* ELKINS & MCKITRICK, *supra* note 5, at 348–61 (discussing reaction to tactics of French minister Edmond Genet during neutrality crisis).

8. *See* Charlie Savage, *Book Reveals Wider Net of U.S. Spying on Envoys*, N.Y. TIMES, May 13, 2014, at A8 (discussing the NSA's role in the diplomatic negotiations leading up to Iran sanctions).

interests in an overall regime of transparency. Instead, privacy advocates have advanced an oversimplified view of the Framers' thought that unduly discounts the virtues of secrecy.

One could also view privacy advocates' stance as a more sophisticated effort in tune with the Framers' efforts to fashion procedural proxies for substantive concerns. Although privacy advocates have urged a narrowing or clarification of the "foreign affairs" provision, they have also pushed for procedural reforms that would add checks and balances to the proceedings of the Foreign Intelligence Surveillance Court (FISC). The USA FREEDOM Act of 2015[9] incorporated some of those reforms, including a panel of amicus curiae that would push back against the government's arguments in the FISC.[10] These procedural reforms would act as a proxy for substantive revisions of § 702, by assuring privacy advocates that a neutral party responsive to the public's concerns would monitor intelligence collection and surveillance. Having robust external constraints in place could also reinforce the internal compliance culture within the NSA and other intelligence agencies, and promote faith in technological safeguards that the NSA and other agencies have installed to protect privacy. A conversation that resulted in an institutionalized public advocate and other robust procedural proxies for substantive reform would protect both privacy and the United States' diplomatic imperatives.

This Essay is in three Parts. Part I discusses the FAA's "foreign affairs" provision and privacy advocates' concerns. It also notes the substantial reforms, including greater transparency, that U.S. intelligence agencies such as the NSA have promulgated since the Snowden revelations, in part because of the process initiated by Presidential Policy Directive No. 28 (PPD-28) in January 2014.[11] Part II discusses views of secrecy and diplomacy during the Founding Era, centering on the Neutrality Crisis with France. This section also mentions subsequent judicial decisions on secrecy and statecraft. Part III argues that privacy advocates'

---

9. Pub. L. No. 114–23, 129 Stat. 268, § 401 (2015) (codified at various sections of Title 50 of the U.S. Code).

10. 50 U.S.C. § 1803(i).

11. *See* Presidential Policy Directive/PPD-28 on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 31, at 5 (Jan. 17, 2015) [hereinafter PPD-28] (promulgating certain policies for safeguarding personal information).

failure to acknowledge the need for secrecy in intelligence-gathering supporting U.S. diplomacy has adversely affected the public discussion of surveillance policy. In addition, this section argues that steering the post-Snowden conversation toward procedural proxies such as an institutionalized public advocate at the FISC would enrich public debate.

II. Section 702 and Post-Snowden Reform

Edward Snowden's revelations have resulted in intense public scrutiny of two types of intelligence collection by the NSA. One is domestic—the so-called metadata program, established under § 215 of the USA Patriot Act,[12] which entails the bulk collection of call record information, including phone numbers and times of calls.[13] The other is foreign—programs operated pursuant to § 702 of the FAA.[14] The discussion in this Part centers on § 702. It then discusses post-Snowden reforms that are already in place, and privacy advocates' arguments that more substantive reform of § 702 is necessary.

A. Section 702 and "Foreign Affairs"

Under § 702, the government may conduct surveillance targeting the contents of communications of non-U.S. persons reasonably believed to be located abroad when the surveillance will result in acquiring foreign intelligence information.[15] The

12. 50 U.S.C. § 1861 (2012).

13. *See* Donohue, *Bulk Metadata Collection*, *supra* note 1, at 127–28 (explaining § 215); David S. Kris, *On the Bulk Collection of Tangible Things*, 1 LAWFARE RES. PAPER SERIES, Sept. 29, 2013, at 2–17, http://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/09/Lawfare-Research-Paper-Series-No.-4-2.pdf (discussing the government's bulk collection practices); Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, 1 LAWFARE RES. PAPER SERIES, Sept. 1, 2013, at 2–7, http://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/08/Bradbury-Vol-1-No-3.pdf (explaining bulk collection pursuant to § 215).

14. 50 U.S.C. § 1881a (2012).

15. *See id.* § 1881a(a) (authorizing certain "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information"). Portions of the discussion in this subsection originated in an earlier

government files a certification with the FISC that details its targeting procedures, as well as minimization procedures that reduce the likelihood that analysts will use or retain purely domestic communications or irrelevant information about U.S. persons, defined as U.S. citizens and lawful permanent residents.[16] The FISC can review these and other materials to determine whether the government has complied with the statute, although the FISC does not need to approve individual targets selected by the government.[17] Under the law as of April 6, 2015, the FISC's review of § 702 procedures was ex parte.[18] The FISC, in other words, reviewed the government's certification on its own, without hearing from individuals or entities who might be subject to collection or surveillance, or any other source that might provide a counterweight to the government's submissions.[19]

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."[20] Foreign intelligence information also comprises information relating to possible sabotage[21] and clandestine foreign

---

piece. *See* Margulies, *The NSA in Global Perspective*, *supra* note 1, at 2140–41 (discussing the domestic surveillance programs exposed in the Snowden disclosures).

16. *See* 50 U.S.C. § 1881a (detailing procedures for targeting certain persons outside the United States other than U.S. persons).

17. *See* PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 135 (2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (explaining when the government need not obtain an individual warrant from the FISC). The lack of a requirement for FISC approval of individual targeting choices under § 702 stems from the constitutional status of foreign surveillance and the path to enactment of § 702. The Supreme Court held in *United States v. Verdugo-Urquidez* that non-U.S. persons (defined as those not citizens, lawful permanent residents, or located in the territorial United States) do not enjoy the protections of the Fourth Amendment. 494 U.S. 259, 265 (1990); *cf.* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 291–94 (2015) (discussing reasons for not extending Fourth Amendment protections to communications between non-U.S. persons abroad).

18. *See* 50 U.S.C. § 1881a(k)(2) (2012) (explaining review procedures).

19. *Id.*

20. *Id.* § 1801(e)(1)(A).

21. *Id.* § 1801(e)(1)(B).

"intelligence activities."[22] Another prong of the definition encompasses information "with respect to a foreign power or foreign territory"[23] relating to the "the conduct of the foreign affairs of the United States."[24]

B. Post-Snowden Internal Reforms

Since Snowden's disclosures, NSA officials have been key participants in an extended conversation about intelligence collection and surveillance. That conversation has involved engagement with privacy advocates. It has also involved internal deliberations. In the second half of 2014, the intelligence community and privacy advocates coalesced around a collection of reforms. However, the intelligence community and privacy advocates continue to disagree on the definition of "foreign intelligence information" under § 702, particularly the "foreign affairs" provision. This section describes a number of steps that the intelligence community has taken to promote transparency and protect Americans' privacy. It then discusses privacy advocates' continued critique of the "foreign affairs" prong of § 702.

In January of 2014, President Obama made a speech that emphasized that individuals *around the world* had an interest in the privacy of their communications vis-à-vis the federal government. To protect this interest, President Obama made a number of commitments about U.S. signals-intelligence collection and surveillance. For example, with respect to the international *bulk* (untargeted) collection of signals intelligence, including content information from phone calls and emails, President Obama narrowed U.S. efforts to "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."[25] In addition, he asserted that the NSA would engage in bulk collection of communications only for purposes of "detecting and countering" terrorism, espionage, nuclear proliferation, threats to U.S. forces, and financial crimes, including evasion of

22. *Id.* § 1801(e)(1)(C).
23. *Id.* § 1801(e)(2).
24. *Id.* § 1801(e)(2)(B).
25. PPD-28, *supra* note 11, at 2 n.2.

duly enacted sanctions.[26] President Obama also clarified what the United States would *not* do in bulk collection. First, it would not collect communications content "for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion."[27] Second, it would only disseminate and store information for any person when Section 2.3 of Executive Order 12,333 permitted such activity for U.S. persons: in cases involving "foreign intelligence or counterintelligence," public safety, or ascertainment of a potential intelligence source's credibility.[28]

While § 702 constitutes targeted collection using specific identifiers, not "bulk" collection, President Obama's directive also affected § 702, because PPD-28 initiated a broad intragovernment process on *all* intelligence collection abroad.[29] This process centered on ways in which surveillance and espionage could proceed with maximum feasible respect for the privacy rights of the world's citizens.[30] Moreover, representatives of each intelligence-collection agency spoke widely before a spectrum of stakeholders, including advocacy groups, journalists, scholars, and practitioners, articulating the IC's policies and getting feedback from their interlocutors.[31] In addition, agencies engaged in intelligence collection shared information with the Privacy and Civil Liberties Oversight Board (PCLOB), which had access to top-secret information in assessing both the USA Patriot Act § 215 "metadata" program and the FISA § 702 program.

---

26. *Id.* at 4.

27. *Id.* at 3.

28. *Id.* at 6; Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *reprinted in* 50 U.S.C. § 401 (1982).

29. *See* PPD-28, *supra* note 11, at 1–3 (providing principles governing the collection of signals intelligence).

30. *See id.* at 5 ("All persons should be treated with dignity and respect, regardless of their nationality or where they might reside, and all persons have legitimate privacy interests in the handling of their personal information.").

31. *See, e.g.*, AM. BAR. ASS'N STANDING COMM. ON L. & NAT'L SEC., 24TH ANN. REV. OF FIELD OF NAT'L SEC. L. (2014), http://www.americanbar.org/content/dam/aba/events/law_national_security/LW1114_prog.authcheckdam.pdf (listing panel including Robert Litt, General Counsel, Office of the Director of Nat'l Intelligence, as well as law professors and privacy advocate from American Civil Liberties Union).

The NSA, for example, drafted a lengthy memo on procedures required under Section 4 of PPD-28.[32] The new procedures implemented by the NSA are consistent with PPD-28 in that they "implement the privacy and civil liberties protections afforded to *non-U.S. persons* in a manner that is comparable, to the extent consistent with national security, to the privacy protections afforded to U.S. persons."[33] The Supplemental Procedures (SPs) state that "[p]rivacy and civil liberties shall be *integral considerations* in the planning of . . . SIGINT activities."[34] The SPs reiterate that the IC will not engage in collection "for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, color, gender, sexual orientation, or religion."[35] Importantly, the NSA has accepted that "personal information" has the same definition for both U.S. and non-U.S. persons.[36]

The NSA procedures also contain useful guidance on electronic search procedures. Here, a primary concern is with tailoring search terms to avoid unduly broad collection. The NSA addressed this concern by instructing its analysts that, "[w]herever practicable," the agency will use "selection terms" for searches with a reasonable degree of specificity.[37] For example, the NSA will, when practicable, hone in on "specific foreign intelligence targets," such as specific international terrorists or terrorist groups, or specific topics, such as nuclear weapons proliferation.[38] Minimization procedures that limit use and distribution of the information acquired will also govern analysts' conduct.[39]

In the course of its PPD-28 review, the NSA identified and addressed the special problems of intelligence collected in bulk. Bulk collection is the collection that can have the broadest impact on privacy protections worldwide because it refers to signals

---

32. *See* NAT'L SEC. AGENCY, PPD-28 SECTION 4 PROCEDURES (2015), [hereinafter NSA § 4 Memo] (providing the supplemental procedures required by PPD-28).

33. *Id.* at 1.

34. *Id.* at 5 (emphasis added).

35. *Id.*

36. *Id.* at 6.

37. *Id.*

38. *Id.*

39. *See id.* at 7 (detailing process for handling collections).

intelligence data that, because of technological challenges or operational imperatives, is initially acquired in a wholesale manner. For example, suppose that the United States collected the content of *all* communications within a given country (say, Afghanistan). That wholesale collection would be called "bulk" collection because collection was done without specific selection terms.[40] The NSA limited itself to using such bulk content collection for the purpose of identifying and addressing espionage and other threats from foreign powers, international terrorism, proliferation of weapons of mass destruction (WMD), cybersecurity threats, threats to United States or allied armed forces, and "[t]ransnational criminal threats," including "illicit finance" and evasion of sanctions.[41]

On retention of information, the NSA's guidelines provide for retention for up to five years.[42] The NSA's procedures also limit the dissemination of personal information to information that, if private, is related to an authorized "foreign intelligence requirement," is "related to a crime," or demonstrates a "possible threat to the safety of any person or organization."[43] To enforce these procedures, the NSA relies on an Inspector General, an executive branch official who regularly issues reports and testifies before Congress, the NSA General Counsel, and the NSA/CSS Civil Liberties and Privacy Director.[44] The NSA also has a Compliance Director who provides advice regarding compliance to agency personnel.[45]

---

40. *See id.* at 7 n.1 (defining bulk collection).

41. *Id.* at 7–8. Content information is collected in bulk abroad pursuant to Executive Order 12,333. Exec. Order 12,333, *supra* note 28.

42. NSA § 4 Memo, *supra* note 32, at 8.

43. *Id.* at 9.

44. *See id.* at 10 (explaining responsibilities of the Inspector General). For a candid discussion featuring Rebecca Richards, NSA's current Civil Liberties and Privacy Director, see *Steptoe Cyber Law Podcast, Episode # 52: An Interview with Rebecca Richards* (Feb. 3, 2015), http://www.lawfareblog.com/steptoe-cyberlaw-podcast-episode-52-interview-rebecca-richards [hereinafter Richards].

45. NSA § 4 Memo, *supra* note 32, at 11. For an argument that the NSA has unduly formalized legal compliance, instead of encouraging its analysts to internalize norms, see Margo Schlanger, *Intelligence Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112 (2015). *But see* Richards, *supra* note 44 (describing interactive and iterative process including NSA compliance officials and analysts).

The intelligence community has also made decisive moves toward public transparency, a necessary step for dialogue. For example, the Office of the Director of National Intelligence (ODNI) has published a trove of FISC opinions, which lay out the groundwork for collection programs such as § 215 and § 702. In some cases, the analysis in the FISC opinions has been slender and conclusory; by disclosing the opinions, ODNI has left itself open to these criticisms and helped galvanize reform efforts. The ODNI has also disclosed internal reports that discuss the implementation of these programs and the efforts made to protect U.S. persons' private information.[46] Moreover, demonstrating that it takes transparency seriously, the ODNI has released an extraordinary document, *Principles of Intelligence Transparency for the Intelligence Community*,[47] which articulates a number of guiding norms, including noting that agencies should be "proactive and clear in making information publicly available through authorized channels," including "provid[ing] timely transparency on matters of public interest," "prepar[ing] information with sufficient clarity and context, so that it is readily understandable," and "classify[ing] only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security."[48] In addition, the transparency principles provide a middle course between absolute classification of a given document and wholesale disclosure, reminding officials that they can use "portion marking" to reveal certain content within a document, while keeping the rest secret.[49]

While the transparency principles may not be fulfilled one hundred percent of the time, they are valuable because they provide a neutral index of best practices. A range of stakeholders can use this index, from agency officials predisposed toward

---

46. *See* NAT'L SEC. AGENCY, NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 (2014), https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf (discussing the implementation of Section 702).

47. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PRINCIPLES OF INTELLIGENCE TRANSPARENCY FOR THE INTELLIGENCE COMMUNITY (2015), http://www.dni.gov/files/documents/ppd-28/FINAL%20Transparency_poster%20 v1.pdf.

48. *Id.*

49. *See id.* (describing the use of portion marking and similar means to distinguish classified and unclassified information).

transparency to outside advocates seeking to hold the agency's feet to the fire. Each group is empowered because the IC has gone "on the record" as supporting these principles. The IC may still err on the side of over-classification. In addition, outsiders still face significant impediments in gauging the extent of over-classification, since outside advocates, to paraphrase Donald Rumsfeld, "don't know what they don't know."[50] However, the transparency principles at least shift the conversation several notches toward disclosure, and provide a readily accessible source of authority for those seeking to promote greater openness.

The United States is not the only country that has gestured in the direction of new governance after the Snowden revelations. Britain's Investigatory Powers Tribunal (IPT) recently noted that Britain had violated provisions of the European Convention on Human Rights prior to the Snowden disclosures.[51] However, the IPT recently concluded, the legal and operational "regime" followed by Britain's intelligence and surveillance agency, GCHQ, regarding the "soliciting, receiving, storing and transmitting" of communications of individuals in Britain was now consistent with the European Convention.[52] The only reasonable inference is that GCHQ "cleaned up its act" at least to some degree because of its response to Snowden's actions.[53]

Privacy groups in the United States have continued to seek substantive reform. While the USA FREEDOM Act included some reforms, the privacy community continued to express concern about the scope of § 702. In particular, privacy advocates questioned the provision of § 702 that authorized targeted collection of information "with respect to a foreign power or foreign territory" relating to the "the conduct of the foreign affairs of the

---

50. *See* Pozen, *supra* note 4, at 259–60 (discussing Rumsfeld's quote).

51. *See* Liberty & Others v. Sec'y of State, UKIPTrib 13 77-H (Feb. 6, 2015), *available at* http://www.ipt-uk.com/docs/Liberty_Ors_Judgment_6Feb15.pdf (discussing disclosure of the Prism and Upstream programs).

52. *See id.* ¶ 23 ("[T]he regime governing the soliciting, receiving, storing and transmitting by UK authorities . . . contravened Articles 8 or 10 ECHR, but now complies.").

53. Britain has since enacted a more restrictive surveillance law, but a British court has held that the new law conflicts with European privacy regulations. Davis v. Home Sec'y, No. CO/3365/2014, [2015] EWHC 2092, ¶ 91(c) (Royal Ct. Justice London Div. 2015).

United States."[54] According to privacy advocates, this formulation was overbroad. As a result, U.S. intelligence collection could cover virtually any person, blurring the distinction between bulk and targeted collection.[55] While the privacy advocates' concerns are not wholly without basis, they have paid insufficient heed to the possibility of a narrower definition that centers on U.S. diplomacy and the protection of specific U.S. interests, such as the protection of U.S. intellectual property from theft by foreign powers or non-U.S. persons located outside the United States. Later in this Article, I will explain why greater specificity about these activities would interfere with legitimate U.S. diplomatic goals. To provide a basis for that discussion, the next subsection examines the Framers' attitudes on secrecy and diplomacy.

II. The Framers and the Utility of Secrecy in Statecraft

While the Framers generally believed in the virtues of transparency, they tempered the belief with a cogent awareness of secrecy's utility.[56] As Washington observed during the Revolutionary War, gathering information in war (and arguably other dealings with foreign states) often required secrecy, which could determine the success of particular operations.[57] The

54. 50 U.S.C. § 1801(e)(2)(B) (2012).

55. There is no legislative history on point. The analysis in the text also assumes that in the subsection's wording, the indefinite article, "a," preceding "foreign power" also modifies "foreign territory." In other words, the subsection authorizes only collection regarding a *specific* unit of land that is controlled by a foreign power, or is legally under the administration of a foreign power, but as a practical matter is not controlled by that power (this might describe certain activities within "failed" or "failing" states such as Yemen). Although one could also read the subsection as authorizing *any* collection on *any* territory that was not part of the United States, that broader definition would render the preceding statutory term, "foreign power," superfluous. Courts generally disfavor superfluity in statutory interpretation.

56. *See* Margulies, *Dynamic Surveillance*, *supra* note 1, at 30–33 (discussing secrecy in American law). Alexander Hamilton, for example, praised the office of the presidency as the Framers had conceived it, highlighting the virtues of decisiveness, efficiency, and secrecy. *See* THE FEDERALIST NO. 70, at 424 (Alexander Hamilton) (Clinton Rossiter ed., 1961) ("Decision, activity, secrecy, and dispatch will generally characterize the proceedings of one man in a much more eminent degree than the proceedings of any greater number . . . .").

57. *See* Letter from George Washington to Col. Elias Dayton (July 26, 1777), *in* 8 THE WRITINGS OF GEORGE WASHINGTON FROM THE ORIGINAL MANUSCRIPT

Framers also understood that secrecy could enhance deliberation by expanding choices for decision makers. Premature disclosure of certain controversial options could compromise those options' effectiveness, effectively taking options off the table.[58] That narrowing of choices did not merely affect the officials themselves; it affected the public that officials served. Illustrating the Framers' views, they ensured the secrecy of the deliberations that informed the Constitution's drafting, which were kept under wraps for thirty years.[59]

Consider a formative episode in both U.S. legal and political history: the crisis in relations with France surrounding President Washington's Neutrality Proclamation of 1793.[60] In the Proclamation, President Washington interpreted a treaty between France and the United States as permitting the United States to remain neutral in the war between Britain and France, even though the treaty appeared to require that each party aid the other in wartime.[61] Alexander Hamilton's famed defense of the

---

SOURCES (John C. Fitzpatrick ed., 1931–1944), *available at* http://web.archive.org/web/20110219010057/http://etext.lib.virginia.edu/etcbin/toccer-new2?id=WasFi08.xml&images=images/modeng&data=/texts/english/modeng/parsed&tag=public&part=397&division=div1 (stressing the importance of secrecy in gathering intelligence); *see also* Cent. Intelligence Agency v. Sims, 471 U.S. 159, 172 n.16 (1985) (quoting Washington's order to a subordinate as support for fashioning exemption to Freedom of Information Act (FOIA) about certain controversial domestic research activities funded by Central Intelligence Agency).

58. *See* RAHUL SAGAR, SECRETS AND LEAKS: THE DILEMMA OF STATE SECRECY 2 (2013) ("[C]itizens may themselves prefer secrecy when it leads to the execution of worthy policies that cannot otherwise be carried out."); Dennis F. Thompson, *Democratic Secrecy*, 114(2) POL. SCI. Q. 181, 182 (1999) (asserting that without secrecy, some policies "to which citizens would consent if they had the opportunity . . . could not be carried out as effectively or at all"); *see also* SISSELA BOK, LYING: MORAL CHOICE IN PUBLIC AND PRIVATE LIFE 176 (1978) (conceding that concealing a controversial diplomatic mission and even issuing a "cover story" to cover diplomat's tracks could be a permissible "white lie," but urging that such tactics should be reduced to "an absolute minimum").

59. Max Farrand, *Introduction* to 1 RECORDS OF THE FEDERAL CONVENTION OF 1787, at xi–xii (Max Farrand ed., rev. ed. 1966).

60. George Washington, The Proclamation of Neutrality 1793, *available at* http://avalon.law.yale.edu/18th_century/neutra93.asp.

61. *See* ELKINS & MCKITRICK, *supra* note 5, at 332–53 (describing neutrality crisis); MICHAEL D. RAMSEY, THE CONSTITUTION'S TEXT IN FOREIGN AFFAIRS 78–80 (2007) (explaining the circumstances surrounding Washington's neutrality proclamation); Martin Flaherty, *The Story of the Neutrality Controversy: Struggling Over Presidential Power Outside the Courts*, *in*

Proclamation, although it does not encompass secrecy per se, illustrates the President's ability to manage the interaction of public deliberation and strategic advantage.[62] The strategic benefits that neutrality provided to the United States were evident to all. War with Britain, Hamilton opined, would be "most dangerous,"[63] since the new republic's military assets were inadequate for fending off Britain's might.[64] Although the Democratic Republican faction led by then Secretary of State Thomas Jefferson opposed Hamilton, both factions wished to avoid U.S. entanglement in a European war, given the weakness of the U.S. military."[65] The President, according to Hamilton, therefore, could read the treaty as foregoing futile measures that would deplete and perhaps destroy the fragile new republic.

The political and diplomatic dynamics of the Neutrality Proclamation also illustrate the importance attached to secrecy by the officials of the Founding Era. The crisis precipitating the Proclamation arose because of the insistent public posturing of the French Minister to America, Edmond Genet. Seeking an alliance with the United States against Britain, Genet publicly called out Washington and his cabinet. Seeking to mobilize the American public to commission privateers that would prey on British shipping, Genet denounced the "ancient politics" of "diplomatic subtleties."[66] Genet's direct communication with the American

---

PRESIDENTIAL POWER STORIES 21 (Curtis A. Bradley and Christopher H. Schroeder, eds., 2008) (examining the constitutional issues presented by the neutrality proclamation and surrounding controversy).

62. *See* Alexander Hamilton, Pacificus No. I (1793), *reprinted in* LETTERS OF PACIFICUS AND HELVIDIUS ON THE PROCLAMATION OF PRESIDENT WASHINGTON 6, 11 (1845) [hereinafter Pacificus Letters], *available at* https://archive.org/details/lettersofpacific00hami (discussing the executive power of the president).

63. *Id.* at 46.

64. *Id.* at 43.

65. Hamilton asserted flatly that the United States was incapable of "external efforts which could materially serve the cause of France." *Id.* at 43. Jefferson condemned efforts by the French to inspire Americans to join the fight against Britain, cautioning that the actions of U.S. citizens who "commit murders and depredations on the members of nations at peace with us . . . [were] as much against the law of the land" as Americans who would murder or rob other United States citizens. Letter from Thomas Jefferson to Edmond C. Genet (June 17, 1793) *in* 9 WRITINGS OF THOMAS JEFFERSON 131, 136 (Andrew A. Lipscomb ed., 1903).

66. ELKINS & MCKITRICK, *supra* note 5, at 348.

public and his contempt for the secrecy that facilitates diplomatic exchanges enraged Washington, who bridled at Genet's public "defiance" of the U.S. government's wishes and the French minister's recklessness in "threaten[ing] the Executive with an appeal to the People."[67] Genet's bent for public appeals also alienated both Jefferson and Hamilton, who agreed on little else.[68] In a letter to future president James Monroe, Jefferson noted that he was desperately trying to tame Genet's "impetuosity," and cure Genet of the "dangerous" view that the people of the US will disavow the acts of their government, and that [Genet] has an appeal from the Executive to Congress."[69] Jefferson also deplored Genet's disregard for secrecy and tact in correspondence with James Madison, describing Genet as "disrespectful and even indecent" towards President Washington. Here, too, Jefferson singled out for special ire Genet's penchant for communicating directly with the U.S. Congress and the public, which Jefferson predicted would lead to "universal indignation."[70]

Even more importantly for our present discussion, Genet's public appeals also threatened the interests of *France* in a productive relationship with the United States. Jefferson, who wished to help France to the extent possible, felt far more threatened than Hamilton by Genet's choice of methods.[71] Hamilton viewed Genet's public posturing as of a piece with the anarchic approach he feared from the ever-changing custodians of the French Revolution.[72] Because Hamilton wished to discredit France, Genet's public confrontation with Washington served his

67. *Id.* at 351.

68. *Id.* at 348–51.

69. Letter from Thomas Jefferson to James Monroe (June 28, 1793), *reprinted in* THE PAPERS OF THOMAS JEFFERSON DIGITAL EDITION (Barbara B. Oberg & J. Jefferson Looney eds., 2008–2015), *available at* http://rotunda.upress.virginia.edu/founders/TSJN-01-26-02-0358.

70. Letter from Thomas Jefferson to James Madison (July 7, 1793), *in* THE PAPERS OF THOMAS JEFFERSON DIGITAL EDITION (Barbara B. Oberg & J. Jefferson Looney eds., 2008–2015), *available at* http://rotunda.upress.virginia.edu/founders/ TSJN-01-26-02-0391.

71. *See* HARPER, *supra* note 5, at 116–18 (explaining Jefferson's interactions with Genet during the neutrality dilemma).

72. *See* ELKINS & MCKITRICK, *supra* note 5, at 355, 361 (discussing Hamilton's role).

interests by making *any* aid to France suspect.[73] Jefferson, on the other hand, wished to preserve the possibility of some aid to France,[74] as did Genet's superiors in Paris.[75] The blowback from Genet's public confrontation with the U.S. government threatened to eliminate this option.[76] In other words, the Neutrality Crisis, which resulted in both the Proclamation and Genet's ultimate recall, demonstrated that most central players of the Founding Era viewed secrecy as essential to the cultivation of options in diplomacy and foreign affairs.

Developing the Framers' insight, the Supreme Court has long recognized that secrecy can be necessary for the preservation of options. In *Totten v. United States*,[77] the Court invoked what later came to be known as the state secrets doctrine[78] to support requiring dismissal of a lawsuit seeking payment for services allegedly provided by a clandestine Union operative during the Civil War. The Court noted the need for secrecy in both war and foreign relations.[79] Writing for the Court, Justice Field cautioned that litigation of disputes over the terms of secret missions could expose sensitive dealings "to the serious detriment of the public."[80] Detriment would result not merely from disclosure of covert sources and methods, but from a narrowing of the government's choices.[81] For analogous reasons, courts have shielded intra-branch advice that aids the President's deliberations.[82]

---

73. *Id.* at 360–61.

74. *Id.* at 357.

75. *Id.* at 366–67.

76. *Id.* at 357.

77. 92 U.S. 105 (1876).

78. *See generally* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1249 (2007) (analyzing the state secrets doctrine).

79. *See* Totten v. United States, 92 U.S. 105, 106 (1876) (noting that the doctrine would be relevant in any case concerning "secret employments of the government in time of war, or . . . matters affecting our foreign relations, where a disclosure of the service might compromise or embarrass our government in its public duties . . . .").

80. *Id.* at 106–07.

81. *See id.* (warning that the prospect of litigation could make clandestine operations "impossible" to attempt). *See generally* Tenet v. Doe, 544 U.S. 1 (2005) (reaffirming state secrets doctrine).

82. *See* United States v. Nixon, 418 U.S. 683, 715 (1974) ("The need for confidentiality even as to idle conversations with associates in which casual

III. Post-Snowden Reforms and the Abiding Importance of Secrecy

Privacy advocates critiquing U.S. surveillance in the wake of Edward Snowden's revelations have not acknowledged the Framers' theory and practice of secrecy. They have targeted § 702's foreign affairs provision, characterizing it as a catch-all provision that licenses wholesale government intrusions.[83] This view unduly discounts the foreign affairs provision's text, nature, and purpose. Substantive critiques of the foreign affairs provision have not informed public debate; they have distorted it. On the other hand, arguing for a robust public advocate at the FISC and other procedural proxies for substantive changes to the foreign affairs provision can turn the post-Snowden conversation toward productive goals.

A. Reading and Misreading § 702's Foreign Affairs Provision

The foreign affairs prong of § 702, read in its entirety, has a narrow and entirely legitimate purpose. Narrowing information-gathering to data "with respect to a foreign power" clearly signals that collection will focus on activities of foreign governments. That activity might include receipt of bribes,[84] trade, foreign-owned industries, or foreign officials' views on matters relating to the enumerated factors, such as sanctions evasion or WMDs. James Dempsey, a member of the Privacy and Civil Liberties Oversight Board (PCLOB) with a background as a distinguished privacy advocate[85] informed by access in his PCLOB

---

reference might be made concerning political leaders within the country or foreign statesmen is too obvious to call for further treatment.").

83. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., PUBLIC HEARING REGARDING THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 285–86 (Mar. 19, 2014) [hereinafter PCLOB § 702 Hearing] (response of Laura Pitter) (asserting that statutory provision for gathering of information regarding "the general foreign affairs of the United States allows for the collection of a vast amount of information that does not necessarily have any national security purpose").

84. *See* Foreign Press Center Briefing Transcript, James Woolsey, Former Director, Central Intelligence Agency, *Intelligence Gathering and Democracies: The Issue of Economic and Industrial Espionage* (Mar. 7, 2000), *available at* http://fas.org/irp/news/2000/03/wool0300.htm.

85. *Cf.* James X. Dempsey & Lara M. Flint, *Commercial Data and National*

role to information about § 702, articulated this narrow mission well. At a 2014 hearing, Dempsey observed that the provision authorized collection about the "intent of foreign governments."[86] Moreover, Dempsey observed, foreign governments also constantly seek to learn "what their adversaries are doing."[87] That would make unilateral restraint by the United States unwise. In addition, provisions of international law on privacy should be read against that backdrop of consistent state practice.[88]

Unfortunately for the merits of public debate, surveillance critics have failed to acknowledge these limits in the statute or the importance of intelligence collection supporting U.S. diplomatic efforts.[89] The privacy advocates' failure to acknowledge the nature and purpose of § 702's "foreign affairs" provision has real costs. A more concrete discussion urged by privacy advocates of U.S. efforts to acquire information "with respect to a foreign power" would entail disclosure of U.S. spying on other countries. This spying is

---

Security, 72 GEO. WASH. L. REV. 1459, 1466–67 (2004) (cautioning about adverse privacy effects of government data mining of domestic business records).

86. PCLOB § 702 Hearing, *supra* note 83, at 286.

87. *Id.* Dempsey's observation echoed James Madison. *See* THE FEDERALIST NO. 41, at 257–58 (James Madison) (Clinton Rossiter ed., 1961) (warning that, because the Constitution could not "chain the ambition or set bounds to the exertions of all other nations," it should not be read as needlessly curbing U.S. officials' discretion regarding national security).

88. PCLOB § 702 Hearing, *supra* note 83, at 286. On one occasion, the International Court of Justice has issued preliminary relief barring one state from conducting surveillance on officials of another state. *See generally* Questions Relating to the Seizure and Detention of Certain Documents and Data (Timor-Leste v. Australia), 2014 I.C.J. 156 (Mar. 3). However, that decision involved the narrow issue of ensuring the integrity of arbitral proceedings involving the two countries. *See id.* ¶ 42 (asserting that the right of a state to engage in arbitration would "suffer irreparable harm" if the state conducting such surveillance used the information acquired to gain an advantage).

89. *See* Jennifer Granick, *Reforming The Section 702 Dragnet (Part I)*, JUST SECURITY (Jan. 30, 2014, 5:54 PM), http://justsecurity.org/6574/reforming-section-702-dragnet-1/ (last visited Aug. 30, 2015) (critiquing surveillance practices) (on file with the Washington and Lee Law Review); Harley Geiger, *Four Key Reforms for NSA Surveillance*, CENTER FOR DEMOCRACY AND TECH. (Mar. 14, 2014), https://cdt.org/blog/four-key-reforms-for-nsa-surveillance/ (last visited Aug. 30, 2015) (proposing surveillance reforms) (on file with the Washington and Lee Law Review); Elizabeth Gotein & Faiza Patel, Brennan Center for Justice, *What Went Wrong With the FISA Court* 27 (Mar. 18, 2015), *available at* https://www.brennancenter.org/publication/what-went-wrong-fisa-court (critiquing the "foreign affairs" provision).

often entirely legal under both domestic and international law.[90] However, as the Framers recognized during the Neutrality Crisis, public disclosure will inevitably impede such activities and the diplomacy they support, thus narrowing the range of permissible deliberation.

Openly acknowledging such efforts would complicate U.S. diplomatic efforts in obvious ways. Suppose that the U.S. needed the support of foreign officials to enforce sanctions against Iran or North Korea. However, suppose that the U.S. was also collecting information about how officials in those countries took bribes from either U.S. companies or international firms. If U.S. officials disclosed this intelligence collection, foreign officials might be far less willing to aid the U.S. on sanctions issues.[91]

Moreover, domestic critics of surveillance fail to realize that diplomacy is often a two-level game.[92] Some foreign leaders might wish to tolerate U.S. surveillance, recognizing that espionage is an activity in which many countries participate. That sense of reciprocity on the utility of espionage has helped crystallize the consensus that espionage does not violate international law.[93] However, other factions in those countries might push their leaders to take a more robust stance against U.S. efforts. An accurate reckoning of disclosure's costs must include the influence

---

90. *See* Deeks, *supra* note 1, at 302–13 (analyzing international law on surveillance); Jordan J. Paust, *Can You Hear Me Now? Private Communication, National Security, and the Human Rights Disconnect*, 15 CHI. J. INT'L L. 612, 647 (2015) (stating that "widely practiced espionage regarding foreign state secrets is not a violation of international law").

91. Jack Goldsmith has written insightfully about the nature of U.S. intelligence-gathering, although Professor Goldsmith apparently does not share my view that more candid conversation about U.S. efforts would be problematic for diplomacy. *See* Jack Goldsmith, *The Precise (and Narrow) Limits on U.S. Economic Espionage*, LAWFARE (Mar. 23, 2105, 7:09 AM), http://www.lawfareblog.com/2015/03/the-precise-and-narrow-limits-on-u-s-economic-espionage/ (last visited July 5, 2015) (discussing economic espionage) (on file with the Washington and Lee Law Review).

92. *See* Robert D. Putnam, *Diplomacy and Domestic Politics: The Logic of Two-Level Games*, 42 INT'L ORG. 427, 436 (1988) (critiquing intelligence practices).

93. *See* Richard R. Baxter, *So-Called 'Unprivileged Belligerency': Spies, Guerillas, and Saboteurs*, 28 BRIT. Y.B. INT'L L. 323, 328–29 (1951) (doubting that espionage is a violation of the law of nations); *cf.* John C. Dehn, *The* Hamdan *Case and the Application of a Municipal Offence: The Common Law Origins of 'Murder in Violation of the Law of War'*, 7 J. INT'L CRIM. JUST. 63, 73–79 (2009) (analyzing Baxter's view).

of those factions on foreign leaders. Failure to acknowledge this two-level dynamic detracts from the merits of arguments made by U.S. critics of surveillance policy.

Part of the problem with the conversation about surveillance policy is an asymmetry in the incentives of the conversation's participants.[94] Domestic critics of surveillance policy have no incentive to acknowledge the complex world that makes surveillance necessary. Instead, critics are largely free to "play to their base," mobilizing adherents and financial support through untempered criticism. On the other hand, a diligent government official will wish to acknowledge the legitimate concerns of critics but will also need to protect U.S. interests. However, protecting those interests may limit the disclosures that U.S. officials can make. The asymmetric incentives that favor surveillance critics make the overall conversation less nuanced than it should be.[95]

B. A Way Forward to a More Productive Conversation: Procedural Proxies

Conscientious critics of surveillance policy may tacitly acknowledge the above critique, because, while not abandoning substantive critique, they have pushed for what I call procedural proxies for substantive reform.[96] This section first explains this term and then discusses specific procedural proxies in the surveillance context.

Procedural proxies are process-based protections that ensure disinterested deliberation. The best example in U.S. law is the

---

94. *See* JACK GOLDSMITH, THE TERROR PRESIDENCY: LAW AND JUDGMENT INSIDE THE BUSH ADMINISTRATION 60 (2007) (critiquing the incentive structure of NGOs); Kenneth Anderson, *"Accountability" as "Legitimacy": Global Governance, Global Civil Society and the United Nations*, 36 BROOK. J. INT'L L. 841, 842–44 (2011) (same).

95. Surveillance critics' sincerity is clear. However, critics' incentive structure gives them little or no reason to temper their arguments. That ability to be "temperate and cool" was a virtue the Framers prized. THE FEDERALIST NO. 3, at 41–45 (John Jay) (Clinton Rossiter ed., 1961).

96. I have developed this analysis elsewhere. *See* Margulies, *Dynamic Surveillance*, *supra* note 1, at 51–62 (analyzing potential reforms); Margulies, *NSA in Global Perspective*, *supra* note 1, at 2165–66 (same); *cf.* Deeks, *supra* note 1, at 343–67 (noting the importance of procedural constraints).

Fourth Amendment's requirement of a neutral magistrate.[97] Without a neutral magistrate, the scope of criminal law might allow the executive branch to be the judge in its own case, permitting targeting of political opponents and the resulting impact on First Amendment rights. A neutral magistrate does not erase this problem, but it does mitigate it. Similarly, procedural reforms in §§ 215 and 702 serve as a proxy—the government will be less likely to target political opponents at home or abroad if it knows someone is watching.[98]

One procedural proxy is an institutionalized public advocate at the FISC.[99] The public advocate would play a role in FISC proceedings, weighing in on legal issues and perhaps on the factual sufficiency of government surveillance requests. The USA Freedom Act firmed up this option.[100] An institutionalized advocate would go further, because its role would not be contingent on a request from the FISC, which has been somewhat wary of participation in proceedings that historically have been ex parte.[101]

---

97. *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 316–17 (1972) (interpreting the Fourth Amendment's neutral magistrate requirement).

98. *See* BENJAMIN WITTES & GABRIELA BLUM, THE FUTURE OF VIOLENCE: ROBOTS AND GERMS, HACKERS AND DRONES 200–01 (2015) (acknowledging the hypothetical risk that U.S. surveillance could target disfavored groups but suggesting that sound safeguards have vastly reduced this risk).

99. *See* Margulies, *Dynamic Surveillance*, *supra* note 1, at 51–61 (evaluating Special Advocate proposal); Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate,"* JUST SECURITY (Nov. 4, 2013, 1:34 PM), https://www.justsecurity.org/2873/fisa-special-advocate-constitution/ (last visited Aug. 30, 2015) (analyzing the Special Advocate proposal) (on file with the Washington and Lee Law Review).

100. *See generally* 50 U.S.C. § 1803(i).

101. *See* Letter, Hon. John D. Bates, Director, Admin. Office of the U.S. Courts, to Hon. Dianne Feinstein, Chairman, U.S. Senate Select Committee on Intelligence 2 (Jan. 13, 2014), http://www.lawfareblog.com/wp-content/uploads/2014/01/1-13-2014-Ltr-to-DFeinstein-re-FISA.pdf (discussing problems with privacy advocates); Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act 3–4 (Jan. 10, 2014), http://www.lawfareblog.com/wp-content/uploads/2014/01/1-10-2014-Enclosure-re-FISA.pdf (commenting on reform proposals). *But see* Steve Vladeck, *Judge Bates and a FISA "Special Advocate*," LAWFARE (Feb. 4, 2014, 9:24 AM), http://www.lawfareblog.com/2014/02/judge-bates-and-a-fisa-special-advocate/ (last visited Aug. 30, 2015) (arguing that criticism of the Special Advocate proposal is misplaced because an advocate would only participate in the cases involving substantial legal issues, would not impede FISC proceedings, and "even the finest jurists can occasionally benefit from exposure to . . . arguments that they might not have known to ask for") (on file with the Washington and Lee Law

On balance, as I and others have written, the objections to the public advocate based on security, efficiency, and constitutionality are overstated.[102] A public advocate would actually increase the effectiveness of surveillance programs, by muting political opposition that could otherwise result in far more severe curbs.

Along similar lines, Chairperson David Medine of the PCLOB and PCLOB member and former D.C. Circuit Court of Appeals Judge Patricia Wald have suggested giving a "special master" at the FISC the ability to review a sample of FISA requests.[103] Sampling could be done by selecting key words or having NSA computers search for relevant documents. Sampling would provide a reasonable indication of the kinds of collection that the IC is engaging in based on the "foreign affairs" prong of § 702. That random sampling would not expressly preclude or eliminate potential overbreadth, but it would raise the costs of overbreadth, making it less likely to occur. Moreover, as Hamilton suggested with respect to the very institution of judicial review, random sampling would lead the agencies sampled to develop even more robust internal privacy cultures[104] because such agencies would be rewarded by less intrusive oversight on contested matters.[105]

Procedural reforms would also provide greater legitimacy and credibility for technological safeguards within the intelligence community. For example, the intelligence community has imposed search filters that prevent analysts from querying databases with terms not approved by the FISC.[106] The NSA is also developing

---

Review).

102. *See* Margulies, *Dynamic Surveillance*, *supra* note 1, at 53–61 (evaluating the Special Advocate proposal); Lederman & Vladeck, *supra* note 99 (same).

103. *See* PCLOB § 702 Report, *supra* note 3, at 157 n.567 (describing the proposal for a FISC special master).

104. *See* THE FEDERALIST NO. 78, at 470 (Alexander Hamilton) (Clinton Rossiter ed., 1961) (discussing the concept of judicial review).

105. *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11, at 117–18 (2012) (explaining effect of FOIA rulings on CIA's disclosure practices).

106. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, SAFEGUARDING THE PERSONAL INFO. OF ALL PEOPLE: A STATUS REPORT ON THE DEVELOPMENT & IMPLEMENTATION OF PROCEDURES UNDER PRESIDENTIAL POLICY DIRECTIVE 28, at 7–8 (2014) (discussing procedures to protect personal information); Margulies, *Dynamic Surveillance*, *supra* note 1, at 43–44 (discussing search protocol constraints in the Fourth Amendment context); Nathan Alexander Sales, *Run for the Border: Laptop Searches and the Fourth Amendment*, 43 U. RICH. L. REV. 1091,

audit mechanisms that monitor analysts' compliance with FISC orders and identify efforts to circumvent legal requirements. A public advocate should be entitled to access those compliance records to assess their efficacy.[107]

IV. Conclusion

While the Snowden revelations have sparked a conversation about surveillance policy, that conversation has sometimes lacked nuance. Overly simplistic analysis is a hallmark of discussion of § 702's foreign affairs provision. Critics of surveillance policy have regarded the provision as a license for indiscriminate content collection, despite the provision's roots in legitimate interests of the United States, such as acquiring information about bribery of foreign officials or the theft of U.S. intellectual property. Critics' failure to acknowledge the importance of the foreign affairs provision would have disturbed the Framers, who understood secrecy's utility for statecraft. Procedural proxies, such as a robust public advocate at the FISC, can put the surveillance conversation back on track.

1123 (2009) (urging search protocols in laptop searches); Athul K. Acharya, Note, *Semantic Searches*, 63 DUKE L.J. 393, 409–23 (2013) (discussing search protocols in Fourth Amendment cases).

107. A public advocate or other independent entity should also receive sufficient data about intelligence collection methodology to determine whether methods used by the United States are accurate and reliable. *Cf.* Margaret Hu, *Small Data Surveillance v. Big Data Surveillance*, 42 PEPPERDINE L. REV. 773, 810–15 (2015) (suggesting application to computerized intelligence collection techniques of the *Daubert* test used by courts to assess reliability of scientific evidence).