VOLUME 56, NUMBER 2, SUMMER 2015

American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change

Daniel Severson*

This Note explores why, as a matter of law and policy, the U.S. government has not extended more privacy protections to foreigners subject to signals intelligence activities conducted outside the United States. Edward Snowden's unauthorized disclosures generated significant international pressure on the United States to reform its surveillance practices, including extending more privacy protections to foreigners. The U.S. government responded by increasing transparency and offering policy reforms. However, most of the changes relating to non-U.S. persons are cosmetic; they largely formalize current practices and incentives, making real changes only at the margins. Several possible reasons explain the U.S. government's approach: the cost of surveillance on the U.S. economy may be exaggerated; the diplomatic costs have already declined; the argument that U.S. government surveillance violates international human rights law is tenuous; and alternative policies are not clearly superior to the status quo. Therefore, while affording non-U.S. persons fewer protections may entail some costs, those costs are uncertain or declining, and national security interests as well as political and pragmatic considerations create powerful incentives to maintain the status quo. Signals collection for foreign intelligence purposes provides not just information to detect and thwart international terrorism and espionage, but also information valuable for the conduct of foreign affairs. It appears that in order to facilitate these goals, the U.S. government decided to maintain the distinction between U.S. persons and non-U.S. persons and their different levels of privacy protection.

INTRODUCTION

Beginning in June 2013, Edward Snowden made unauthorized disclosures of sensitive documents regarding U.S. government surveillance around the world. The disclosures revealed a range of details on American electronic surveillance, including the National Security Agency's telephone metadata program at home and other foreign intelligence surveillance programs abroad, the cooperation of global technology companies and other Western intelligence organizations, and the surveillance of world leaders. These revelations generated a media firestorm in the United States and other countries. The United States suffered initial diplomatic fallout, and some sources esti-

* Harvard Law School, J.D. 2016; Harvard Kennedy School, M.P.P. 2016. Daniel Severson served as a Harvard Presidential Public Service Fellow at the U.S. Department of Defense, and a Council of American Ambassadors Fellow at the U.S. Department of State. All statements of fact, analysis, or opinion are those of the author and do not reflect the official policy or position of the U.S. Government. This Note benefited from insights of several people, including Yochai Benkler, Susan Crawford, Laura Donohue, Jack Goldsmith, Philip Heymann, Susan Landau, and Richard Schiffrin. Thank you to the *Harvard International Law Journal* editing team. Special thanks to Becca Donaldson for her generous support. Thank you also to my parents for fostering my love of learning.

mated that the international backlash would cost U.S. firms billions of dollars in lost revenues and market share.[1]

Responding to these pressures, President Obama and Congress directed several reviews of U.S. surveillance practices[2] and initiated policy reforms of intelligence activities, including transparency initiatives.[3] While much of the public debate has centered on the constitutionality of surveillance programs and whether protections for U.S. persons are adequate to safeguard privacy and civil liberties, the sharp international reaction to U.S. surveillance practices abroad also spurred the government to consider whether to afford foreigners more privacy protections. On January 17, 2014, President Obama issued Presidential Policy Directive 28 ("PPD-28"). PPD-28 discusses the protections to be afforded to non-U.S. persons in the context of U.S. signals intelligence programs. The directive states that the U.S. government's "signals intelligence activities must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."[4]

This Note argues that, despite its aspirational language, PPD-28 largely formalizes current practices and incentives within the U.S. Intelligence Community ("IC"), and makes real policy changes only at the margins. Given the extent of international pressure for increased privacy protections, PPD-28's cosmetic changes remain a puzzle. This Note attempts to explain why the U.S. government has not extended more privacy protections to foreigners in the context of signals intelligence.[5] Although the answer surely depends on classified information and other imponderables, much can be gleaned from publicly available information.

---

1. *See, e.g.*, Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. Times (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

2. The President's Review Group conducted a comprehensive assessment of U.S. communications intelligence activities. *See* President's Review Group on Intelligence and Communications Technologies, Exec. Office of the President, Liberty and Security in a Changing World: Report and Recommendations (2013) [hereinafter PRG]. The Privacy and Civil Liberties Oversight Board, an independent executive branch agency, issued detailed reports on two of the National Security Agency's surveillance programs. Under Section 215 of the USA PATRIOT Act, the NSA collects domestic telephone metadata in bulk. *See* Privacy and Civil Liberties Oversight Bd., Exec. Office of the President, Report on the Telephone Records Program Conducted Under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court (2014) [hereinafter PCLOB 215]. Under Section 702 of the Foreign Intelligence Surveillance Act, the NSA collects the contents of electronic communications on targets reasonably believed to be non-U.S. persons located outside the United States. *See* Privacy and Civil Liberties Oversight Bd., Exec. Office of the President, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (2014) [hereinafter PCLOB 702].

3. The Office of the Director of National Intelligence created a website to catalogue these initiatives. *See* IC on the Record, Office of the Director of Nat'l Intelligence, http://icontherecord.tumblr.com/ (last visited Mar. 26, 2015).

4. Exec. Office of the President, Presidential Policy Directive 28: Signals Intelligence Activities (2014) [hereinafter PPD-28].

5. The Note considers only signals intelligence activities, not other intelligence gathering operations.

The Note proceeds as follows. Part I provides the historical and legal context to understand PPD-28. It describes the legal authorities under which the U.S. government conducts signals intelligence collection, the distinction between U.S. persons and non-U.S. persons, and the different levels of privacy protection afforded to each. Prior to PPD-28, the U.S. government made no public commitment to protect the privacy of non-U.S. persons.

Part II analyzes PPD-28's purported reforms. This Note concludes that PPD-28 largely formalizes current practice in the Intelligence Community and that the directive provides sufficient flexibility for the IC to maintain the status quo. PPD-28 is largely cosmetic, and provides real changes only at the margins. However, the explicit, public recognition of foreigners' privacy interests may open the door to future reforms.

Part III analyzes why, despite significant international backlash and apparent costs, PPD-28 did not extend more privacy protections to foreigners. This Note concludes that the economic costs are difficult to calculate and may be exaggerated. The diplomatic costs have declined. At the same time, the benefits domestically are clearer and represent a safeguard that any President has little incentive to abandon. The argument under international law for extending more privacy protections to foreigners is weak and inconsistent with current state practice. Finally, none of the additional available policy proposals analyzed in this Note presents a clearly superior alternative to the status quo as formalized by PPD-28.

I. Historical and Legal Context

In order to appreciate PPD-28, one must understand the previous legal framework and its history. This part describes the legal authorities under which the U.S. government conducts signals intelligence activities, the distinction between U.S. persons and non-U.S. persons, and the different levels of privacy protection afforded to each.

A. Legal Authorities

Before the 1970s, the U.S. government conducted surveillance primarily relying on the President's constitutional authority pursuant to his powers as Commander in Chief, head of the Executive Branch, and the "sole organ" in foreign affairs.[6] Surveillance for foreign intelligence purposes remained unregulated both in and outside the United States. When Congress passed the criminal wiretap act (referred to as "Title III"),[7] section 2511(3) expressly

6. *Cf.* United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936) (noting the "plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations").

7. 18 U.S.C. §§ 2510–22.

provided that the provisions did not "limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the national security of the United States . . . ."[8] The Fourth Amendment served as the only limit on foreign intelligence collection.[9]

Following Watergate, the Church and Pike Committees uncovered and documented abuses by the IC, spurring Congress to enact the Foreign Intelligence Surveillance Act ("FISA") of 1978.[10] For the first time in U.S. history, FISA created statutory authority over foreign intelligence collection conducted within the United States. The Act established the Foreign Intelligence Surveillance Court ("FISC") to review the government's applications for warrants. FISA also formalized the distinction between U.S. persons and non-U.S. persons. As with Title III, however, Congress did not intend to limit the President's authority to conduct foreign intelligence surveillance abroad.[11] Through its narrow definition of "electronic surveillance," Congress limited FISA's application, excluding from the statute foreign-to-foreign wire and radio communications, as well as surveillance conducted abroad of targets located abroad.[12]

Soon after the enactment of FISA, in 1981, President Reagan issued Executive Order 12333.[13] That document carries the force of law within the Executive Branch and establishes rules for the exercise of intelligence activities outside FISA's scope.[14] Authority comes from the Constitution and congressional statutes. Executive Order 12333 specifies the missions and authorities of each element of the IC, imposes restrictions on certain intelli-

8. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, § 802, 82 Stat. 214 (1968). *See also* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 308 (1972) (holding that section 2511(3) is merely a "congressional disclaimer" of intent to define presidential powers in matters affecting national security). The Court held that electronic surveillance in domestic security matters requires a warrant, but noted that there may be an exception to the warrant requirement when the government conducts electronic surveillance for foreign intelligence purposes. *Id.* at 308, 321–22.

9. In *Katz v. United States*, the Supreme Court held that individuals have a reasonable expectation of privacy in the content of their telephone communications, and that a wiretap is therefore a search within the meaning of the Fourth Amendment. 389 U.S. 347 (1967).

10. 50 U.S.C. § 1801 *et seq.* For the history leading up to the enactment of FISA, see generally DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS §§ 2.1-2.7 (2d ed. 2012).

11. KRIS & WILSON, *supra* note 10, § 17:1.

12. *Id.* § 7:17.

13. Exec. Order No. 12333, 3 C.F.R. 200 (1981). In 1976, President Ford issued Executive Order 11905—the first executive order on intelligence—in part to preempt efforts by Congress to create a statutory charter for intelligence activities that he feared would infringe on the President's broad constitutional authority in the sphere of national security. Two years later, President Carter replaced that document with Executive Order 12036, reflecting his administration's balance of priorities. In 1981, fulfilling a campaign promise to reinvigorate America's intelligence capabilities vis-à-vis the Soviet Union, President Reagan issued Executive Order 12333. The document has proven "remarkably durable." Stephen B. Slick, *The 2008 Amendments to Executive Order 12333, United States Intelligence Activities*, 58.2 STUD. IN INTELLIGENCE 2 (June 2014) (chronicling the history of Executive Order 12333 and its reforms).

14. The President's authority to issue Executive Orders comes from the vesting clause in Article II. U.S. CONST. art. II, § 1 ("The executive Power shall be vested in a President of the United States of America.").

gence activities,[15] and establishes principles to strike the balance between intelligence collection and privacy protection.[16] Any intelligence activity that does not fall under FISA is subject to Executive Order 12333 restrictions. Thus, Executive Order 12333 generally governs intelligence activities conducted outside the United States.[17]

The FISA scheme came under pressure as the IC committed to acquiring more information after 9/11 and as changes to communications technology expanded the scope of FISA.[18] As undersea fiber optic cables replaced communications satellites, the use of radio waves to transmit international communications declined. Because FISA regulates international wire communications, but exempts international radio communications, transoceanic communications increasingly fell within the FISC's jurisdiction. The government claimed it therefore increasingly had to spend substantial resources to obtain a FISA court order based on probable cause before it could conduct surveillance on even purely foreign-to-foreign communications.[19] These trends created an incongruity between the law, technology, and intelligence operations, thereby frustrating Congress's original intent.

President George W. Bush responded to 9/11 by authorizing warrantless surveillance, arguably in violation of FISA.[20] That surveillance included four programs: the collection of Internet communications content, Internet communications bulk metadata, telephone communications content, and telephone communications bulk metadata.[21] In 2008, Congress enacted the FISA Amendments Act ("FAA").[22] Section 702 of the FAA provided authority for conducting two of those programs—the collection of Internet and telephone communications content. With sections 703 and 704, Congress required an individualized court order for targeting U.S. persons

15. Specific restrictions include a ban on assassination and limits on human experimentation. *See* Exec. Order No. 12333, *supra* note 13, §§ 2.10, 2.11.

16. *See id.* § 1.1(b) ("All means, consistent with applicable United States law and this Order, and with full consideration of the rights of United States persons, shall be used to develop intelligence information for the President and the National Security Council.") The order provides procedures for collecting and handling information on U.S. persons, including a requirement to use the "least intrusive means." *Id.* §§ 2.3, 2.4.

17. PRG, *supra* note 2, at 70.

18. PCLOB 702, *supra* note 2, at 16.

19. *Id.* at 18. David Kris argues that the government exaggerated this claim. *See* David Kris, *Modernizing the Foreign Intelligence Surveillance Act* 9–13 (Brookings Inst. Series on Counterterrorism & American Statutory Law, Working Paper, 2007), *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15-nationalsecurity-kris/1115_nationalsecurity_kris.pdf.

20. The U.S. government defended the program in a white paper released on January 19, 2006. *See* U.S. Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (2006). A group of scholars argued that the program was illegal. *See February 2, 2006 Letter from Scholars and Former Government Officials to Congressional Leadership in Response to Justice Department Whitepaper of January 19, 2006*, 81, 85 Ind. L.J. 1415 (2006).

21. PCLOB 702, *supra* note 2, at 16.

22. 50 U.S.C. § 1881. The FISA Amendments Act reauthorized many provisions of the Protect America Act of 2007, an interim law that removed FISA's warrant requirements for any surveillance "directed at a person reasonably believed to be located outside the United States," regardless of where the surveillance occurs. Protect America Act of 2007, Pub. L. No. 110–55, § 105A, 121 Stat. 552 (2007).

abroad to acquire foreign intelligence information.[23] Previously, the government conducted targeted surveillance of U.S. persons abroad pursuant to section 2.5 of Executive Order 12333 based on the Attorney General's finding of probable cause. Thus, the FAA expanded the scope of FISA and the jurisdiction of the FISC, removing the targeting of U.S. persons located abroad from executive discretion.[24]

The authorizations for foreign intelligence surveillance create an intricate framework, but can be summarized roughly as follows. With limited exceptions, FISA requires the government to seek an individualized court order when targeting a U.S. person anywhere in the world. "Traditional FISA," the framework that existed before Congress enacted the FAA, governs electronic surveillance conducted within the United States. The FAA governs electronic surveillance where the target is reasonably believed to be abroad. Sections 703 and 704 of the FAA focus on the targeting of U.S. persons outside the United States.[25] Section 702 of the FAA focuses on the targeting of non-U.S. persons outside the United States with the compelled assistance of communications service providers. Executive Order 12333 governs all other intelligence activities, including electronic surveillance outside the United States where the IC resorts to self-help (that is, without the compelled assistance of communications service providers).

B. U.S. Person Status

"U.S. person" is a legal term of art. The term appears both in FISA and Executive Order 12333. A U.S. person is defined as a citizen of the United States or a permanent resident alien lawfully admitted into the United States.[26]

Traditional FISA authorized the government to target specific individuals for surveillance if it could show probable cause to believe that the individual was a foreign power or an agent of a foreign power, and that the target would use the facilities to be placed under surveillance. In enacting FISA, Congress concluded that giving non-U.S. persons within the United States no privacy protections would advance the national security of the United States in countering threats of international terrorism and espionage. For example, the legislative history indicates that Congress received testimony

23. PCLOB 702, *supra* note 2, at 20.

24. *See* EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 13 (2013).

25. When a U.S. person is located outside the United States and acquisition occurs inside the United States, the government must use Section 703. When a U.S. person is located outside the United States and acquisition occurs outside the United States, the government must use section 704. 50 U.S.C. §§ 1881b, 1881c.

26. *See* Exec. Order No. 12333, *supra* note 13; 50 U.S.C. § 1801(i) (2012). Besides individual natural persons, the following can also count as U.S. persons: unincorporated associations substantially composed of citizens or lawful permanent resident aliens, and corporations incorporated in the United States but not controlled by a foreign power. *Id.* For more detail on the definition of U.S. person, see KRIS & WILSON, *supra* note 10, § 8:37.

demonstrating that some aliens who come to the United States temporarily "work[ ] for foreign intelligence networks."[27] Congress also noted the possibility that aliens in the United States on student visas were conducting clandestine intelligence gathering, but that the government could not show that those persons violated U.S. law knowingly, the standard required for U.S. persons.[28] Recognizing the need to conduct foreign intelligence, however, Congress was careful to provide privacy protections for U.S. persons.[29] Executive Order 12333 adopts the same distinction and emphasizes that "[a]ll means, consistent with applicable United States law and this Order, and *with full consideration of the rights of United States persons*, shall be used to develop intelligence information for the President and the National Security Council."[30]

To determine whether a person enjoys U.S. person status, the IC uses presumptions based on physical location and foreignness, and requires analysts to consider information that could rebut those presumptions. Agency policy documents create rebuttable presumptions of U.S. person status.[31] A person located in the United States is presumed a U.S. person unless "the nature of the communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief" to the contrary.[32] Similarly, a person located outside the United States is presumptively a non-U.S. person.[33] An unincorporated association with headquarters outside the United States is likewise presumptively not a U.S. person, unless information indicates a substantial number of its members are U.S. persons themselves.[34] In determining U.S. person status, these presumptions apply regardless of whether the government conducts collection pursuant to FISA or Executive Order 12333.[35]

27. S. Rep. No. 95604 (I), at 21 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904. *See also* Kris & Wilson, *supra* note 10, § 8:44.

28. Kris & Wilson, *supra* note 10, § 8:44. Limiting surveillance on U.S. persons predates FISA. In 1940, President Roosevelt authorized Attorney General Robert H. Jackson to conduct surveillance on communications "of persons suspected of subversive activities against the Government of the United States, including suspected spies," but directed that the use of listening devices be limited "to a minimum" and "insofar as possible to aliens." *Id.* § 3:3. Part of President Roosevelt's memorandum appears in Zweibon v. Mitchell, 516 F.2d 594, 673–74 (D.C. Cir. 1975).

29. *See* H. R. Rep. No. 95-1283, pt. 1, at 63 (1978) ("The bill is designed to provide primary protection to 'United States persons.'").

30. Exec. Order No. 12333, *supra* note 13, § 1.1(b) (emphasis added).

31. *See, e.g.*, Nat'l Sec. Agency, United States Signals Intelligence Directive 18: Legal Compliance and U.S. Persons Minimization Procedures § 9.18(e) (2011) [hereinafter USSID 18]; Def. Intelligence Agency, DoD HUMINT Legal Workshop: Fundamentals of HUMINT Targeting 5, *available at* https://www.aclu.org/files/assets/eo12333/DIA/DoD%20HUMINT%20Legal%20Workshop%20Fundamentals%20of%20HUMINT%20Targeting.pdf (noting that "[a] person or organization outside of the U.S. is presumed not to be a U.S. Person unless information to the contrary becomes known").

32. USSID 18 § 9.18(e)(1).

33. *Id.* § 9.18(e)(2).

34. *Id.* § 9.18(e)(4).

35. *Id.* § 1.2 (implementing minimization requirements stipulated in FISA, Executive Order 12333, and Department of Defense regulations).

Intelligence analysts must determine U.S. person status based upon the "totality of the circumstances available."[36] If the initial lead information does not state the target's location or U.S. person status, then the analyst must infer U.S. person status. An analyst must take into account all available information and cannot ignore information that would rebut the presumption of U.S. person status.[37]

In practice, determining U.S. person status may prove difficult and fact-specific. For instance, when the government seeks to target a particular email account, the fact that a U.S. company (for example, Google) services the account does not determine U.S. person status because many foreigners use U.S. Internet Service Providers ("ISP"). Instead, the government may look to other factors to determine "foreignness," such as the Internet Protocol ("IP") address or the physical means by which the data travels. When the government seeks to target unincorporated associations, it remains unclear in publicly available sources what counts as a "substantial number" of members sufficient to bring a club, student group, lobbying organization, or charitable group within the definition.[38] While the answers to these and other questions remain unclear from publicly available information, a classified directive exists that provides more detailed guidance concerning the determination of U.S. person status.[39] In the context of surveillance conducted pursuant to section 702, the IC has developed "a common understanding" for what constitutes a sufficient basis to determine that a person is not a U.S. person.[40]

According to reports, the National Security Agency ("NSA") appears to determine U.S. person status accurately. The Department of Justice ("DOJ") reviewed one year of data derived from section 702 programs to assess how often NSA's foreignness determinations proved inaccurate. In other words, the DOJ assessed how often the NSA requested information from a communications service provider and subsequently realized that the target was a U.S. person or was located in the United States. DOJ determined that only 0.4% of NSA's targeting decisions turned out to be wrong.[41]

---

36. PCLOB 702, *supra* note 2, at 43. Note that neither FISA nor Executive Order 12333 places any particular burden on the analyst to seek out the relevant information. Instead, that requirement comes from operational guidelines. *See, e.g.*, Office of Civil Liberties & Privacy, Nat'l Sec. Agency, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702, at 5 (2014), *available at* http://www.dni.gov/files/documents/0421/702%20Unclassified%20Document.pdf.

37. PCLOB 702, *supra* note 2, at 43 n.173.

38. Under FISA, to bring an unincorporated association within the definition of U.S. person, Congress specified only that "substantial" means "a significant portion, but less than a majority" of the members must be U.S. persons. Kris & Wilson, *supra* note 10, § 8:37.

39. Office of the Att'y Gen., Attorney General's Guidelines for Domestic FBI Operations VII.U. (2008).

40. PCLOB 702, *supra* note 2, at 43.

41. *Id.* at 44-45.

C. Privacy Protection

This Note concerns the privacy protections at play in signals intelligence activities. The NSA defines signals intelligence, or SIGINT, as "intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems."[42] In conducting signals intelligence, the U.S. government collects some information by targeting specific persons or means of communication and then minimizing information that is irrelevant but that was collected incidentally or inadvertently. The U.S. government also collects some signals intelligence information in bulk. For bulk collection, this paper adopts the definition offered by the National Research Council: collection "in which a significant portion of the retained data pertains to identifiers that are not targets at the time of collection."[43] Under this definition, size alone is not the controlling factor; a set of collected data could be small and still be considered bulk if it included a large proportion of irrelevant information.[44]

The analysis here focuses on the privacy protections under Executive Order 12333 and section 702 of FISA, two authorities under which the government conducts signals intelligence activities. Executive Order 12333 governs most intelligence operations, including bulk and targeted signals intelligence programs. The order provides protections to U.S. persons. Section 702 authorizes a particular, targeted surveillance program that requires minimization in large quantities.[45] Section 702 provides protections for U.S.

---

42. *Signals Intelligence*, NSA, www.nsa.gov/sigint (last visited Mar. 20, 2015).

43. Nat'l Research Council, Bulk Collection of Signals Intelligence: Technical Options 2-9 (2015) [hereinafter Technical Options].

44. *See id.*

45. What counts as bulk collection is not obvious. PPD-28 defines signals intelligence collected in bulk as "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)." PPD-28, *supra* note 4. This definition creates a sharp dichotomy, where bulk collection represents the antithesis of targeted collection (that is, the use of specific discriminants to collect on certain persons). PCLOB adopted this definition and concluded that the section 702 program does not involve bulk collection "because it is based entirely on targeting the communications identifiers of specific people." PCLOB 702, *supra* note 2, at 113. PCLOB nevertheless acknowledged that the number of targets is "considerable" and that the program differs from traditional domestic surveillance based on individual findings of probable cause. *Id.* at 113. However, the IC's definition of bulk collection may be too narrow. Whether a program amounts to bulk collection depends at least in part on how broad the discriminant is, who can be targeted as a person, and, perhaps, how many persons are targeted. For instance, if under section 702 the NSA targets an IP address of a foreign corporate site (a discriminant much broader than one email account for a specific known individual), it can acquire all traffic to or from that address, potentially vacuuming up a huge amount of U.S. person data that has no foreign intelligence value. Arguably, another way the NSA could collect data in bulk under section 702 is by using automated algorithms to generate lists of discriminants based on abstract communications characteristics. Because the FISC does not review each targeting decision individually, there is no bar to using a wide set of discriminants and then narrowing the relevant information. Moreover, even if collection is "targeted," the government still collects a vast amount of irrelevant data incidentally. For more on why the section 702 program may arguably involve bulk collection, see Julian Sanchez, *All the Pieces Matter: Bulk(y) Collection Under § 702*, Just Security (July 25, 2014, 12:15 PM), http://justsecurity.org/13227/pieces-matter-bulky-collection-%702/.

persons whose communications the government *incidentally* acquires when targeting non-U.S. persons abroad. Incidental collection involves collecting information on persons who are not subjects of interest. Other portions of FISA (including traditional FISA, and sections 703 and 704) provide even stronger protections for U.S. persons when the government *intentionally* targets U.S. persons for surveillance,[46] but this Note does not discuss those protections. The protections outlined here govern the incidental or inadvertent collection of U.S. person information in the course of targeting non-U.S. persons. The following discussion first analyzes the protections under Executive Order 12333 and then the protections under section 702 of FISA.

1. *Protections for U.S. Persons Under Executive Order 12333*

Executive Order 12333, the Reagan-era order that governs intelligence activities outside FISA's scope, channels the President's constitutional authority to conduct foreign intelligence collection. Part 2 of the order provides the principles for ensuring privacy protection.[47] The order specifies that surveillance must be conducted pursuant to procedures established by the heads of agencies and approved by the Attorney General.[48] An unclassified document, DoD 5240.1-R,[49] provides those procedures for the Department of Defense ("DoD"). Because NSA is a DoD Intelligence Component, DoD 5240.1-R governs NSA's activities. An NSA document, USSID-18,[50] in turn provides more specificity on those procedures.

Executive Order 12333 and its implementing regulations provide restrictions on the collection, retention, and dissemination of U.S. person information. Procedures 2, 3, and 4 of DoD 5240.1-R appear the most important in the context of signals intelligence activities.[51] Procedure 2 limits collection. It restricts the type of information that the government may collect about U.S. persons to one of 13 categories.[52] Procedure 2 also specifies that when collecting information about U.S. persons the government must use the "least intrusive" means.[53] In other words, the government must first consult

46. Those portions of FISA require that before the government can target U.S. persons, the FISC must make a finding of probable cause to believe that the U.S. person is a foreign power or an agent thereof. 50 U.S.C. § 1881b(c)(1)(B); 50 U.S.C. § 1881c(c)(1)(B).

47. *See* Exec. Order No. 12333, *supra* note 13, § 2.

48. *Id.* § 2.3.

49. Dep't of Def., DoD 5240.1-R: Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons (1982) [hereinafter DoD 5240.1-R].

50. USSID 18, *supra* note 31.

51. Other procedures found in DoD 5240.1-R do not appear to apply to the collection and handling of signals intelligence. For instance, procedures 6, 7, 8, and 9 govern concealed monitoring, physical searches, searches and examination of mail, and physical surveillance, respectively. DoD 5240.1-R C6–C9.

52. Those categories are: information obtained with consent; publicly available information; foreign intelligence; counterintelligence; potential sources of assistance to intelligence activities; protection of intelligence sources and methods; physical security; personnel security; communications security; narcotics; threats to safety; overhead reconnaissance; and administrative purposes. DoD 5240.1-R C2.3.

53. Exec. Order No. 12333, *supra* note 13, § 2.4.

publicly available information or information from cooperating sources before using investigative techniques that would require a warrant.[54]

Procedure 3 limits retention. It stipulates that the government may retain the information only if it acquired such information lawfully pursuant to Procedure 2 or acquired it "incidentally."[55] USSID 18 further specifies that communications "may be retained for five years, unless the Signals Intelligence Director determines in writing that retention for a longer period is required to respond to authorized foreign intelligence requirements."[56] Incidentally collected information may be retained if the information "is necessary to understand or assess foreign intelligence or counterintelligence."[57] USSID 18 further provides that communications may be retained "to maintain technical data bases for cryptanalytic or traffic analytic purposes . . . for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably likely to become, relevant to a current or future foreign intelligence requirement."[58] Identity information not needed to maintain such databases should be "deleted or replaced by a generic term when practicable."[59] Once retained, access to U.S. person information is limited to those persons "with a need to know."[60]

Procedure 4 limits dissemination. Once an agency collects and analyzes information, it may want to report that intelligence to policymakers or share it with other agencies. Procedure 4 governs "the kinds of information about United States persons that may be disseminated, without their consent, outside the DoD intelligence component that collected and retained the information."[61] Information about U.S. persons that identifies those persons may be disseminated only if the information was lawfully collected or retained or both pursuant to Procedures 2 and 3, and "the recipient is reasonably believed to have a need to receive such information for the performance of a lawful governmental function."[62] In addition, the identity of the U.S. person must be "necessary to understand the foreign intelligence information or assess its importance."[63] When an agency disseminates information, USSID 18 further specifies that all SIGINT reports be written "to focus solely on the activities of foreign entities and persons and their agents."[64] The agency must substitute generic phrases (e.g., "U.S. PERSON") for spe-

54. *See* DoD 5240.1-R C2.4.2.
55. *See id.* at C.3.3.1, C.3.3.2.
56. USSID 18 § 6.1.a(1).
57. DoD 5240.1-R C3.3.2.2.
58. USSID 18 § 6.1.a(2).
59. *Id.*
60. DoD 5240.1-R C3.4.1.
61. *Id.* at C4.1.
62. *Id.* at C4.2.1, C4.2.2.
63. USSID 18 § 7.2.c.
64. *Id.* § 7.1.

cific information (e.g., the name of a particular U.S. person) so as not to identify U.S. persons.[65]

Procedure 5 provides specific limitations for electronic surveillance. However, the details remain classified. Procedure 5 specifies only that signals intelligence activities of foreign communications and military tactical communications that incidentally collect U.S. person data must be conducted exclusively in accordance with a classified annex to the procedure.[66]

The procedures under Executive Order 12333 are subject to both internal and external oversight. NSA's Inspector General ("IG") is charged with conducting regular inspections and reporting compliance with the procedures quarterly and annually to the Director of NSA and the President's Intelligence Oversight Board.[67] NSA's General Counsel ("GC") must provide legal advice regarding SIGINT, as well as "review and assess" the legal implications of all new major requirements and signals intelligence activities.[68] Although NSA is the chief producer of SIGINT, other intelligence agencies must meet similar reporting and oversight requirements.

2. *Protections for U.S. Persons Under Section 702 of FISA*

Section 702 of FISA provides more detailed privacy protections for U.S. persons. While Executive Order 12333 can authorize a range of signals intelligence activities, section 702 of FISA regulates only one specific type of surveillance. Section 702 permits the Attorney General and the Director of National Intelligence to authorize jointly the (1) targeting of non-U.S. persons; (2) reasonably believed to be located outside the United States; (3) with the compelled assistance of an electronic communications service provider; (4) to acquire foreign intelligence information.[69] In practice, the NSA conducts two known programs under section 702: PRISM and upstream collection.[70]

The main privacy protections for U.S. persons include express limitations, targeting and minimization procedures, and at least nominal judicial review of the program. As a threshold matter, section 702 expressly imposes five limitations: the government may not intentionally target persons inside the United States; may not engage in reverse targeting;[71] may not intentionally target U.S. persons abroad; may not knowingly collect wholly domestic communications; and must conduct the surveillance in accordance with the Fourth Amendment to the U.S. Constitution.[72] Taken together, these base-

65. *Id.*
66. DoD 5240.1-R C5.3.
67. USSID 18 § 8.1 (c)–(d).
68. *Id.* § 8.2.
69. 50 U.S.C. § 1881a(a); *id.* § 1881a(b); *id.* § 1881a(g)(2)(A).
70. For a description of these programs, see PCLOB 702, *supra* note 2, at 7, 33–41.
71. Reverse targeting involves conducting surveillance against a non-U.S. person for the purpose of targeting a U.S. person.
72. 50 U.S.C. § 1881a(b).

line limitations ensure that the section 702 program targets non-U.S. persons reasonably believed to be located abroad.

The chief privacy protections for surveillance conducted under section 702 are targeting and minimization procedures.[73] It may be useful to think of the targeting procedures as "front-end" protections on collection; they reinforce the five threshold limitations. Minimization procedures provide "back-end" protections on the handling of information already collected. Targeting procedures are procedures "reasonably designed" to "ensure that any acquisition . . . is limited to targeting persons reasonably believed to be located outside the United States" and to prevent acquisition of purely domestic communications.[74] Minimization procedures must be "specific procedures . . . that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[75] In practice, minimization involves removing the names and references to U.S. persons unless necessary to assess foreign intelligence information.

The NSA's minimization procedures implementing section 702 provide several key protections for U.S. persons. In general, when the government collects U.S. person information incidentally or inadvertently it must purge such information when that information positively identifies a U.S. person based in the United States and is not relevant to a foreign intelligence purpose. The government must "destroy inadvertently acquired communications of or concerning a United States person at the earliest practical point in the processing cycle at which such communication can be identified . . . ."[76] When processing Internet data acquired through NSA upstream collection techniques, the minimization procedures also specify that data which potentially includes U.S. person communications must be segregated into a separate repository and reviewed by specially trained analysts.[77] If, upon review, the information includes communications from an identifiable U.S. person, then the government may use such communications only "to protect against an immediate threat to human life (e.g., force protection or hostage situations)."[78] Communications of or concerning U.S. persons must

73. For the latest declassified minimization procedures, see IC ON THE RECORD, *supra* note 3.

74. 50 U.S.C. § 1881a(d)(1).

75. *Id.* § 1801(h)(1).

76. NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 3(b)(1) [hereinafter MINIMIZATION PROCEDURES], *available at* https://www.aclu.org/files/assets/minimization_procedures_used_by_nsa_in_connection_with_fisa_sect_702.pdf.

77. *Id.* § 3(b)(5).

78. *Id.* § 3(b)(5)(b)(2)(c).

be "destroyed upon recognition."[79] Likewise, communications identified as wholly domestic communications will be "promptly destroyed upon recognition" unless the NSA Director specifically determines in writing that the communication is reasonably believed to contain foreign intelligence information, is evidence of a crime, or is reasonably believed to contain technical database information or information necessary to understand a communications security vulnerability.[80]

Like DoD 5240.1-R, NSA's minimization procedures for section 702 also impose restrictions on the retention and dissemination of U.S. person data. NSA may only retain or disseminate information reasonably believed to contain foreign intelligence information or evidence of a crime.[81] Information of or concerning U.S. persons may be retained only if it is necessary for the maintenance of technical databases, is evidence of a crime, or indicates that the U.S. person is an agent of a foreign power, targeted by foreign intelligence, engaged in the unauthorized disclosure of classified information, or engaged in international terrorism.[82] Communications that do not meet the retention standards must be destroyed after two years (in the case of upstream collection) or five years (in the case of communications collected through PRISM).[83]

Unlike programs conducted under Executive Order 12333, the FISC provides judicial oversight for the section 702 program. The court reviews the targeting and minimization procedures to ensure that they satisfy the statutory requirements and the Fourth Amendment.[84] The court also reviews the certification made by the Attorney General and the Director of National Intelligence, though this review is only a matter of form to ensure that it "contains all the required elements."[85] The FISC therefore cannot second-guess the government's assertion of a foreign intelligence purpose. Moreover, it is important to note that the FISC does not review individual targeting decisions and does not find probable cause to believe the target is a foreign power or an agent of a foreign power, as is required under traditional FISA and sections 703 and 704 of the FAA. Thus, while the FISC provides an external check on the section 702 program—a check not present for programs conducted under executive discretion pursuant to Executive Order

79. *Id.* § 3(c). The minimization procedures also provide that monitoring must cease as soon as the NSA discovers communications between a U.S. person under criminal indictment and her attorney. *Id.* § 4 ("The relevant portion of the communication containing that conversation will be segregated and the National Security Division of the Department of Justice will be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein.").

80. *Id.* § 5.

81. *Id.* § 3(b)(4).

82. *Id.* § 6(a)–(b).

83. *Id.* § 3(c).

84. 50 U.S.C. § 1881(a)(i).

85. *Id.* § 1881(a)(i)(2)(A).

12333—the FISC's role remains limited to reviewing the overall constraints of the program.[86]

Based on publicly available information, compared to oversight of programs under Executive Order 12333, oversight for the section 702 program is more extensive. Internally, the NSA and other agencies participating in the section 702 program have developed measures to evaluate and oversee compliance with the minimization procedures, as well as facilitate external oversight.[87] A host of various NSA entities oversee NSA's use of section 702 authorities. They include the Office of the Director of Compliance, the Office of General Counsel, the Signals Intelligence Directorate's Oversight and Compliance section, and the Director of Civil Liberties and Privacy Office. In order to ensure compliance with the targeting and minimization procedures, these entities provide NSA-wide compliance risk assessments, as well as random tests of individual targeting decisions and decisions to query, retain, or disseminate acquired data.[88] Incidents of noncompliance must be reported to the DOJ and the Office of the Director of National Intelligence ("ODNI"). On an annual basis, NSA and other agencies conducting the section 702 program must report specific statistics, including the number of disseminations of U.S. person identities, the number of U.S. person identities that were subsequently unmasked, and the number of section 702 targets that were subsequently determined to be located within the United States.[89] In enacting the FAA, Congress mandated that the Attorney General and the Director of National Intelligence ("DNI") provide a semiannual report of the program to four congressional committees.[90] That report includes a complete set of documents—government filings, hearing transcripts, and FISC orders—related to the court's consideration of the section 702 certification of the program.[91] It also includes the classified Attorney General and Director of National Intelligence's semiannual assessment regarding compliance with procedures, the annual reports of agency heads that conduct section 702 acquisition, and any reports by the inspectors general.[92]

Taken together, whether under Executive Order 12333 or section 702 of FISA, the privacy protections for U.S. persons subject to signals intelligence activities fall into four broad categories: restrictions on what kinds of information may be collected; restrictions on what information can be retained and for how long; restrictions on what information may be disseminated; and oversight mechanisms. The system is designed to protect only the pri-

86. For more details on FISC review of section 702, see KRIS & WILSON, *supra* note 10, § 17:3.

87. PLCOB 702, *supra* note 2, at 66.

88. *Id.* at 67.

89. *Id.* at 69–70.

90. The committees are the Senate Select Committee on Intelligence, the Senate Committee on the Judiciary, the House Permanent Select Committee on Intelligence, and the House Judiciary Committee. *See* 50 U.S.C. § 1881a(l)(1).

91. PCLOB 702, *supra* note 2, at 77.

92. *Id.*

vacy of U.S. persons. Both Executive Order 12333 and section 702 start with the presumption that the government has free license to collect and handle foreign intelligence information. On top of that presumption, the Congress and the Executive Branch then added layers of protections for U.S. persons.

3. *Treatment of Non-U.S. Persons*

Overall, prior to PPD-28 the U.S. government made no public commitment to protect the privacy of non-U.S. persons. For electronic surveillance under FISA, none of the NSA's minimization procedures for the section 702 program applied to non-U.S. persons: "Foreign communications of or concerning a non-United States person may be retained, used, and disseminated *in any form* in accordance with other applicable law, regulation, and policy."[93] Similarly, none of the restrictions on collection, retention, and dissemination under Executive Order 12333 apply to non-U.S. persons. The one exception is that, as a matter of *policy*, the U.S. government treats the information of persons from so-called Second Party countries (Australia, Canada, New Zealand, and the United Kingdom) with the same standards as U.S. person information.[94] Otherwise, the framework protects foreigners only by restricting the types of information that the government can collect.[95] Under the section 702 program, those types of information are limited. The government can only acquire "foreign intelligence information."[96] The statute defines such information as limited to information that relates to, or is necessary to: protecting against actual or potential attacks; protecting against international terrorism and proliferation of weapons of mass destruction; conducting counterintelligence; and collecting information with respect to a foreign power or territory that concerns U.S. national defense or foreign affairs.[97] As PCLOB has emphasized, "[t]hese limitations do *not* permit unrestricted collection of information about foreigners."[98] Under Executive Order 12333, the categories that limit the types of information that the government may collect on U.S. persons do not apply to collection on non-U.S. persons.[99] No formal constraints exist; the types of information that may be collected are therefore broader. However, operational requirements and resource constraints provide some limitation on the type of information collected. On a semi-annual basis, the President approves the National Intelligence Priorities Framework, which directs intelligence components to con-

93. MINIMIZATION PROCEDURES, *supra* note 76, § 7 (emphasis added).

94. *See infra* note 238.

95. The statute also stipulates certain civil penalties for improper information collection practices, though they apply equally where victims are U.S persons and where victims are non-U.S. persons. *See* PCLOB 702, *supra* note 2, at 99.

96. 50 U.S.C. § 1881a(a).

97. *See* 50 U.S.C. § 1801(e).

98. PCLOB 702, *supra* note 2, at 99.

99. *See supra* note 52.

centrate scarce resources on collecting certain types of information in accordance with priorities set by the Principals Committee of the National Security Council ("NSC") and approved by the President.[100] This document ensures that the IC focuses resources on, say, assessing Iran's nuclear program rather than the hobbies of Czech nationals. Still, these constraints are not formalized or binding.

In sum, other than the requirements that information collected meet foreign intelligence needs and the general oversight provided by the inspectors general and through reporting to Congress, non-U.S. persons have virtually no privacy protections under programs conducted pursuant to Executive Order 12333. Section 702 of FISA is unique among U.S. intelligence programs in that it provides at least nominal judicial review for non-U.S. persons. Yet the FISC does not review individual targeting decisions, and the minimization procedures do not apply to non-U.S. persons. Overall, persons with U.S. person status enjoy greater privacy protections under programs conducted pursuant to both Executive Order 12333 and FISA Section 702.

II. PPD-28 Formalizing Current Practice

President Obama issued Presidential Policy Directive 28 on January 17, 2014. The directive "articulates principles to guide why, whether, when and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes."[101] Specifically, the directive discusses the protections to be afforded to non-U.S. persons in the context of signals intelligence activities. This Note concludes that each of the purported policy reforms formalizes current practices and incentives within the IC, and the directive provides sufficient authority for the IC to maintain the status quo.

PPD-28 is divided into six major sections, four of which are worth examining here.[102] Section 1 establishes principles governing the collection of signals intelligence. These principles formalize current practice. The first requirement stipulates that the collection of signals intelligence be lawful. This requirement offers nothing new, since all signals intelligence activities are conducted either pursuant to executive order or statute.

The second requirement stipulates that the government collect signals intelligence "exclusively where there is a foreign intelligence or counterintelligence purpose to support national and departmental missions and not

100. *See* Office of the Dir. of Nat'l Intelligence, Intelligence Community Directive 204: Roles and Responsibilities for the National Intelligence Priorities Framework (2007) [hereinafter ICD 204], *available at* http://www.dni.gov/files/documents/ICD/ICD_204.pdf.

101. PPD-28.

102. Sections 1–4 provide the substantive policy changes. Sections 5 and 6 mandate subsequent reports and provide general disclaimers, respectively.

for any other purposes."[103] While this provision requires privacy and civil liberties be "integral considerations," and prohibits collection to suppress dissent, the crux of the provision is that intelligence agencies must collect to meet the mission. Again, this requirement does not depart from current practice. The intelligence agencies conduct surveillance in order to meet certain collection requirements set by the White House and ODNI in the National Intelligence Priorities Framework.[104]

The third requirement stipulates that the government may not conduct economic espionage. Collection of foreign private commercial information is authorized only to protect national security and not "to afford a competitive advantage to U.S. companies and U.S. business sectors commercially."[105] This policy also does not seem to alter the relevant landscape. The prohibition is consistent with U.S. government statements that American intelligence agencies do not practice economic espionage, where such espionage entails government agencies illicitly acquiring foreign technology or business information and giving it to American companies for competitive advantage. At the same time, however, the directive allows room for other types of economic espionage. In a footnote the directive clarifies that "identifying trade or sanctions violations or government influence or direction" are exempted from this principle.[106] The United States could engage in economic espionage to help U.S. business sectors, though not "commercially," at least indirectly. Under PPD-28, the U.S. government could still conduct activities to understand how sanctions regimes are operating, to monitor dangerous dual-use technologies, to learn about bribery practices, or to gather intelligence from foreign private defense and intelligence firms.[107]

The fourth requirement stipulates that signals intelligence activities be "as tailored as feasible."[108] On its face, this requirement does not seem to alter current practice. The IC has an incentive to tailor its collection activities; to do otherwise would be inefficient. This stipulation could track a provision that appears in Executive Order 12333, which requires the IC to use the "least intrusive" collection techniques within the United States and against U.S. persons abroad.[109] However, "as tailored as feasible" and "least intrusive" do not necessarily amount to the same standard. A collection technique (such as collecting email content from a specific account) could be tailored but still quite intrusive. Therefore, PPD-28 does not adopt the stricter requirements for U.S. persons under Executive Order 12333.

---

103. PPD-28 § 1.

104. *See supra* note 100 and accompanying text.

105. PPD-28 § 1.

106. *Id.* at n.4.

107. For a brief but useful overview of economic espionage, see Jack Goldsmith, *Why the USG Complaints Against Chinese Economic Cyber-Snooping Are so Weak*, LAWFARE (Mar. 25, 2013, 9:01 AM), http://www.lawfareblog.com/2013/03/why-the-usg-complaints-against-chinese-economic-cyber-snooping-are-so-weak/.

108. PPD-28 § 1.

109. Exec. Order No. 12333, *supra* note 13, § 2.4.

In section 2, PPD-28 purports to place "new limits" on the use of signals intelligence collected in bulk. The limits apply to non-U.S. persons located outside the United States.[110] The limits essentially restrict the use of bulk signals intelligence to detecting and countering six types of *actual threats* to the United States: (1) espionage; (2) terrorism; (3) weapons of mass destruction; (4) cybersecurity; (5) threats to U.S. or allied military personnel; and (6) transnational criminal threats.[111] The directive emphasizes that "[i]n no event may signals intelligence collected in bulk be used for the purpose of . . . achieving any purpose other than those identified in this section."[112] While this provision appears to prohibit the collection of bulk signals collection for purposes other than detecting or countering actual threats, the directive includes key exceptions. Section 2 pertains to "the use" of bulk signals intelligence, not the collection itself. To reinforce this point, the directive includes a footnote that states: "The limitations contained in this section do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection."[113] In addition, the directive does not apply to activities undertaken to "test or develop signals intelligence capabilities."[114] Taken together, these exceptions mean that U.S. intelligence agencies could acquire bulk signals intelligence *temporarily* and then search that information in a targeted manner for purposes other than to detect or counter actual threats. The acquisition would not count as "collection," and therefore the limitations would not apply.[115] Because "temporarily" remains undefined, under this exception agencies could use bulk signals intelligence collection for purposes beyond detecting and countering actual threats.

Section 3 of PPD-28 requires national security policymakers to consider the risks and benefits of signals intelligence collection activities. This provision requires the heads of departments and agencies involved in signals intelligence activities to review on an annual basis whether the government should maintain such programs.[116] The provision explicitly acknowledges that signals intelligence collection entails certain risks, including "the risk

110. "These limits are intended to protect the privacy and civil liberties of all persons, whatever their nationality and regardless of where they might reside." PPD-28 § 2.

111. *Id.*

112. *Id.*

113. *Id.* at n.5.

114. *Id.* at n.3.

115. This interpretation would mirror other legal interpretations the IC has employed to shift the burden of procedures from gathering information to analyzing information. For instance, the Defense Intelligence Agency interprets "collection" as a term of art to mean "gather[ ] . . . plus": "For the purposes of DoD 5240.1-R, 'collection' is officially gathering or receiving information, plus an affirmative act in the direction of use or retention of that information. For example, information received from a cooperating source (for example, the FBI) about a terrorist group is not 'collected' unless and until that information is included in a report, entered into a database, or used in some other manner which constitutes an affirmative intent to use or retain that information." DEF. INTELLIGENCE AGENCY, INTELLIGENCE LAW HANDBOOK: DEFENSE HUMINT SERVICE 3–5 (2004), *available at* https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf.

116. PPD-28 § 3.

of damage to [U.S.] national security interests and [U.S.] law enforcement, intelligence-sharing, and diplomatic relationships should [U.S.] capabilities . . . be compromised."[117] One hopes that policymakers adequately considered such risks prior to the issuance of PPD-28. Perhaps naming the risks will focus more attention on them. Though it may impose additional internal procedures, this policy reform appears modest because officials could merely acknowledge the risks without ensuring that the benefits justify them.

Section 4 offers a bigger apparent change. It stipulates that the Secretary of State create a "Coordinator for International Diplomacy" to coordinate with the intelligence agencies the U.S. government's foreign policy efforts related to international information technology issues and to serve as a point of contact for foreign countries that raise concerns about signals intelligence activities. In March 2014, the Secretary of State assigned this role to the Under Secretary of State for Economic Growth, Energy, and the Environment.[118] Allocating these responsibilities to an undersecretary charged with fostering economic development and advancing American leadership on Internet issues likely signals the seriousness with which the Obama administration treats the economic and diplomatic concerns of allies and international partners relating to information disclosure from signals intelligence activities. Given her portfolio, this official is in a good position to think strategically about these issues.

Perhaps more important, section 4 also requires the Director of National Intelligence and the Attorney General to develop policies and procedures that protect the personal information of non-U.S. persons collected through signals intelligence activities. The directive stipulates that "[t]o the maximum extent feasible consistent with the national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."[119] In practice, these policies and procedures refer to how the intelligence agencies disseminate and retain foreign intelligence information. PPD-28 stipulates that personal information of non-U.S. persons "shall" be disseminated and retained only according to the standards applicable to U.S. persons under Executive Order 12333.[120]

Interestingly, the interim status report to PPD-28, which the DNI released on October 17, 2014, changes the operative language from "shall" to "should."[121] "Shall" generally imposes a requirement, while "should" is

117. *Id.*

118. U.S. Dep't of State, *Designation of the Senior Coordinator for International Information Technology Diplomacy* (Mar. 5, 2014), *available at* http://www.state.gov/r/pa/prs/ps/2014/03/223001.htm.

119. PPD-28 § 4.

120. *Id.* § 4(a)(i).

121. Office of the Dir. of Nat'l Intelligence, Safeguarding the Personal Information of All People: A Status Report on the Development and Implementation of Procedures Under Presidential Policy Directive 28 (2014), *available at* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf [hereinafter PPD-28 Interim Report].

merely advisory. Under the status report, each intelligence agency "should consider" disseminating and retaining non-U.S. person information using U.S. person standards. The status report further emphasizes that "[w]hile comparable protections are to be sought, PPD-28 does not require the Intelligence Community to apply the *identical* procedures to both U.S. person and non-U.S. person information."[122] Executive Order 12333 only serves "as an appropriate starting point."[123] The status report thus allows each agency to decide for itself what privacy protections to adopt and under what circumstances. This change may reflect a lack of consensus among the 17 intelligence agencies. In fact, in the 2015 Anniversary Report on Signals Intelligence Reform, the DNI released 12 agency-specific procedures to implement section 4 of PPD-28.[124] Some agencies provide fewer details because they are not involved in collecting signals intelligence or have different mission requirements. Agencies also emphasize different exceptions to their procedures implementing PPD-28. In terms of general principles, however, the procedures track closely the language of PPD-28. For instance, both the NSA and CIA's new supplemental procedures for information on non-U.S. persons reiterate that privacy and civil liberties shall be "integral considerations" in planning signals intelligence activities, and that the agencies will not collect signals intelligence to suppress dissent or to conduct economic espionage.[125]

In perhaps the biggest policy change to emerge from PPD-28, the 2015 Anniversary Report lays down a five-year destruction requirement for non-U.S. person information. Under the new rule, IC components must delete information on non-U.S. persons within five years unless the agency determines that the information is "relevant to, among other things, an authorized foreign intelligence requirement," or if the DNI determines, "after considering the views of the Office of the Director of National Intelligence Civil Liberties Protection Officer and agency privacy and civil liberties officials, that continued retention is in the interest of national security."[126] In addition to this broad exception, agency-specific exceptions highlight how this rule may not alter current practice. The NSA's procedures emphasize that the retention requirement applies only to information in its "original

122. *Id.* at n.2.

123. *Id.*

124. Office of the Dir. of Nat'l Intelligence, *Signals Intelligence Reform: 2015 Anniversary Report*, IC on the Record, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28 (last visited Mar. 26, 2015).

125. Nat'l Sec. Agency, USSID 18 SP0018: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data of Non-United States Persons §§ 3.2, 3.4 (2015) [hereinafter SP0018], *available at* https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf; Cent. Intelligence Agency, Policies and Procedures for CIA Signals Intelligence Activities 1, 3 (2015) [hereinafter CIA Policies and Procedures], *available at* https://www.cia.gov/library/reports/Policy-and-Procedures-for-CIA-Signals-Intelligence-Activities.pdf.

126. *Signals Intelligence Reform: 2015 Anniversary Report*, *supra* note 124.

and transcribed" form, which could exclude finished intelligence products.[127] The NSA also excepts information in unintelligible form, such as encrypted or enciphered information.[128] The CIA's procedures include a list of ten broad exceptions to the five-year requirement.[129] The five-year destruction requirement and accompanying exceptions track the provisions for U.S. persons in USSID 18 and Executive Order 12333; however, the IC can likely find an exception for non-U.S. person information far more easily than for U.S. person information. Thus, while the new destruction requirement may shift the starting presumption and require more internal procedures before an agency can retain non-U.S. person data, in practice the IC will likely not need to alter its activities.

The 2015 Anniversary Report also reinforces the current paradigm by granting stronger protections to U.S. persons. For information collected pursuant to section 702 of FISA, the NSA will now need to supply a written statement of facts showing that a query is likely to return foreign intelligence information.[130] The government must also delete U.S. person information that has been determined to lack foreign intelligence value, and the government cannot introduce such information into a criminal proceeding against the person without the approval of the Attorney General.[131] Taken together, these heightened requirements for U.S. person information—requirements that do not extend to non-U.S. person information—serve to reinforce the status quo distinction based on territory and nationality.

In sum, while PPD-28 may create some changes at the margins by adding internal government procedures and coordination, in practice the directive's aspirational language still allows the IC to maintain the status quo.

III. Why PPD-28 Makes Mostly Cosmetic Changes

In one sense, it comes as no surprise that the United States continues to afford greater privacy protections to Americans. Across most topics and in most contexts, every nation favors its own citizens. At the same time, however, in the wake of Snowden's unauthorized disclosures, the U.S. government felt pressure to reform surveillance practices, including surveillance on non-U.S. persons. This section attempts to explain why, given apparently large economic and diplomatic costs and international legal obligations, the U.S. government did not extend more substantive privacy protections to foreigners.

127. SP0018, *supra* note 125, § 6.1(a).
128. *Id.*
129. CIA Policies and Procedures, *supra* note 125, at 4.
130. *Signals Intelligence Reform: 2015 Anniversary Report*, *supra* note 124.
131. *Id.*

A. Economic Costs

By some estimates, U.S. companies stand to lose billions of dollars from consumers choosing non-U.S. technology service providers that they perceive as less vulnerable to U.S. surveillance. In July 2013, a month after the Snowden disclosures, a Cloud Security Alliance survey found that 66% of non-U.S. members reported that they had either canceled a project with or were less likely to use U.S.-based cloud service providers.[132] Analysts estimated that the U.S. cloud computing industry could lose between $35 billion and $180 billion.[133] A January 2014 survey suggests these predictions may already be playing out: 25% of 300 British and Canadian businesses surveyed indicated that they were moving their data outside of the United States.[134] One Washington, D.C.-based privacy lawyer warns that American companies are "taking a beating in the market place" as a result of perceived discrepancies in privacy protections.[135] In anticipating that countries will develop stricter domestic privacy regulations and data-localization laws, the Information Technology and Innovation Fund predicts that growth in the U.S. technology-services industry could slow by as much as four percent.[136]

Perceived indiscriminate signals intelligence collection has also adversely affected American companies in other industries.[137] The German government announced that it would end its contract with Verizon in response to the company's cooperation with the NSA.[138] And in December 2013, Brazil decided to award a $4.5 billion contract to replace its fighter jets to Saab instead of Boeing, the presumed favorite.[139] As for international trade, the United States and the European Union ("EU") are seeking to update the Safe Harbor framework, a way for companies in Europe to legally transfer data on EU citizens to the United States without running afoul of EU data protection directives. Updating the Safe Harbor arrangement is a predicate for finalizing the Transatlantic Trade and Investment Partnership, yet nego-

132. Cloud Security Alliance, Government Access to Information Survey Results 2 (2013), *available at* https://downloads.cloudsecurityalliance.org/initiatives/surveys/nsa_prism/CSA-govt-access-survey-July-2013.pdf.

133. Miller, *supra* note 1.

134. Cloud Security Alliance, *supra* note 132, at 2.

135. Telephone Interview with Bret Cohen, Associate, Hogan Lovells LLP (Oct. 29, 2014).

136. Danielle Kehl et al., Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity 3 (2014), *available at* http://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf.

137. The problem extends beyond bulk signals intelligence activities; U.S. firms also complain about the impact on international business of targeted collection, backdoors, and efforts to undermine encryption standards. Still, because the costs and benefits across these issues are likely to be similar, this Note focuses on bulk signals intelligence activities, as well as targeted, large-scale collection under section 702.

138. Kehl et al., *supra* note 136, at 2.

139. *Id.*

tiations over a national security exemption have proven the "most difficult."[140]

Given these apparently large economic costs, one might expect U.S. firms to pressure the U.S. government to change its surveillance policy in order to help them avert further losses. In fact, following Snowden's unauthorized disclosures, top leaders of major U.S. tech firms, like Apple, Google, and Twitter, visited the White House to call for surveillance reform.[141] Yet the U.S. government did not extend more privacy protections to foreigners subject to signals intelligence collection. This is a puzzle that might be explained on several different grounds.

First, the economic costs may be exaggerated. Whether high-tech business leaders, lawyers, journalists, or consultants, each party has an interest in exaggerating the damage from electronic surveillance in order to bolster sales, readers, or the attention of lawmakers. Exaggeration is possible. In the context of cybercrime, computer security companies claimed that the economic cost from intellectual property theft was high—as much as $1 trillion.[142] These estimates may have been exaggerated, however, because the assessments relied on self-reported figures and because the computer security companies had an incentive to portray a more dangerous threat environment to drive business.[143]

Second, some of the most dramatic economic concerns have failed to materialize. Take data localization, for instance. Roughly speaking, data localization laws require companies to store citizens' data within a country's borders.[144] Such initiatives are not new. China, Iran, and Russia have imposed policies that require all citizen data to remain in-country.[145] Snowden's unauthorized disclosures prompted democratic governments like Brazil to pursue these expansive policies, as well.[146] However, Brazil ultimately dropped a data localization requirement from its Internet reform

140. *U.S. Refuses to Change National Security Exemption in Safe Harbor Talks*, 32 INSIDE U.S. TRADE 1–2 (2014).

141. *See* Dominic Rush et al., *Tech Companies Call for 'Aggressive' NSA Reforms at White House Meeting*, THE GUARDIAN (Dec. 17, 2013), http://www.theguardian.com/world/2013/dec/17/tech-companies-call-aggressive-nsa-reforms-white-house (noting that some U.S. tech firms sought surveillance reform because they believed a "perceived lack of security" put them at a disadvantage in securing international business); *see also* REFORM GOVERNMENT SURVEILLANCE, https://www.reformgovernmentsurveillance.com/ (last visited Apr. 12, 2015) (arguing on behalf of several major U.S. tech firms that governments "should not undertake bulk data collection of Internet communications").

142. *See* Peter Maass & Megha Rajagopalan, *Does Cybercrime Really Cost $1 Trillion?*, PROPUBLICA (Aug. 1, 2012), http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

143. *See id.*

144. For a summary and analysis of data localization policies, see Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders*, 2.3 LAWFARE RESEARCH PAPER SERIES (July 21, 2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/07/Lawfare-Research-Paper-Series-Vol2No3.pdf.

145. *Id.* at 3.

146. *Id.* at 3–4.

bill.[147] Building data centers has turned out to be expensive and complicated. Analysts have also argued that such data localization may actually reduce privacy because data held offshore and outside of U.S. firms would be less secure and would result in lower legal hurdles for NSA collection.[148] Besides data localization, some observers also worried that suspicion about the integrity of U.S. technology firms in the wake of the Snowden revelations would cost these companies,[149] but stock prices for companies like Facebook and Cisco have not suffered.[150]

Third, when the economic costs are indeterminate, a change in policy may prove difficult to justify. With regard to signals intelligence activities abroad—whether bulk collection or perceived indiscriminate collection—it is difficult to calculate whether the domestic benefits of such activities are more important than the economic losses to U.S. firms. In the face of uncertain costs and benefits, any President has little incentive to abandon what she may consider a safeguard against low-probability, high-impact risks.

Fourth, the U.S. government may view the economic costs as tolerable. One recent study attempted to quantify the annual costs of cyber crime and cyber espionage by analogizing them to the costs of doing business in other industries. The report noted that car crashes, maritime piracy, and pilferage of sales inventory each cost society roughly one percent of national income per year.[151] Despite these costs, we continue to drive cars, use giant merchant ships, and sell goods because these activities provide aggregate benefits in efficiency and convenience. The U.S. government may have made a similar calculation: although surveillance may cost U.S. firms, such costs are acceptable in light of the benefits to national security, whether that means information to combat international terrorism or strategic intelligence to inform foreign policy. The costs may even be more tolerable than other accepted costs. For instance, automobile accidents cost the United States between $99 billion to $168 billion per year, or between 0.7% and 1.2% of GDP, a cost we are willing to accept because of the benefits such

147. Alison Grande, *Brazil Nixes Data Localization Mandate from Internet Bill*, LAW360 (Mar. 20, 2014), http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill.

148. *See* BRUCE SCHNEIER, DATA AND GOLIATH 188 (2015); Hill, *supra* note 144, at 29.

149. *See, e.g.*, Eamon Javers, *Is a Snowden Effect Stalking US Telecom Sales*, CNBC (Nov. 15, 2013), http://www.cnbc.com/id/101202361.

150. Cisco stock prices reached a seven-year high in February 2015. Julie Bort, *Cisco's Stock Soars to a 7-Year High as the Company's Turnaround Takes Hold*, BUS. INSIDER (Feb. 12, 2015), http://www.businessinsider.com/ciscos-stock-soars-to-a-7-year-high-2015-2. Facebook's share price more than tripled from $23.29 on June 3, 2013 to $83.80 on March 16, 2015. *Facebook, Inc. (FB)*, YAHOO! FIN., http://finance.yahoo.com/echarts?s=FB+Interactive#{%22range%22%3A%225y%22%2C%22scale%22%3A%22linear%22} (last visited Mar. 27, 2015).

151. MCAFEE & CTR. FOR STRATEGIC AND INT'L STUDIES, NET LOSSES: ESTIMATING THE GLOBAL COST OF CYBERCRIME: ECONOMIC IMPACT OF CYBERCRIME II 11 (2014), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf.

transportation provides.[152] By contrast, estimates indicate NSA surveillance costs U.S. cloud computing firms (a major sector of the U.S. economy) less—between $17.5 billion and $90 billion over two years (2014–2016).[153] While these cost figures are not entirely comparable, they suggest that the government may have reason to consider the costs to society as acceptable.

Fifth, it is possible that the damage is done, and that further government action will not help U.S. firms in a meaningful way. In this sense, Snowden's unauthorized disclosure of sensitive documents may have created a one-time sunk cost. If this is true, then the economic cost is unavoidable but should not affect future decision-making.

The analysis of economic costs from electronic surveillance necessarily involves imponderables, but some combination of the factors outlined here probably accounts for the lack of substantive change to privacy protections for foreigners.

B. Diplomatic Costs

Snowden's unauthorized disclosures of NSA surveillance on U.S. allies definitely strained U.S. foreign relations in the short term, but the consequences appear to be receding. Brazil and Germany—two of the most outspoken critics of U.S. surveillance post-Snowden—provide good examples. Brazilian President Dilma Rousseff canceled a visit to the White House in response to revelations that the NSA spied on her and the Brazilian oil company, Petrobas.[154] Her decision marked the first time a world leader turned down a state dinner with the President of the United States.[155] However, in an interview in July 2014, Rousseff eased tensions by indicating that the Obama administration was not directly responsible for the increased spying measures established after September 11, 2001.[156] In signs of warming relations, in January 2015, Vice President Joe Biden attended President Rousseff's second inauguration, and in March 2015, the White House re-invited Rousseff for a state visit.[157] As for Germany, for months after the Snowden revelations, Chancellor Angela Merkel refused to visit the United States. But

152. McAfee & Ctr. for Strategic and Int'l Studies, The Economic Impact of Cybercrime and Cyber Espionage 5 (2013), *available at* http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf.

153. *See* Miller, *supra* note 1.

154. Simon Romero, *Brazil Says It Spied on U.S. and Others Inside Its Borders*, N.Y. Times (Nov. 4, 2013), http://www.nytimes.com/2013/11/05/world/americas/brazil-acknowledges-spying-on-diplomats-from-us.html.

155. Heather Arnet, *Why Dilma Canceled on Obama*, Daily Beast (Oct. 23, 2013), http://www.thedailybeast.com/witw/articles/2013/10/23/dilma-rousseff-and-the-state-visit-that-didn-t-happen.html.

156. Mia de Graaf, *Joe Biden Turns on the Charm in Historic Visit to Brazil*, Daily Mail (Jan. 1, 2015), http://www.dailymail.co.uk/news/article-2893982/Joe-Biden-turns-charm-historic-visit-Brazil-president-s-inauguration-grapples-rebuild-damaged-relationship.html.

157. Bryan Winter, *Exclusive: U.S. Bets on Brazil, Extends New Invitation to Rousseff,* Reuters (Mar. 24, 2015), http://www.reuters.com/article/2015/03/24/us-brazil-usa-rousseff-idUSKBN0MK29W20150324.

in a February 2015 visit to the White House, not only did Merkel not criticize U.S. surveillance, but she also praised the U.S. intelligence community for its coordination with German agencies in mitigating security threats.[158]

Evidence suggests other countries have muted their political and legal responses. One year after Snowden's unauthorized disclosures, a report analyzed responses from legal and Information Technology ("IT") experts in 29 countries. The report concluded that

> the overwhelming majority of countries assessed . . . have not responded in any tangible, measurable way to the Snowden disclosures that began in June 2013. While there has been a notable volume of "activity" in the form of diplomatic representations, parliamentary inquiries, media coverage, campaign strategies, draft legislation and industry initiatives, there has—at the global level—been an insignificant number of tangible reforms adopted to address the concerns raised by the Snowden disclosures.[159]

The report came just one year after the initial revelations, and states could take more action over time. Still, the report suggests that the revelations may not spur other countries to take meaningful action, particularly since attention fades over time. By June 2014, global media coverage had already declined to less than two percent of the reporting from the initial maelstrom.[160] Therefore, the U.S. government might reasonably conclude that diplomatic tensions will ease over time.

Assessing the economic and diplomatic costs versus the benefits of U.S. surveillance necessarily involves a high degree of indeterminacy. It would be difficult to measure the impact of extending various privacy protections to non-U.S. persons. Even if the impact could be measured, some of the key supporting facts and conclusions would certainly (and perhaps justifiably) remain classified. The risks associated with granting more protections to non-U.S. persons are not obviously large or small. They involve uncertainty. In this sense, the lack of protections may be viewed as a safeguard against international terrorism, espionage, and other threats to national security. Does it make sense to terminate that policy? In the face of uncertain but potentially devastating risks, incentives push in the other direction. Moreover, it is important to remember that the IC collects information not only to detect and thwart international terrorism and espionage, but also to facilitate the conduct of foreign affairs. Extending privacy protections may slow

158. Julia Edwards, *Obama Acknowledges Damage from NSA Eavesdropping on Angela Merkel*, HUFFINGTON POST (Feb. 9, 2015), http://www.huffingtonpost.com/2015/02/09/obama-angela-merkel-nsa_n_6647058.html.

159. SIMON DAVIES, A CRISIS OF ACCOUNTABILITY: A GLOBAL ANALYSIS OF THE IMPACT OF THE SNOWDEN REVELATIONS 5 (2014), *available at* http://www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf.

160. *Id.* at 6.

or restrict such activities to the point where valuable information is lost. If valuable information is lost, then the question becomes whether it is worth incurring the cost of economic harm and diplomatic irritation. Only if the diplomatic and economic harms are significant and sustained should the United States consider placing substantial constraints on signals intelligence gathering. In the event, the economic costs may be exaggerated, and such costs may also decline over time as the controversy fades from view. The diplomatic costs also appear temporary; many countries, including U.S. allies and partners, spy on each other's citizens, and diplomatic relations are improving.

C. International Legal Obligations

A case can be made that U.S. signals intelligence collection against foreigners abroad violates international law, but this argument is tenuous. The argument could be framed as follows. The United States ratified the International Covenant on Civil and Political Rights ("ICCPR") in 1992. Drawing on the text of the Universal Declaration of Human Rights,[161] Article 17 of the ICCPR enshrines the right to privacy under international law. It states:

> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.[162]

With regard to this and other rights, by its terms the treaty prohibits discrimination, including discrimination on the basis of national origin.[163] The Human Rights Committee ("HRC") has further emphasized that the Covenant's "guarantee applies to aliens and citizens alike."[164] Moreover, with respect to the rights to privacy, family, home or correspondence, "[t]here

161. Article 12 of the Declaration reads: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Universal Declaration of Human Rights art. 12, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1948).

162. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, S. Treaty Doc. No. 95-20, 6 I.L.M. 368 (1967), 999 U.N.T.S. 171 [hereinafter ICCPR].

163. Article 26 reads:

> All persons are equal before the law and are entitled without any discrimination to the equal protection of the law. In this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

Id. at art. 26.

164. U.N. Human Rights Comm., *CCPR Gen. Comm. 15: The Position of Aliens Under the Covenant*, ¶ 2, U.N. Doc. HRI/GEN/1/Rev. 1 (Sept. 30, 1986), *available at* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=INT%2fCCPR%2fGEC%2f6625&Lang=en.

shall be no discrimination between aliens and citizens in the application of these rights."[165]

Continuing the argument, the ICCPR's jurisdictional clause indicates these obligations apply to U.S. activities both inside and outside the United States. Article 2 defines the scope of the ICCPR as binding a State Party "to respect and to ensure" the rights recognized in the treaty "to all individuals within its territory and subject to its jurisdiction."[166] At the very least, then, international law requires the United States to provide equal privacy protections to citizens and non-citizens alike when conducting surveillance within U.S. territory.[167] The United States has agreed to guarantee the right to privacy to *all individuals* within its territory.[168] The HRC interprets the ICCPR such that these obligations apply to U.S. activities outside U.S. territory, as well. As explained below, the United States contests this view, but the Committee emphasizes that a State Party must "respect and ensure the rights laid down in the Covenant to anyone within the power or effective control of that State Party, even if not situated within the territory of the State."[169] Essentially, the HRC reads the phrase "subject to [a State Party's] jurisdiction" expansively to include persons "within the power or effective control of the forces of a State Party acting outside its territory."[170] The Committee emphasizes that such obligations would obtain, for instance, for persons under the control of a State Party's peacekeeping force, but the Committee notes that the obligations apply "regardless of the circumstances in which such power or effective control was obtained."[171] Given this interpretation, some human rights advocates argue that the NSA's surveillance of foreigners abroad amounts to "effective control" of their correspondence, and therefore that such surveillance "interfer[es]" with the right to privacy.[172] Because the section 702 program involves the compelled assistance

165. *Id.* ¶ 7.

166. ICCPR, *supra* note 162, at art. 2.

167. With respect to the right to privacy, some advocates argue that international human rights law may also require the United States to provide additional protections, including transparency, independent oversight, and the right to a remedy in cases of abuse. *See Public Hearing Regarding the Surveillance Program Conducted Pursuant to Section 702 of the Foreign Intelligence Surveillance Act before the Privacy and Civil Liberties Oversight Board*, 7–14 (2014) (public comment by Amnesty International USA and the American Civil Liberties Union) [hereinafter ACLU Public Comment], *available at* https://www.aclu.org/sites/default/files/assets/aiusaaclusubmissiontopclob.pdf.

168. Interestingly, this obligation is broader than obligations under domestic law. In *United States v. Verdugo-Urquidez*, the Supreme Court held that the Fourth Amendment protections against unreasonable search and seizure do not apply to non-U.S. persons located outside the United States. United States v. Verdugo-Urquidez, 494 U.S. 259, 265-66 (1990). The Court underscored that the Fourth Amendment only applies to "the people," which refers to a "class of persons who are part of [the] national community or who have otherwise developed sufficient connection with [the United States] to be considered part of that community." *Id.* at 265. But the Court left unanswered whether an illegal alien in the United States would receive such protections. *Id.* at 272–73.

169. U.N. Human Rights Comm., *CCPR Gen. Comm. 31: The Nature of the General Legal Obligation Imposed on States Parties to the Covenant*, ¶ 10, U.N. Doc. CCPR/C/21/Rev.1/Add. 13 (May 26, 2004).

170. *Id.*

171. *Id.*

172. ACLU Public Comment, *supra* note 167, at 17–22.

of communications service providers, these advocates argue the surveillance necessarily occurs within U.S. territory or within its jurisdiction. And because large volumes of foreign-to-foreign Internet traffic travel over U.S.-based infrastructure, the treaty may also apply to many surveillance activities conducted pursuant to Executive Order 12333.[173]

The argument is tenuous for several reasons. First, the Human Rights Committee's interpretations are not binding, and the U.S. government has never committed to them. The HRC is charged with receiving reports submitted by nations under the ICCPR's self-reporting provisions and issuing "such general comments as it may consider appropriate."[174] The Committee has assumed broader powers of interpretation, but its original mandate is narrower and nonbinding.[175] Contrary to the HRC, the U.S. government contends that the ICCPR's obligations do not run to activity outside a State Party's jurisdiction. According to the U.S. government, the text of the treaty imposes a "dual requirement": obligations only apply when a person is *both* within U.S. territory *and* under its jurisdiction.[176] The treaty's negotiating history confirms this interpretation. Anxious about the ICCPR applying to foreign persons under U.S. occupation after World War II, the United States suggested adding the phrase "within its territory."[177] The language was adopted, and subsequent efforts to remove the phrase failed.[178] But even if one reads "and" as "or" and the ICCPR were to apply to U.S. electronic surveillance activities outside the United States, the U.S. government may nevertheless satisfy its obligations. For instance, section 702 programs—which limit collection to specific national security purposes—are not necessarily "arbitrary or unlawful," especially in the absence of an international norm as to when surveillance of another state's citizens amounts to "arbitrary or unlawful" action.[179] In sum, under the ICCPR the United States is bound—as a matter of international law, but not domestic law—to protect the right to privacy of citizens and aliens alike. But, according to longstanding U.S. interpretations of international law, that obligation does not apply extraterritorially.[180]

---

173. *Id.* at 18–22.

174. ICCPR, *supra* note 162, at art. 40(4).

175. The Human Rights Committee's General Comments provide States Parties with authoritative interpretations of rights protected by the ICCPR. Although not legally binding, the HRC's interpretations are considered persuasive authority. *See* CURTIS A. BRADLEY & JACK L. GOLDSMITH, FOREIGN RELATIONS LAW 315 (5th ed. 2014) ("The HRC technically has no official power to issue binding legal interpretations of the ICCPR.").

176. *Public Hearing Regarding the Surveillance Program Conducted Pursuant to Section 702 of the Foreign Intelligence Surveillance Act before the Privacy and Civil Liberties Oversight Board* 3 (2014) (statement of John Bellinger, former Legal Adviser, U.S. Department of State), *available at* https://www.pclob.gov/library/20140319-Testimony-Bellinger.pdf.

177. *Id.* at 2.

178. *Id.*

179. *Id.* at 4.

180. John Bellinger, former Legal Adviser at the U.S. Department of State under President George W. Bush, argues that the United States has taken this position consistently since 1950. *Id.* at 2. For an

As a practical matter, it is also worth noting that currently no one can obtain a legal remedy for U.S. violations of the ICCPR. Under the U.S. Constitution, treaties are the "supreme Law of the Land,"[181] but the Supreme Court has held that only self-executing treaties provide rules of decision for U.S. courts.[182] When the Senate provided its advice and consent to the ICCPR, it attached a declaration that Articles 1–27 of the treaty are not self-executing.[183] Consequently, although the treaty binds the United States as a matter of international law, state and federal courts are not bound to enforce its terms. On the international plane, the United States has not signed the Optional Protocol to the ICCPR, which extends the Human Rights Committee's powers to cover complaints by private individuals.[184] Therefore, individuals also cannot appeal alleged violations to the HRC.

Second, even if the ICCPR did apply to U.S. extraterritorial activities, surveillance does not naturally amount to "effective control" of a person. Such an interpretation seems strained. Interference with correspondence hardly amounts to effective control of a person in the same manner as physical detention. It is far from obvious that intercepting an individual's communications would render her subject to the jurisdiction of the state conducting surveillance.

Third, international human rights law was not thought to cover foreign surveillance until very recently. Snowden's unauthorized disclosures are not the first to reveal the U.S. government's spying on Western allies. As recently as 2001, a major controversy emerged over ECHELON, a signals intelligence collection program conducted by the United States and certain allies. Although the means and scope always remained unclear, under the program Anglo-American countries intercepted communications around the world, including in Europe. European leaders protested, and the European

argument that the U.S. position on the extraterritorial application of the ICCPR has not been as clear and long-standing as the government claims, see Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L. J. 301, 322–28 (2015). President Obama has maintained the U.S. government's position on the ICCPR's extraterritorial application, despite disagreement by Harold Koh, the State Department's Legal Adviser in the first Obama administration. *See* Charlie Savage, *U.S. Seems Unlikely to Accept that Rights Treaty Applies to Its Actions Abroad*, N.Y. TIMES (Mar. 7, 2014), at A6, *available at* http://www.nytimes.com/2014/03/07/world/us-seems-unlikely-to-accept-that-rights-treaty-applies-to-its-actions-abroad.html.

181. U.S. CONST. art. VI.

182. Medellin v. Texas, 552 U.S. 491 (2008); *see also* Foster v. Neilson, 27 U.S. (2 Pet.) 253 (1829).

183. U.S. Reservations, Declarations, and Understandings, International Covenant on Civil and Political Rights, 138 CONG. REC. S4781-01 (daily ed., Apr. 2, 1992). Even if the U.S. Senate had not attached a specific declaration to that effect, the U.S. Supreme Court would not have recognized the treaty as self-executing. In *Medellin*, the Court found that the language "undertakes to comply" indicated the U.S. Congress must still enact implementing legislation for a treaty to become a rule of decision in domestic courts. *Medellin,* 552 U.S. at 508. The jurisdictional clause of the ICCPR uses similar language: "each State Party to the present Covenant *undertakes to take the necessary steps,* in accordance with its constitutional processes and with the provisions of the present Covenant, to adopt such laws or other measures as may be necessary to give effect to the rights recognized in the present Covenant." ICCPR, *supra* note 162, at art. 2 (emphasis added).

184. TEMP. COMM. ON THE ECHELON INTERCEPTION SYSTEM, REPORT ON THE ECHELON INTERCEPTION SYSTEM 84 (2001).

Parliament created a special committee to investigate the program. The resulting report noted that ECHELON could conduct "quasi-total surveillance" by intercepting "any telephone, fax, Internet or e-mail message sent by any individual."[185] However, the report concluded that ECHELON did not violate existing EU law,[186] and failed to address whether the program violated the ICCPR.[187] The EU report noted that European states conducted massive surveillance programs,[188] but it did not address whether those programs violated the ICCPR, either. That the Committee investigated ECHELON thoroughly but did not study the program's compliance with the ICCPR nor EU country surveillance programs' compliance with the treaty, suggests the EU may have believed either that such espionage did not in fact violate international law or that any such violations were so pervasive as to be legally irrelevant. Moreover, given that states have practiced massive surveillance routinely under the ICCPR, the proper interpretation is that the ICCPR does not apply to such electronic surveillance. In any event, the idea that international human rights law applies to electronic surveillance appears to be of only recent vintage.

Fourth, no international law prohibits peacetime espionage. Under the *Lotus* principle, absent an explicit prohibition, sovereign states retain general freedom of action.[189] Because international law has never prohibited intelligence gathering,[190] states may engage in it freely, subject to traditional con-

185. *Id.* at 23.

186. The Committee reasoned that "activities and measures undertaken for the purposes of state security or law enforcement do not fall within the scope of the EC [European Community] treaty." *Id.* at 80.

187. *See id.* at 82–83. Although the report noted generally that "the interception of communications . . . represents a serious violation of an individual's privacy," it also emphasized that "potential violations are authorised only following analysis of the legal considerations and in accordance with the principle of proportionality." *Id.* at 83. The report failed to analyze whether ECHELON's interceptions actually violated international law. Instead, it noted simply that the Anglo-American countries had complied with HRC decisions, and that private individuals could not seek a remedy against the United States for alleged violations because the United States had not ratified the Optional Protocol to the ICCPR. *Id.* at 83–84. But a State Party to a treaty can still violate its international legal obligations even if no private remedy exists. The European Parliament failed to weigh in on that matter.

188. *Id.* at 27.

189. The Permanent Court of International Justice established the *Lotus* principle in a case involving the collision of French and Turkish steamships. The key passage reads:

> International law governs relations between independent States. The rules of law binding upon States therefore emanate from their own free will as expressed in conventions or by usages generally accepted as expressing principles of law and established in order to regulate the relations between these co-existing independent communities or with a view to the achievement of common aims. Restrictions upon the independence of States cannot be presumed.

S.S. Lotus (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7).

190. Glenn Sulmasy & John Yoo, *Counterintuitive: Intelligence Operations and International Law*, 28 MICH. J. INT'L L. 625, 637 (2007). The authors note that few scholars have questioned the legality of peacetime espionage. *Id.* at 629. *See also* David B. Silver, *Intelligence and Counterintelligence*, *in* NATIONAL SECURITY LAW 935, 965 (John Norton Moore & Robert F. Turner eds., 2d ed. 2005).

sequences outside international law, such as diplomatic expulsions, punishment of captured spies, and public denunciations.[191]

State practice underscores the legitimacy of espionage. Brazil, one of the harshest critics of U.S. spying in the wake of Snowden's revelations, had to acknowledge spying on U.S. and other foreign diplomats within its borders.[192] But other states have not confined their spying to government officials. In its report on ECHELON, the European Parliament noted that "interception of private communications by foreign intelligence services is by no means confined to the US or British foreign intelligence services."[193] Instead, the report showed that among 14 European countries, 12 spied on "communications in foreign countries," including 8 on "civilian communications."[194] Moreover, although European governments publicly denounced the U.S. surveillance programs Snowden revealed, the European Parliament has again acknowledged concerns about similarly broad surveillance programs among its member states, including France, Germany, Poland, the Netherlands, Sweden, and the United Kingdom.[195] This state practice reinforces the conclusion that international law does not generally prohibit signals intelligence activities. If "everyone does it," then customary international law cannot prohibit it. Moreover, the *tu quoque* principle may prevent victims of espionage from claiming international law violations. As a Department of Defense report on the legality of information operations concluded, "[t]he lack of strong international legal sanctions for peacetime espionage may also constitute an implicit application of the international law doctrine called '*tu quoque*' (roughly, a nation has no standing to complain about a practice in which it itself engages)."[196]

To say that U.S. signals intelligence activities do not violate international law as it currently stands does not mean that international law might not change, and this does not erase potential moral concerns. The NSA's actions—including mass surveillance and attempts to break encryption standards—may appear antithetical to U.S. efforts to protect human rights, freedom of expression, and an open and interoperable Internet.[197] Such surveillance may therefore undermine broader American foreign policy, partic-

191. *See* Dep't of Def., Office of Gen. Counsel, An Assessment of International Legal Issues in Information Operations 46 (1999) [hereinafter Information Operations], *available at* http://www.au.af.mil/au/awc/awcgate/dod-io-legal/dod-io-legal.pdf.

192. Romero, *supra* note 154.

193. Temp. Comm. on the ECHELON Interception System, *supra* note 184.

194. *Id.* at 27–29.

195. Sara Miller Llana, *After Slapping US, France Finds Itself in Spotlight for Spying*, Christian Sci. Monitor, (July 5, 2013), *available at* http://www.csmonitor.com/World/Europe/2013/0705/After-slapping-US-France-finds-itself-in-spotlight-for-spying.

196. Information Operations, *supra* note 191, at 46..

197. For instance, following Snowden's unauthorized disclosures, the Chinese government accused the U.S. government of hypocrisy in its open Internet and cyber security policies. *See* Bill Chappell, *In China, Anger at U.S. Hacking Charges—and Claims of Hypocrisy*, NPR (May 20, 2014, 7:20AM), http://www.npr.org/blogs/thetwo-way/2014/05/20/314211468/in-china-anger-at-u-s-hacking-charges-and-claims-of-hypocrisy.

ularly to represent a republic worthy of emulation—a city upon a hill. Bulk collection also raises concerns about fair play. If the United States engages in bulk surveillance abroad, then it invites other countries to spy on Americans in similar fashion. As new technologies become more prevalent, some may fear that the powers of government surveillance may approach omniscience. Assembling bulk data from credit cards, cell phone signals, voice and facial recognition, and Internet communications could offer an exceptionally detailed picture of a person's life. The U.S. government, and the American people, may not want a world where foreign governments have the capability, incentive, and apparent license to conduct such surveillance on Americans. Nevertheless, that the international law argument is not compelling may be another factor accounting for the U.S. government's decision not to extend more privacy protections to foreigners.

D. Alternative Legal and Policy Options

A lack of clearly superior alternatives also explains why the U.S. government did not extend more privacy protection to non-U.S. persons. Theoretically, a range of policy options could address the economic, diplomatic, and international legal concerns that signals intelligence activities generate. Options include: (1) abandoning bulk signals intelligence collection; (2) extending identical privacy protections to U.S. persons and non-U.S. persons; (3) maintaining the distinction and extending some of the chief privacy protections for U.S. persons to non-U.S. persons; (4) expanding existing arrangements or creating a club of countries that agrees to refrain from collecting signals intelligence on each other's nationals; and (5) requiring more extensive interagency coordination. The following section analyzes the costs and benefits of each of these policy options. This Note concludes that none of these options is clearly superior to the status quo as formalized by PPD-28.

1. *Abandoning Bulk Signals Intelligence Activities*

Theoretically, one extreme option is to abandon bulk signals intelligence collection altogether, but this option is imprudent. Available information suggests that bulk signals intelligence collection serves important national security and foreign policy goals and should not be abandoned. Bulk collection entails the collection of large amounts of data, most of which is irrelevant but, when aggregated, provides opportunities for refined analysis and identification of patterns. According to the government, bulk collection and analysis can help identify unknown threats as well as address specific knowledge gaps that other collection methods cannot provide. Caitlyn Hayden, spokesperson for the NSC, asserts that "new or emerging threats" are "often hidden within the large and complex system of modern global communications, and the United States must consequently collect signals intelligence

in bulk in certain circumstances in order to identify these threats."[198] Senator Diane Feinstein has emphasized that NSA's surveillance capabilities are crucial to countering terrorism.[199]

Other sources confirm the value of bulk signals intelligence activities in certain contexts. In PPD-28, President Obama directed the Director of National Intelligence to investigate the technical feasibility of creating software-based alternatives that would allow the IC to avoid bulk collection.[200] The resulting report, released in January 2015 by the National Research Council, concluded that no such alternatives could provide a complete substitute for bulk collection to detect some national security threats.[201] The report emphasized that "[i]n contrast to domestic law enforcement . . . the world of intelligence analysis has many fewer tools available for investigation. In hostile foreign environments, personal interviews and observations and records review are much more limited. Accordingly, the role of bulk data as a way to understand the significance of past events is important . . . ."[202] In fact, "[f]or investigations that have little or no prior targeting history, bulk collection may be the only source of useful information."[203]

It is important to emphasize that bulk collection does not simply help detect and thwart terrorist attacks; it also plays an important role in informing the U.S. government's other national security and foreign policy goals and strategies. Although PCLOB concluded that the U.S. government's domestic bulk telephone metadata program conducted under section 215 "has shown only limited value" and recommended that it be terminated,[204] bulk signals intelligence collection abroad can prove extremely useful for foreign intelligence purposes. The National Research Council's unclassified report cited certain contexts in which bulk collection may prove especially useful for strategic intelligence. For instance, monitoring a range of communications can reveal statistical patterns on agricultural production, electric power supply, health care conditions, or migration patterns that a foreign government may report inaccurately or not at all.[205] Further, sampling everyday communications, including social media, can help the government under-

198. Barton Gellman & Ashkan Soltani, *NSA Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 18, 2014), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html.

199. Ryan Lizza, *State of Deception*, NEW YORKER (Dec. 16, 2013), *available at* http://www.newyorker.com/magazine/2013/12/16/state-of-deception. ("'It is very difficult to permeate the vast number of terrorist groups that now loosely associate themselves with Al Qaeda or Al Nusra or any other group. It is very difficult, because of language and culture and dialect, to really use human intelligence. This really leaves us with electronic intelligence.'") (quoting Senator Feinstein).

200. PPD-28 § 5(d).

201. TECHNICAL OPTIONS, *supra* note 43, S-6.

202. *Id.* at 4-1.

203. *Id.* at 3-8.

204. PCLOB 215, *supra* note 2, at 16.

205. TECHNICAL OPTIONS, *supra* note 43, at 4-2.

stand local reactions to political trends that might result in a change in government, violent or otherwise.[206] While none of these purposes necessarily involves a direct threat to life, policymakers have a legitimate interest in gathering this foreign intelligence to advance American interests. Abandoning bulk signals intelligence collection of non-U.S. persons would therefore frustrate valid national security and foreign policy goals.

2. *Abolishing the U.S. Person Distinction and Extending Identical Privacy Protections*

While the U.S. government could, in theory, abolish the distinction between U.S. persons and non-U.S. persons, that policy would prove unwise. Extending identical protections to non-U.S. persons threatens to compromise national security and the effective conduct of foreign affairs, would lower the protections U.S. persons currently enjoy, and may encounter political opposition.

Would eliminating the distinction compromise national security? On one view, foreigners do not necessarily cause more harm to the United States than U.S. persons. Domestic terrorists and criminal gangs can, depending on the circumstances, pose a greater threat to Americans than foreign spies and terrorists. Moreover, according to the government the unauthorized disclosure of classified documents by U.S. persons has also caused great damage to U.S. national security.[207] Under this view, one might argue that if the government directed more resources against domestic threats, it could prevent more harm to Americans.

This argument misses several key points, however. First, the IC operates under the assumption that a person's non-U.S. person status predicts a higher *likelihood and severity* of potential harm to Americans. While this assumption may be difficult to verify and such an assessment lies outside the scope of this Note, the logic is as follows. Non-U.S. persons have not developed ties of allegiance to the United States. They may take advantage of safe havens where they can plan and execute terrorist attacks. Because they operate outside the United States and its law enforcement system, the government generally has fewer opportunities to gather information on them. They may have greater resources, training, equipment, and perhaps even backing from a hostile state. Foreign militaries, spies, terrorists, and other hostile forces are therefore thought more willing and capable to inflict grievous harm than domestic terrorists. The attacks on September 11, 2001, resulted in higher casualties than all previous terrorist incidents in the United States

206. *Id.*

207. For example, Keith Alexander, Director of the NSA, noted that Edward Snowden's disclosures caused "irreversible and significant damage," and an internal investigation is said to confirm this assessment. Tom Gjelten, *The Effects of the Snowden Leaks Aren't What He Intended*, NPR (Sept. 20, 2013, 4:34 PM), http://www.npr.org/2013/09/20/224423159/the-effects-of-the-snowden-leaks-arent-what-he-intended.

combined.[208] The logic also assumes that among the people who are opposed to the United States, more of them live abroad than within the country. It follows that the threat is greater overseas.

Second, the government does not collect foreign intelligence information merely to thwart international terrorist or other hostile attacks. The government also collects information to generate knowledge and seize opportunities for foreign affairs purposes, such as preparing for trade negotiations and assessing economic trends in foreign countries.

Third, by enacting FISA the Congress determined that foreign intelligence collection in the domestic context presents a special danger to U.S. democratic institutions. The risk of politically motivated targeting and other abuses rises when the government directs its powerful tools of foreign surveillance inward.[209] A government's surveillance against its own people is particularly dangerous because the government can deprive liberty or allocate benefits and burdens based on what it knows about a person's private life. Surveillance also risks chilling freedom of expression and association, as persons change their behavior in order to avoid these risks. Because most foreigners are not subject to U.S. jurisdiction, government surveillance of foreigners generally poses fewer risks. To be sure, signals intelligence collection on foreigners could chill freedom of expression abroad, as foreigners change their communication behaviors in an attempt to avoid U.S. surveillance. Given international commerce, such a chilling effect abroad could negatively impact U.S. economic interests, as foreigners restrict the scope of their creative activities. But these chilling effects are speculative and any effect would be smaller than in the domestic context. Therefore, even though some may argue that the government could possibly save more American lives by directing its surveillance powers inward, the cost to democratic institutions would prove too high. Overall, the U.S. person distinction serves an important purpose.

Eliminating the distinction would also threaten to lower the protections U.S. persons already enjoy. Under the current legal framework, providing identical protections to U.S. persons and non-U.S. persons would effectively prevent bulk signals intelligence collection outside of the United States altogether. Sections 703 and 704 of the FAA restrict the targeting of U.S. persons outside the United States, a category of foreign intelligence previously outside the scope of FISA. Under both sections, the FISC must find probable

208. *Current and Projected National Security Threats to the United States: Hearing Before the S. Select Comm. on Intelligence*, 107th Cong. 89 (2002) (statement of Dale L. Watson, Executive Assistant Director, FBI).

209. The *Keith* court emphasized that a government's surveillance against its own citizens is dangerous because the government can use perceived threats to domestic security as a justification for suppressing political dissent. United States v. U.S. District Court (*Keith*), 407 U.S. 297, 314 (1972) ("Fourth Amendment protections become the more necessary when the targets of official surveillance may be those suspected of unorthodoxy in their political beliefs. The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect 'domestic security.'")

cause that the target is reasonably believed to be located outside the United States, and probable cause that the target is a foreign power, an agent of a foreign power, or an officer or employee of a foreign power. If non-U.S. persons were afforded the same protections as U.S. persons—in other words if the scheme "leveled up" protections for non-U.S. persons—then all collection on foreigners outside the United States would need to follow section 703 and 704 prescriptions. Because these provisions require an individualized showing of probable cause, the government would need to make individual applications for FISC warrants, thereby preventing bulk collection. Faced with this prospect, the government would either need to cancel bulk signals intelligence collection programs or alter the legal standard, which would effectively water down the predicate for U.S. persons.

The above analysis outlines the costs involved in abandoning the distinction, but other considerations are noteworthy, too. At present, political considerations probably push against abolishing the distinction. An American president considering extending privacy protections to foreigners may need to convince a skeptical public that increased protections for non-U.S. persons would not expose the United States to greater threat. The American public may also wonder why the U.S. government should extend protections to foreigners if no other country has so far been willing to do the same.[210] Few if any countries protect non-citizens in signals intelligence collection abroad. Indeed, as Justice Powell has noted, "[i]t would be contrary to the public interest for Government to deny itself the prudent and lawful employment of those very techniques which are employed against the Government and its lawabiding [sic] citizens."[211] It is worth noting that the constituencies most likely to favor eliminating the distinction—illegal aliens and lawfully admitted aliens on student or other temporary visas in the United States, as well as foreigners outside the United States—have limited political power within the United States. Perhaps for this reason, Congress has never publicly debated altering the standards for non-U.S. persons.[212] Foreigners do have some leverage, however. For instance, if citizens in Italy or Germany grew sufficiently upset about U.S. signals intelligence activities, those countries could withdraw support for U.S. naval and other military installations. Those bases are crucial to U.S. force projection around the world. Because the U.S. government depends on cooperative relationships with other countries to achieve its national security and interests, strong objections from key partners could prompt more serious consideration of this issue. Absent a change in circumstances, however, the political

210. In fact, other countries do not draw distinctions among citizens and non-citizens. For instance, the United Kingdom's laws regulating surveillance do not draw a distinction based on nationality. *See* Regulation of Investigatory Powers Act, c. 23, 2000 (U.K.); Anti-terrorism, Crime and Security Act, c. 24, 2001 (U.K.).

211. *Keith*, 407 U.S. at 312.

212. KRIS & WILSON, *supra* note 10, § 8:44.

climate in the United States will likely not prompt active consideration of any changes to the protections for non-U.S. persons.

An understanding of the U.S. government's legal scheme in comparative perspective is also noteworthy, though not decisive to the appropriate policy choice. Available evidence suggests that with section 702 the United States already offers more transparency and more protections to foreigners than most other countries.[213] While it may come as little surprise that China "maintains almost unlimited and unfettered access to private sector data"[214] collected both domestically and abroad, France and the United Kingdom both conduct broad surveillance under laws that do not require prior judicial approval and that allow collection not only for counterterrorism but also to advance economic interests, a justification lacking under FISA.[215] With section 702, Congress extended judicial oversight to a category of surveillance that it had previously left outside judicial supervision. This requirement goes beyond what many other intelligence agencies require when they collect against persons who are not their nationals. According to one study of thirteen countries, eight governments—Australia, Canada, China, France, Germany, India, Israel, and the United Kingdom—do not require a court order for foreign intelligence surveillance.[216] Under the U.S. scheme, judicial oversight does not apply to surveillance conducted pursuant to Executive Order 12333 (an admittedly large exception), but many other countries do not require a court order under any scenario. Of course, lack of reciprocity should not preclude appropriate action. That the United States provides more protections to foreigners than other countries does not mean the U.S. policy is adequate or correct. Given the American commitment to personal liberty and the fact that American surveillance capabilities far surpass those of other countries, the United States may have a heightened obligation to provide more transparency, if not more privacy protections. Moreover, a country may decide to do the right thing unilaterally, for instance, by refraining from torturing or using chemical weapons. Nevertheless, the public

213. *See* Winston Maxwell & Christopher Wolf, Hogan Lovells, A Sober Look at National Security Access to Data in the Cloud: Analyzing the Extravagant Claims About U.S. Access that Ignore Access by Foreign Jurisdictions 5 (2014) (arguing that "Section 1881a [section 702] imposes at least as much, if not more, due process and oversight on foreign intelligence surveillance than other countries afford in similar circumstances").

214. Ira S. Rubenstein et al., *Systematic Government Access to Personal Data: A Comparative Analysis*, 4 Int'l Data Privacy Law 96, 98 (2014).

215. In France, Article L 241-2 of the Internal Security Code provides authorization to conduct "broad, untargeted, random monitoring of radio traffic" for "defense of national interests," as well as to protect France's "economic and scientific potential." Christopher Wolf, Hogan Lovells, An Analysis of Service Provider Transparency Reports on Government Request for Data 1 n.3 (2013); Maxwell & Wolf, *supra* note 213, at 8. The United Kingdom conducts surveillance pursuant to the Regulation of Investigatory Powers Act ("RIPA"), which grants the Foreign Secretary the authority to issue warrants "for the purpose of safeguarding the economic wellbeing of the United Kingdom." Rubenstein et al., *supra* note 214, at 102.

216. *See* Ctr. for Democracy & Tech., *Comparative Study of Standards for Government Access: National Security*, *available at* http://govaccess.cdt.info/standards-ns-country.php (last visited Nov. 12, 2014). Of the countries studied, Brazil, Italy, Japan, and Korea require a court order.

may question a policy that, on its face, risks compromising national security. And unilaterally restricting signals intelligence activities denies the possibility of bargaining with other countries over such collection in the future.[217] Overall, extending identical protections to non-U.S. persons threatens to compromise national security and the effective conduct of foreign policy, would lower the protections U.S. persons currently enjoy, and may encounter political opposition. Such a policy is, on balance, inadvisable.

3. *Maintaining the U.S. Person Distinction and Extending Some Key Protections to Non-U.S. Persons*

U.S. law and policy currently provide four main protections to U.S. persons: (1) restrictions on what kinds of information may be collected; (2) restrictions on what information may be retained and for how long; (3) restrictions on what information may be disseminated; (4) oversight mechanisms; and (5) legal remedies under the Privacy Act. What would happen if the United States extended some of those protections to Europeans, for instance? The analysis below suggests that providing such protections would involve significant administrative costs and potential harm to national security.

Collection. Section 702 and Executive Order 12333 do not impose substantial limits on the types of information the government can collect. Both authorities enumerate certain categories of foreign intelligence information (such as international terrorism, weapons of mass destruction, and espionage), but they also include broader categories (such as the conduct of foreign affairs). These categories, as well as the National Intelligence Priorities Framework, already apply to collection against non-U.S. persons, however. Executive Order 12333 provides that the government must use the "least intrusive" means when collecting on U.S. persons. Applying this rule to collecting against non-U.S. persons would benefit foreigners, but at probably a large cost to efficient collection. Intelligence collection inevitably entails breaking foreign laws. To require the IC to use publicly available sources before turning to investigative techniques that require a warrant would impede efficiency.

It is also worth noting that creating a rule that restricts collection to certain categories of targets or sources would prove difficult to implement. Signals intelligence activities range from activities whose legitimacy no one questions—such as collection on hostile forces to support tactical battlefield operations—to activities that may seem unnecessary and unwarranted—say, collection on French high school students. Perhaps the IC could extend the protections to certain classes of persons assessed to pose a low threat, and no terrorist attack would succeed. Then again, perhaps not. Even a country friendly to the United States, like France, contains nationals who would do

217. Similarly, this is one reason states may hesitate to voluntarily give up nuclear weapons programs.

the United States harm. In an ideal world, the government would not collect on segments of the population or modes of communication that never yield information of value. But if a rule prohibited collecting on particular targets, there is no guarantee that a risk would not materialize there. And if a rule prohibited collection on certain types of communications, one could imagine nefarious actors starting to use such communication channels. Intelligence agencies need flexibility in order to anticipate and adapt to new threats and communications platforms. This is not to say that the government should not tailor its signals intelligence collection to the extent feasible. Doing so saves resources and focuses collection efforts. However, a rule that narrows collection absolutely seems untenable in practice.

Retention. The main restriction on retention is that information with no foreign intelligence value must be purged no later than five years from collection. A commitment to purge irrelevant information would theoretically benefit foreigners who do not want the government to retain highly personal or embarrassing information about them. And if the data is irrelevant, then the government loses nothing if it purges the data. However, limiting retention would be unlikely to satisfy foreigners who worry more about the collection of information in the first instance. Such a policy then would provide little value. Even if limits on retention were seen as valuable, it would prove difficult to implement. When reviewing intelligence, analysts often find it difficult to assess whether a given piece of information has foreign intelligence value. In order to justify purging a piece of information, an NSA analyst must determine not only that the piece of information has no present foreign intelligence value to her, but also that such intelligence would not offer valuable information to any present or future foreign intelligence need.[218] Valuable information might be lost. Five years might not afford a sufficient period of time for the data to be exploited, as the IC might wish to use the data for assessing patterns over longer time periods. Moreover, a rule that requires purging information of no value could impose a high administrative cost, not to mention privacy cost, as analysts would be required to examine information that would have gone untouched. The increased costs could be time-bound; if the government imposed retention standards, it could spur the IC to invest in technologies to filter and purge information automatically. However, the viability of such solutions remains unknown. Therefore, absent a viable technological solution, additional retention requirements would likely impose significant administrative cost and could result in loss of valuable information. For some or all of these reasons, the five-year destruction requirement announced in the Signals Intelligence Reform 2015 Anniversary Report includes significant exceptions.

Dissemination. The chief privacy protections with regard to dissemination are twofold. First, identifying information can only be disseminated if it is

218. *See* PCLOB 702, *supra* note 2, at 62.

necessary to understand the value of the foreign intelligence. Second, generic phrases must be substituted so as not to identify U.S. persons. As applied to non-U.S. persons, the purported benefits of these measures would be to ensure that personal information is redacted and viewed only by those officials with a need to know. While these prescriptions seem reasonable, in practice they would entail significant costs. Policymakers often need to know names, places, and other identifiers in order to assess foreign intelligence information. If an agency must use a vague identifier, such as "SOMALI PERSON 1," before it shares that information with another agency, it could turn intelligence sharing into a guessing game. The dissemination protections therefore also entail nontrivial cost.

Oversight. Another option would be to pass legislation that places all signals collection programs (not only the one authorized in section 702) under the FISA framework. In general, FISA does not cover surveillance conducted outside of the United States.[219] In theory, a congressional debate and vote to bring more programs under FISA would ensure the public weighs the costs and benefits of the programs. Having the FISC sign off on programs—even if through broad certifications, such as the section 702 certifications that do not specify facilities or targets—would also lend a judicial imprimatur of legitimacy to the programs. In addition, reporting statistics on U.S. intelligence gathering abroad could bolster confidence that the U.S. government does not engage in indiscriminate mass surveillance.

The costs of judicial supervision and statistical reporting for signals intelligence collection programs may prove prohibitive, however. First, the rationale for including the PRISM program under FISA likely does not apply to other programs. Section 702 is a unique program that requires the compelled assistance of U.S. telecommunications and Internet service providers to target foreigners.[220] When the government cooperates with domestic businesses to conduct surveillance, the risk of abuse and threat to democratic institutions increases. Such adverse consequences are not present when the government targets foreign powers, companies, or persons.

Second, a public debate about bringing sensitive signals intelligence collection programs under FISA would likely require disclosure of some details of the programs. Disclosure of sensitive sources and methods could harm national security. Meanwhile, disclosure of general statistics on surveillance targets would seem to do little to reassure allies and international partners, but could tip off foreign governments or terrorist groups as to how much the U.S. government knows about their activities. When the privacy rights

219. The exceptions are where the government intentionally targets a particular, known U.S. person or where the surveillance acquires radio communications in which the sender and all intended recipients are located outside the United States and a warrant would be required in a law enforcement context. 50 U.S.C. §§ 1801(f), 1881c.

220. *See id.* § 1881a(g)(2)(A)(vi).

of U.S. persons are not at issue, and the national security interests are strong, the need for transparency is substantially lower.

Third, bringing more programs under the FISA framework raises a potential constitutional objection. A full treatment of the constitutional question remains outside the scope of this Note. However, it is worth noting that the President and Congress share war powers and some foreign affairs responsibilities. On the one hand, enacting legislation that sets standards for executive action appears to be well within Congress's Article I powers. On the other hand, the President has expertise in conducting foreign affairs and needs discretion to exercise his Article II powers effectively.[221] When the President directs foreign surveillance, he does so pursuant to his powers as Commander in Chief and head of the Executive Branch. Conducting foreign surveillance to understand the capabilities, plans, and intentions of foreign actors and threats to the United States falls squarely within those powers. For Congress to inject statutory constraints on those powers or impose judicial oversight would alter the distribution of foreign affairs powers between the President and the Congress, thereby raising a potential constitutional problem.

Fourth, it remains unclear whether FISA would provide any meaningful additional oversight in the context of foreign intelligence collection against foreigners abroad. Each intelligence agency already has an inspector general that reports directly to Congress. While certain violations have occurred with respect to the communications of foreigners, one source estimates that only a handful occurred over the last decade.[222] Moreover, most of those violations were self-reported, and each one resulted in termination of the employee.[223] But whether or not the current oversight system is sufficient, it is unclear that extending additional judicial oversight would allay the concerns of foreigners. According to one legal expert on the technology industry, foreign firms now cite the PATRIOT Act as a reason to switch away from American products, even though that legislation has little to do with current signals intelligence collection conducted overseas.[224]

The Privacy Act of 1974. With regard to surveillance of non-U.S. persons, the President's Review Group recommended extending the Department of Homeland Security's ("DHS") policy that applies the Privacy Act of 1974 in the same manner to both U.S. persons and non-U.S. persons.[225] In prac-

221. As the Fourth Circuit has noted, "the executive branch not only has superior expertise in the area of foreign intelligence, it is also constitutionally designated as the pre-eminent authority in foreign affairs." United States v. Truong Dinh Hung, 629 F.2d 908, 914 (4th Cir. 1980).

222. Andrea Peterson, *LOVEINT: When NSA Officers Use Spying Power on Love Interests*, WASH. POST (Aug. 24, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/08/24/loveint-when-nsa-officers-use-their-spying-power-on-love-interests/. One reason for this low figure may be that, because Congress cares less about the rights of non-U.S. persons, the inspectors general focus less attention on such complaints.

223. *Id.*

224. Telephone Interview with Bret Cohen, Associate, Hogan Lovells LLP (Oct. 29, 2014).

225. PRG, *supra* note 2, at 157.

tice, however, that recommendation may turn out not to provide much recourse to non-U.S. persons. The Privacy Act regulates the federal government's collection, use, and disclosure of personal data.[226] The Act criminalizes the disclosure of personally identifiable information.[227] Intended as a protection against the state exercising its coercive power based on faulty information, the Act also provides individuals a right—enforceable in federal court—of access to personal data held by a federal agency and to petition for correction of data that is not accurate, relevant, timely, or complete.[228] In the context of surveillance for foreign intelligence purposes, the Privacy Act provides little aid to individuals concerned about the government's control of their personal data. The Privacy Act includes numerous exemptions, including for records relating to national defense or foreign policy,[229] and for those maintained by the Central Intelligence Agency and law enforcement agencies.[230] Moreover, the Privacy Act includes specific definitions that courts have interpreted narrowly, such that personal data held by the government may not qualify for the Act's protections.[231] If other federal agencies adopted the DHS policy, a non-U.S. person would receive notice of the system of records and the intended use of the personally identifiable information, but the policy does not extend the jurisdiction of federal courts to hear disputes of non-U.S. persons against DHS for failure to amend personal records.[232] The Director of National Intelligence is working with Members of Congress on legislation to extend judicial remedies for violations of the Privacy Act to persons of certain countries designated by the Attorney General, in concurrence with the Secretaries of State, Treasury, and Homeland Security.[233] Even if it passes, such legislation may not provide much aid to non-U.S. persons seeking to protect their privacy in practice. The draft legislation would restrict the civil remedies available to covered non-U.S. persons to only a government agency's willful and intentional disclosures of personal data; covered non-U.S. persons would not have a remedy for damages for an agency's refusal to make records available or for failing to amend personal data.[234]

While the Review Group's Recommendation and the DNI's work with members of Congress may not provide substantial additional privacy protec-

226. 5 U.S.C. § 552a (1974).

227. *Id.* § 552a(l).

228. *Id.* § 552a(d).

229. *Id.* §552a(k)(1).

230. *Id.* §552a(j).

231. For an assessment of these and other limitation of the Privacy Act as applied to national security records, see Francesca Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. Rev. 609, 631–35 (2007).

232. *See* Hugo Teufel III, *An Explanation of the DHS Privacy Policy Behind Review Group Recommendation #14*, Lawfare (Jan. 8, 2014, 11:47 AM), http://www.lawfareblog.com/2014/01/an-explanation-of-the-dhs-privacy-policy-behind-review-group-recommendation-14/.

233. *Signals Intelligence Reform: 2015 Anniversary Report*, *supra* note 124; H.R. 1428, 114th Cong. (2015).

234. H.R. 1428, 114th Cong. § 2(a)–(b) (2015).

tions for non-U.S. persons, these approaches might have symbolic benefits. The Privacy Act's provisions, however limited, would apply to U.S. persons and non-U.S. persons alike, responding to calls for change. Still, because the Privacy Act's enforcement provisions pertain to the handling and disclosure—but not the collection—of personal information, the government could still collect far more information on non-U.S. persons than U.S. persons.

While the current legal and policy framework may strip non-U.S. persons of more privacy protection than necessary, given the potential and actual costs involved, extending privacy protections to non-U.S. persons does not appear to offer a clearly superior policy approach.

4. *Restricting Signals Intelligence Activities Through Multilateral Agreement*

Proposals to extend surveillance cooperation agreements are unlikely to be implemented to an extent sufficient to reassure key allies. One arrangement is called the Five Eyes. The Five Eyes refers to the agreement between the United States, the United Kingdom, Canada, Australia, and New Zealand to share signals intelligence information. The Five Eyes originated with the British–U.S. Communication Intelligence Agreement of March 5, 1946.[235] While the full scope of the Five Eyes agreement remains classified, available evidence suggests that the agreement combines signals intelligence information sharing with an agreement to refrain from conducting surveillance on each other's citizens.[236] The Five Eyes agreement provides significant benefits. Surveillance cooperation builds trust among allies. It is also efficient, as the United States can complement its capabilities with partner country assets. The United States also need not spend resources collecting on British or other "second party" nationals.

In practice, the number and scope of such agreements will likely remain limited for several reasons. First, the Five Eyes agreement is predicated on trust built over time, which would prove difficult to replicate. Many factors contribute to that trust. The Five Eyes share the same cultural and linguistic

235. British–U.S. Communication Intelligence Agreement, U.S.–U.K., Mar. 5, 1946, *available at* http://discovery.nationalarchives.gov.uk/details/r/C11536914#imageViewerLink.

236. The original U.S.–U.K. agreement does not include a prohibition on spying on each other's citizens. Instead, the parties agree to "unrestricted" exchange of intelligence products relating to "foreign communications," including "collection of traffic," "acquisition of communication documents and equipment," "traffic analysis," "cryptoanalysis," "decryption and translation," and "acquisition of information regarding communication organizations, practices, procedures, and equipment." *Id.* at art. 3. However, a recently declassified NSA document reveals that the NSA's Signals Intelligence Directorate (SID) treats persons from the Five Eyes the same as U.S. persons at all phases of intelligence gathering and processing. Nat'l Sec. Agency, Overview of Signals Intelligence (SIGINT) Activities 11 (2007), *available at* https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf ("As a matter of SID policy, and in accordance with agreements between the NSA and Second Party partners, Second Party persons—those from Australia, Canada, New Zealand, and Great Britain—are generally treated like U.S. persons to the extent consistent with our national security interests. This applies to collection and targeting, processing, dissemination, and retention of communications of or about Second Party persons.").

roots, as well as the tradition of the common law. They also fought alongside each other in World War II and other more recent military missions. The United States and its four partners do not share many of these attributes with France or Germany, the countries recently put forward as possible new partners. Moreover, France, Germany, Israel, and other close allies and partners spy on the United States.[237]

Second, the United States is unlikely to want to give up valuable intelligence information derived from allies. Spying on allies is more complex than is generally understood. U.S. allies have relationships with other countries, and those relationships sometimes implicate U.S. national security. The U.S. government has a legitimate interest in understanding those relationships. For instance, reports indicate that the German Foreign Ministry and Germany's central bank helped finance Iranian nuclear and missile programs, circumventing U.S.–EU sanctions to which Germany committed.[238] If certain officials in the German government are lax in enforcing sanctions against Iran the U.S. government has a legitimate interest in understanding how high up in the German government that attitude runs.

One might argue that governments will always spy on each other, and the real concern lies in spying on ordinary citizens in foreign countries. Under this line of argument, the U.S. government should not collect the communications of European nationals. These citizens live and participate in democracies committed to the rule of law, and they should enjoy greater privacy protections. Instead of extending the Five Eyes agreement on exchange of information, another option then would be to create a non-proliferation treaty on mass surveillance. The treaty would create a club of countries. Under the treaty, each government would agree to collect on another country's citizens only when meeting the same standards and procedures the target country affords its own citizens. For example, if France passed a signals intelligence law requiring probable cause to believe the target is a terrorist or spy, the NSA could not spy on French citizens unless it satisfied that standard. Such a system would have the benefit of encouraging countries to adopt more rigorous privacy protections. The agreement would pertain to democratic countries committed to the rule of law, not authoritarian regimes. Since the agreement would focus on prohibiting surveillance, it would also ease worries that intelligence sharing agreements among governments may create a system of pervasive surveillance worldwide.

Like the Five Eyes agreement, however, a club of democratic countries approach is unlikely to succeed for several reasons. First, the United States

237. *See, e.g.*, Adam Taylor, *Allies Spy on Allies All the Time. Did Israel Do Something Worse?*, WASH. POST (Mar. 24, 2015) http://www.washingtonpost.com/blogs/worldviews/wp/2015/03/24/allies-spy-on-allies-all-the-time-did-israel-do-something-worse/.

238. Benjamin Weithal, *Why Has Germany Snubbed Obama over Iran Sanctions?*, FOUND. FOR DEF. OF DEMOCRACIES (Mar. 28, 2015), *available at* http://www.defenddemocracy.org/media-hit/why-has-germany-snubbed-obama-over-iran-sanctions1/ (last visited Apr. 11, 2015).

would likely be unwilling to count on other countries to mitigate threats. The United States may wish to monitor certain German or French nationals (or persons within those jurisdictions) because it suspects such persons sympathize with violent extremism. Bulk signals intelligence collection may be the best way to detect and monitor such persons. Even if the United States and the members of the club of countries agreed on the targets and the purposes of surveillance, the United States might be unwilling to participate since, compared to the NSA's capabilities, other countries' capabilities may be substantially lower. Second, beyond protecting against threats, the United States may gather valuable intelligence information from foreign citizens, even citizens of allies. The purpose of foreign intelligence gathering is not merely to thwart attack but also to understand the capabilities, plans, and intentions of foreign powers. Executive Order 12333 is instructive: "Timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents, is essential to the national security of the United States."[239] This is a broad and important mandate. An agreement that prevents, or even substantially limits, such foreign intelligence collection is unlikely to succeed.

5. *Increasing Oversight Through Interagency Coordination*

A policy that requires greater interagency coordination seems most feasible and could better advance the overall national interest. If diplomatic irritation and economic cost to American companies represent two of the main harms generated by bulk or perceived indiscriminate signals intelligence collection, then it seems appropriate to require intelligence agencies to consult or at least inform the Secretary of State and Secretary of Commerce before implementing new signals intelligence activities. Both Departments provide important perspectives to inform the overall national interest. The Department of State provides policy expertise on foreign affairs and could inform the IC of the diplomatic consequences of signals intelligence activities. The Department of Commerce's mission is to assist American businesses to promote job creation and economic growth. Both departments also provide unique and relevant expertise with regard to the Internet. The State Department's Office of International Communications and Information Policy owns the "Internet Freedom" agenda. The Commerce Department's National Institute of Standards and Technology has established encryption standards, and its National Telecommunications and Information Administration facilitates the functioning of the Internet's Domain Name System. Requiring high-level coordination with these agencies would ensure that, before it engages in signals intelligence collection, the IC would be sufficiently informed of the views of other components that may hold different assessments of the national interest.

239. Exec. Order No. 12333, *supra* note 13, pmbl.

To be sure, this proposal has potential downsides. To be practical, such coordination would need to be delegable to the Deputy Secretary in each Department, and possibly an Undersecretary. As with any intelligence activity, the likelihood of operations being compromised increases as the number of people involved increases. This coordination could prove redundant, too. The National Intelligence Priorities Framework—the document that guides resource allocation in collecting and analyzing foreign intelligence information—already includes an interagency process at the NSC.[240] Without knowing details about the NSC coordination process, it remains unclear how much value this policy would provide. If current NSC coordination focuses mainly on setting intelligence collection priorities, then a process that affords heads of departments and agencies the opportunity to challenge the IC to ensure that the benefits of such programs justify the costs could prove useful. While this solution may ensure interagency coordination and send a message to allies and foreign partners that the U.S. government takes their concerns seriously, at the end of the day it represents a modest change to current policy. The Coordinator for International Diplomacy created under PPD-28 moves in this direction, but the directive does not specify reporting lines and policymaking procedures that would ensure this official has sufficient authority to change practices where necessary.

Another possible mechanism for encouraging interagency coordination would be to require a signals intelligence program privacy impact statement. The statement could be modeled after environmental impact statements, which provide a discussion of significant environmental impacts and reasonable alternatives. Instead of making the statement open for public comment, however, a privacy impact statement would solicit input from within the IC and from select departments, including State and Commerce. Section 3 of PPD-28 provides that the heads of agencies that participate in the policy processes for establishing signals intelligence priorities and requirements will review annually those priorities and requirements.[241] But this provision does not require the agencies to weigh the costs and benefits of the programs themselves. By reducing to writing the costs and benefits, such a statement could force the IC to actively consider the economic and diplomatic costs of intelligence activities. The statement could have significant downsides, however. If a privacy impact statement were required for individual programs, it could stifle innovation. Because signals intelligence activities necessarily involve invasions of privacy, an analyst might hesitate to propose a new collection technique if the value of the information derived, though possibly highly valuable, is still speculative. In order to avoid stifling innovation, then, a privacy impact statement might best consider programs in the aggregate.

240. ICD 204, *supra* note 100.
241. PPD-28 § 3.

Conclusion

This Note sought to explain an apparent puzzle in U.S. government policy. Following Snowden's unauthorized disclosures of sensitive documents on U.S. surveillance practices, including mass surveillance on foreigners abroad, international pressure mounted for the U.S. government to reform its intelligence activities. Yet in the face of apparently high economic and diplomatic costs, the U.S. government extended few tangible privacy protections to foreigners. In fact, as this Note argues, the President's response in PPD-28 largely formalizes current practice within the U.S. Intelligence Community. This Note offered several possible explanations for this puzzle. The government may discount the economic costs because they may be exaggerated. The diplomatic costs have already begun to decline. The international human rights law argument is not compelling, and no international law prohibits peacetime espionage. Finally, no alternative policy options are clearly superior to the status quo.

At this stage, the U.S. government has chosen a policy that maintains the status quo, while tinkering at the edges. Ultimately, perhaps the greatest change to come from PPD-28 is a public acknowledgement that foreigners have a legitimate privacy interest. The directive states that when conducting U.S. signals intelligence activities, the U.S. government "must take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."[242] While even this pronouncement is limited—since it applies only to the *handling* of information, not its *collection*—still, the statement opens the door for further oversight and reform. The Privacy and Civil Liberties Oversight Board will also weigh in on the matter. Although the agency deferred consideration of the treatment of non-U.S. persons,[243] it has slated the issue for its short-term agenda.[244] PPD-28 itself leaves room for more reform. Such reform is not unprecedented. When enacted in 1978, FISA regulated only electronic surveillance; Congress later expanded the scope of FISA to apply to physical searches within the United States,[245] and then to activities conducted outside the United States.[246] PPD-28's public recognition of all individuals' legitimate privacy interests is also important because it changes the debate from *whether* non-U.S. persons should receive privacy protections to *how many* they should receive. While such changes may afford greater protections to non-U.S. persons, they may not necessarily have a salutary effect. For instance, additional protections for non-U.S. persons

242. PPD-28 pmbl.

243. *See* PCLOB 702, *supra* note 2, at 9, 98–102.

244. Privacy and Civil Liberties Oversight Bd., *PCLOB Announces Its Short-term Agenda* (Sept. 3, 2014), https://www.pclob.gov/newsroom/20140807.html.

245. *See* Kris & Wilson, *supra* note 10, § 3:8.

246. *See id.* § 17.

could reduce protections for U.S. persons, since restricting review of non-U.S. person data conserves resources for more intensive review of U.S. person data.[247] In addition, more oversight will not necessarily prove beneficial for an organization with large but finite resources. Former NSA General Counsel Stewart Baker has emphasized that the FISC, inspectors general, and other current oversight mechanisms have a large impact on NSA's performance. He warns that, "[a]rguably, existing oversight mechanisms have already led NSA to protect privacy better than it protects national security. Adding more oversight, as Congress seems inclined to do, will shift NSA's priorities further in the same direction. At some point, I fear, that will lead to a serious national security failure."[248] While PPD-28 largely reflects current practice, it could create room for further expansions in the future. Policymakers will want to weigh these options carefully. In an age of rapid technological change, balancing privacy and national security admits of no easy solutions.

247. *See id.* § 8:44.

248. Jack Goldsmith, *Reflections on NSA Oversight, and a Prediction That NSA Authorities (and Oversight, and Transparency) Will Expand*, LAWFARE (Aug. 9, 2013, 7:52 AM) (quoting Stewart Baker), http://www.lawfareblog.com/2013/08/reflections-on-nsa-oversight-and-a-prediction-that-nsa-authorities-and-oversight-and-transparency-will-expand/.