Catholic University Law Review

Volume 69
Issue 1 *Winter 2020*

Article 8

5-22-2020

Adapting U.S. Electronic Surveillance Laws, Policies, and Practices to Reflect Impending Technological Developments

Eric Manpearl

Adapting U.S. Electronic Surveillance Laws, Policies, and Practices to Reflect Impending Technological Developments

Cover Page Footnote

Law Clerk to the Honorable John M. Rogers of the United States Court of Appeals for the Sixth Circuit. J.D. 2018, The University of Texas School of Law; Master of Public Affairs 2018, Lyndon B. Johnson School of Public Affairs; B.A. 2013, Rice University. Eric Manpearl clerked for the Honorable Royce C. Lamberth of the United States District Court for the District of Columbia and was previously the Brumley Next Generation Senior Graduate Fellow in the Intelligence Studies Project at the Robert S. Strauss Center for International Security and Law. Special thanks to Professors Robert Chesney, William Inboden, and Steve Slick for their thoughtful and invaluable suggestions, guidance, and advice. Also, thank you to Elisebeth B. Collins, Carrie F. Cordero, Michael Daniel, Laura Donohue, Timothy Edgar, Eric Greenwald, David S. Kris, Robert S. Litt, Benjamin A. Powell, Matt Tait, Stephen I. Vladeck, Nicholas Weaver, and Benjamin Wittes for their insights. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense, the United States Government, or Judge Rogers.

ADAPTING U.S. ELECTRONIC SURVEILLANCE LAWS, POLICIES, AND PRACTICES TO REFLECT IMPENDING TECHNOLOGICAL DEVELOPMENTS

Eric Manpearl[†]

[†] Law Clerk to the Honorable John M. Rogers of the United States Court of Appeals for the Sixth Circuit. J.D. 2018, The University of Texas School of Law; Master of Public Affairs 2018, Lyndon B. Johnson School of Public Affairs; B.A. 2013, Rice University. Eric Manpearl clerked for the Honorable Royce C. Lamberth of the United States District Court for the District of Columbia and was previously the Brumley Next Generation Senior Graduate Fellow in the Intelligence Studies Project at the Robert S. Strauss Center for International Security and Law. Special thanks to Professors Robert Chesney, William Inboden, and Steve Slick for their thoughtful and invaluable suggestions, guidance, and advice. Also, thank you to Elisebeth B. Collins, Carrie F. Cordero, Michael Daniel, Laura Donohue, Timothy Edgar, Eric Greenwald, David S. Kris, Robert S. Litt, Benjamin A. Powell, Matt Tait, Stephen I. Vladeck, Nicholas Weaver, and Benjamin Wittes for their insights. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense, the United States Government, or Judge Rogers.

Intelligence collection must always evolve to meet technological developments. Following the September 11, 2001 terrorist attacks, President George W. Bush authorized several surveillance programs to enhance intelligence collection on the severe threats facing the United States.[1] However, these programs appeared to be inconsistent with the Foreign Intelligence Surveillance Act of 1978 (FISA), which governed intelligence collection that occurred inside the United States.[2] Technology had evolved in the intervening decades in a manner that could not have been foreseen by FISA's drafters and the statute was implicated by intelligence collection efforts that were likely never intended to be covered by the original statute. These outdated provisions posed significant challenges for the Intelligence Community. Ultimately, Congress passed the Protect America Act of 2007 (PAA) as a stop-gap measure, and the FISA Amendments Act of 2008 (FAA) to enable the government to target non-United States persons reasonably believed to be outside the United States to collect foreign intelligence information.[3] Section 702 of the FAA is likely the most important statutory tool for intelligence collection, especially against terrorism, and is vital for protecting United States national security. In 2018, there were more than 164,000 Section 702 targets.[4] The Intelligence Community would simply not be able to maintain nearly the same level of intelligence collection without Section 702. Further, Section 702 allows for collection to occur in a stable and safe domestic environment and can yield intact copies of the entirety of communications. This has been an extraordinary

1. OIG, DEP'T OF DEFENSE ET AL., REPORT NO. 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 4–14 (2009), https://oig.justice.gov/special/s0907.pdf [hereinafter OIG, DOD, REPORT ON SURVEILLANCE PROGRAM].

2. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 1785, 1790 (codified at 50 U.S.C. §§ 1801, 1805 (2012)).

3. Foreign Intelligence Surveillance Act of 1978, Amendments Acts of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (codified as amended at 50 U.S.C. § 1881a (2012)); Protect America Act of 2007, Pub. L. No. 110-55, § 105B, 121 Stat. 552, 552–54 (codified as amended at 50 U.S.C. § 1801 (2007)).

4. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES FOR CALENDAR YEAR 2018 13 (2019), https://www.dni.gov/files/CLPT/documents/2019_ASTR_for_CY2018.pdf [hereinafter DNI, TRANSPARENCY REPORT 2018].

success story for United States signals intelligence (SIGINT) and developed as a response to changing technology and a new threat landscape.

While the collection programs under Section 702 have produced a great deal of valuable intelligence over the last decade, the United States must begin to think about foreseeable technological developments and strategically consider how to conduct SIGINT collection in the future. This Article identifies four technological trends that could significantly impact the way the United States conducts SIGINT. Individuals now have access to sophisticated technologies that formerly only governments seemed capable of creating, and this decentralization of capabilities will likely only increase in the future. The increased prevalence of anonymity and location-spoofing technologies offer benefits to individual users but may create significant difficulties for the Intelligence Community in determining the location of targets, which is a fundamental aspect of the current legal regime governing SIGINT activities. Also, the United States' "home field" advantage is receding. This trend means that the United States will have a smaller share of the world's communications traffic transit its physical infrastructure, which will reduce the Intelligence Community's ability to acquire precise and intact communications by serving directives on United States companies. The push towards data localization laws may further reduce the United States' home field advantage. Finally, technology companies have begun to innovate in a manner that reduces their capability to respond to lawful government orders. Technology companies are increasingly adopting encryption technologies and may shift data overseas to try to avoid complying with lawful surveillance orders. Decisions by major private sector technology companies have the ability to shift how SIGINT is collected.

If a person's true location becomes increasingly more difficult to ascertain, the law should adapt to the uncertainty of location. This Article analyzes several possible reforms. Some have argued that the Fourth Amendment should apply to all individuals or that the Fourth Amendment should be presumed to apply unless that government can establish that no party to the communication is a United States person.[5] In a world in which location becomes extremely difficult to determine accurately, the FISA legal regime governing SIGINT activities could create a new category for non-United States persons appearing to be located in the United States. These individuals would be legitimate targets if the Foreign Intelligence Surveillance Court (FISC) determined on an individualized basis that there is reasonable suspicion to believe that these individuals are likely to possess, receive, and/or communicate foreign intelligence information. Alternatively, if anonymity and location-spoofing technologies become more advanced and are widely adopted such that determining location becomes an extreme problem for SIGINT collection under Section 702, it could be necessary to reform FISA by creating two categories, one for United States persons and

5. *See, e.g.*, David Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, JUST SEC. (Oct. 29, 2013), https://www.justsecurity.org/2668/foreigners-nsa-spying-rights/; Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 383 (2015).

one for non-United States persons. The more security-oriented reforms would push the limits of the foreign intelligence exception to the warrant clause in the Fourth Amendment. Ultimately, this Article concludes that the best reform approach in a world in which location becomes extremely difficult to determine accurately would be to reform FISA to create a new category for non-United States persons appearing to be located in the United States, though it may be necessary to go even further depending on the severity of the problem. In addition to legislative reforms, it may be prudent to create more forward leaning procedures to ease some of the difficulties that could be caused by increased uncertainty of the location of targets.

Finally, as Section 702 becomes less useful in the future, the Intelligence Community must improve collection under Executive Order 12333 to ensure that the government continues to acquire vital intelligence to protect United States national security interests. The National Security Agency (NSA) must continue to invest resources in being able to decrypt communications and acquiring unencrypted communications. The United States government should continue to work to develop strong relationships with United States technology companies and seek to reduce the strains that have been created in the aftermath of the Snowden disclosures. Also, as SIGINT collection under Executive Order 12333 becomes more important, the Intelligence Community must increase its focus on obtaining the cooperation of foreign entities and compromising key strategic targets. Beyond enhancing SIGINT collection capabilities, the Intelligence Community must focus on improving the ability to conduct intelligence analysis at scale by investing in technological tools that can assist with this work.

This Article proceeds in six parts. Part I recounts the history that led to the enactment of Section 702. This part describes how SIGINT collection under Section 702 operates and analyzes why this has been such an enormously important intelligence authority. Part II describes the technological developments that could change how the United States conducts SIGINT in the future. The increased prevalence of anonymity technologies, increased prevalence of location-spoofing technologies, reduction in the United States' home field advantage, and technological innovations by companies that reduce their ability to comply with government surveillance orders all challenge the effectiveness of Section 702.

Part III proposes strategies to address the difficulties in accurately determining location presented by anonymity and location-spoofing technologies. This part analyzes several legislative and procedural reform proposals. Part IV encourages the Intelligence Community to pursue a number of strategies to enhance Executive Order 12333 SIGINT collection to ensure that the government continues to acquire vital intelligence to protect United States national security interests even as Section 702 becomes less useful. Finally, Part V offers concluding remarks about how the United States should reform the laws and procedures governing SIGINT collection and shift intelligence collection

and analysis efforts under Executive Order 12333 to protect United States national security interests.

I. THE ORIGINS AND IMPORTANCE OF SECTION 702

A. The History of Section 702

In the aftermath of the September 11, 2001 terrorist attacks, President George W. Bush authorized the NSA to collect the contents of international communications between people inside and outside the United States without a FISC order under the Terrorist Surveillance Program (TSP).[6] In 2005, the *New York Times* revealed the existence of the TSP and the program faced numerous legal challenges.[7] The original FISA statute had defined electronic surveillance to include the acquisition of the contents of wire communication when at least one party is in the United States and the collection itself occurs in the United States, and compelled the government to obtain approval from the FISC to conduct electronic surveillance for foreign intelligence purposes inside the United States.[8] The original FISA statute required the government to establish probable cause that "the target of the electronic surveillance is a foreign power or an agent of a foreign power;" probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;" that the "proposed minimization procedures" are consistent with the statutory requirements; and that the information could not "reasonably be obtained by normal investigative techniques."[9] The President relied on his inherent Article II authority under the Constitution as the Commander in Chief and sole organ of the country to conduct foreign affairs, and the existence of the 2001 Authorization for Use of Military Force (AUMF) as legal justifications for the TSP, which appeared to be inconsistent with FISA.[10]

---

6. OIG, DOD, REPORT ON SURVEILLANCE PROGRAM, *supra* note 1, at 4–14.

7. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?mcubz=0; *e.g.*, ACLU v. NSA, 438 F. Supp. 2d 754, 782 (E.D. Mich. 2006) (holding that the TSP violated the First and Fourth Amendments), *vacated*, 493 F.3d 644 (6th Cir. 2007); *see* ACLU v. NSA, 493 F.3d 644, 648 (6th Cir. 2007) (finding that the plaintiffs lacked standing and reversing the district court's decision).

8. FISA § 101(f)(2), 92 Stat. at 1785, 1790.

9. *Id.* §§ 104–05, 92 Stat. 1790. Minimization procedures are a set of rules that dictate how a government agency will limit the accessibility, retention, and dissemination of inadvertently acquired material concerning United States persons who are not the target of the surveillance. § 101(h).

10. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITY SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT 2 (2006), https://www.justice.gov/sites/default/files/olc/opinions/2006/01/31/nsa-white-paper.pdf.

In January 2007, the government sought and obtained an order from the FISC authorizing the government to conduct certain electronic surveillance when "the *government* made a probable cause determination regarding one of the communicants, and the email addresses and telephone numbers to be tasked were reasonably believed to be used by persons located outside the United States."[11] When the government sought to renew this order in May 2007, a different FISC judge approved the program, but under a different legal theory, which required changes to the program. The May 2007 FISC order required that the FISC, instead of the government, make the probable cause determination.[12] This ruling led NSA analysts to be "significantly divert[ed] . . . from their counterterrorism mission to provide information to the Court," and then-Director of National Intelligence (DNI) Vice Admiral (Ret.) Mike McConnell determined that it "degraded capabilities in the face of a heightened terrorist threat environment."[13]

In addition to the TSP, the government used FISA to obtain court orders, based on probable cause, authorizing surveillance against individuals suspected of engaging in terrorist activities located outside the United States who used United States-based communications service providers.[14] The government expended "considerable resources" to meet FISA's requirement that it demonstrate there was probable cause to believe that these individuals were agents of a foreign power, which included international terrorist organizations, and used the specific communication facility that the government sought to surveil.[15] The necessity of drafting applications that met the probable cause standard "slowed down and in some cases prevented the acquisition of foreign intelligence information."[16] Then-DNI McConnell complained that it took

---

11. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 17 (2014), https://www.nsa.gov/about/civilliberties/resources/assets/files/pclob_section_702_report.pdf [hereinafter PCLOB, REPORT ON SURVEILLANCE PROGRAM];

see also Certification of Michael B. Mukasey, Att'y Gen. of the United States at para. 37, *In re* NSA Telecomms. Records Litig. (N.D. Cal. May 5, 2014) (No. 4:08-cv-04373-JSW), ECF No. 219,

https://www.dni.gov/files/documents/0505/AG%20Mukasey%202008%20Declassified%20Declaration.pdf [hereinafter AG Mukasey Certification].

12. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 17; AG Mukasey Certification, *supra* note 11, at para. 38.

13. S. SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACTS OF 2007, S. REP. NO. 110-209, at 5 (2007).

14. *Modernizing the Foreign Intelligence Surveillance Act: Hearing on S. 110-399 Before S. Select Comm. on Intelligence*, 110th Cong. 29–30 (2007) (statement of Kenneth L. Wainstein, Assistant Att'y Gen., Nat'l Sec. Div., Dep't of Justice) [hereinafter *Hearing on Modernizing FISA*].

15. *Id.*

16. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 18.

"about 200 man hours to do [a FISA application for] one telephone number."[17] The targeted individuals were foreigners, though, and were not intended to be protected by FISA when the statute was originally enacted in 1978. FISA was intended to provide privacy protections for Americans and guard against domestic political abuse, not protect foreigners whose only connection to the United States was that they were using United States-based communications service providers.[18] Yet, technology had evolved in a manner that could not have been foreseen by FISA's drafters and the statute was implicated by intelligence collection efforts directed at individuals outside the United States.

When FISA was originally enacted, domestic communications were almost entirely carried on a wire and international communications were wireless, radio communications.[19] FISA therefore closely regulated the collection of wire communications and less-stringently regulated the collection of radio communications.[20] However, technology shifted and international communications mostly traveled over physical cables—especially fiber optic cables—and domestic communications increasingly became transmitted wirelessly.[21] This meant that FISA ended up covering a significant amount of foreign intelligence collection activities targeting foreigners overseas that the statute was never actually intended to cover because of the statute's focus on how a communication was transmitted and where it was intercepted. Further, there was an enormous increase in commercial technologies that consumers could use, and consumers were able to use and change e-mail addresses and telephone numbers frequently across services.[22] This created

> a significant challenge for intelligence services which, under FISA 1978, had to obtain explicit approval for each and every selector they wanted to target. In 2008, there was a growing body of evidence that terrorists were making effective use of this agility, acquiring and

17. Chris Roberts, *Transcript: Debate on the Foreign Intelligence Surveillance Act*, EL PASO TIMES (Aug. 22, 2007, 1:05 AM), https://www.eff.org/files/filenode/att/elpasotimesmcconnelltranscript.pdf.

18. *See* H.R. PERMANENT SELECT COMM. ON INTELLIGENCE, FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978 AMENDMENTS ACTS OF 1978, H.R. REP. NO. 95-1283, at 68 (1978) (describing the House Permanent Select Committee on Intelligence's (HPSCI) consensus view that a "judicial warrant should be required whenever the [F]ourth [A]mendment rights of Americans might be involved"); RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 67–68, (2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (describing FISA's safeguards against domestic misuse and politicization).

19. *Hearing on Modernizing FISA*, *supra* note 14, at 29.

20. CHRIS INGLIS & JEFF KOSSEFF, HOOVER INST., IN DEFENSE OF FAA SECTION 702 5 (2016), https://www.hoover.org/research/defense-faa-section-702.

21. *Hearing on Modernizing FISA*, *supra* note 14, at 29; INGLIS & KOSSEFF, *supra* note 20, at 5.

22. INGLIS & KOSSEFF, *supra* note 20, at 5.

> shedding e-mail addresses and telephone numbers faster than US intelligence services could prepare, submit, and obtain required selector-by-selector approvals.[23]

In addition to the challenges posed by shifts in technology that rendered the original FISA outdated, global communications had evolved in a way that offered the United States a "home field" advantage.[24] Internet traffic was broken own into packets, which were transmitted based on the most efficient path, rather than linear geographic path between the sender and recipient.[25] Packets could travel around the world *en route* from the sender to the recipient, which presented the United States with a tremendous intelligence collection opportunity because a large amount of Internet traffic passed through equipment physically located in the United States.[26] This provided the United States with an opportunity to obtain foreign intelligence targets' communications from a stable and safe domestic environment instead of difficult circumstances overseas.[27] The Bush administration ultimately proposed modifications to FISA in spring 2007.[28] Congress passed the PAA to authorize the TSP by ensuring that "electronic surveillance" would not be defined to include "surveillance directed at a person reasonably believed to be located outside of the United States."[29] Under the PAA, the FISC no longer had jurisdiction over surveillance targeted at such individuals. Instead, the DNI and the Attorney General had the power to authorize such surveillance, and the FISC's only role was to ensure that the procedures for determining the surveillance was targeted at persons reasonably believed to be outside the United States were not "clearly erroneous."[30]

Congress then passed the FAA when the PAA expired to enable the government to target non-United States "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[31] Unlike traditional FISA surveillance, surveillance under Section 702 of the FAA did not require a probable cause standard that the target was a foreign power or

---

23. *Id.*

24. *FISA for the 21st Century: Hearing on S. 109-1055 Before S. Comm. on the Judiciary*, 109th Cong. 6–10 (2006) (statement of Michael V. Hayden, Dir., Cent. Intelligence Agency) [hereinafter *FISA for the 21st Century Hearing*].

25. *Id.*

26. *Id.*; John Markoff, *Internet Traffic Begins to Bypass the U.S.*, N.Y. TIMES (Aug. 29, 2008), http://www.nytimes.com/2008/08/30/business/30pipes.html.

27. *See FISA for the 21st Century Hearing*, *supra* note 24, at 9; INGLIS & KOSSEFF, *supra* note 20, at 4.

28. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 19.

29. Protect America Act of 2007, Pub. L. No. 110-55, § 105A, 121 Stat. 552, 552 (codified as amended at 50 U.S.C. § 1805a (2007)).

30. *Id.* § 105C(c), 121 Stat. at 555.

31. FISA § 702, 122 Stat. at 2438.

agent of a foreign power and did not require individual FISC orders.[32] Section 702 only required the Attorney General and DNI to obtain approval for the targeting procedures, minimization procedures, and certifications from the FISC, which then enabled the government to compel cooperation by issuing directives to companies.[33] The legal standard under Section 702 was less stringent than FISA Title I surveillance, which was focused primarily on United States persons, and the judicial oversight occurred less frequently than under FISA Title I. Once the government obtained certification from the FISC under Section 702, the government could then issue directives to private sector companies to compel the companies to cooperate with the government in the surveillance.[34]

B. How Section 702 Operates

Under Section 702, NSA analysts identify non-United States persons who are reasonably believed to be located outside the United States as potential targets for gathering foreign intelligence regarding a purpose that the FISC has certified. Analysts apply the NSA's targeting procedures "to make a determination regarding the assessed location and non-U.S. person status of the potential target (the *foreignness determination*) and whether the target possesses and/or is likely to communicate or receive foreign intelligence information authorized under an approved certification (the *foreign intelligence purpose determination*)."[35]

The analyst must first identify the specific selector (such as an email address or telephone number) that is used by the target.[36] The analyst then checks to verify that the target is indeed a non-United States person reasonably believed to be located outside the United States and that the target is connected to the selector.[37] The foreignness determination is based on the "totality of the circumstances" and NSA analysts must consult multiple sources in making the determination.[38] NSA procedures require "analysts [to] conduct 'due diligence'"

32. *Id.*

33. *Id.* § 702(d), (e), (g), 122 Stat. at 2439.

34. *Id.* § 702(h), 122 Stat. at 2442.

35. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 43.

36. INGLIS & KOSSEFF, *supra* note 20, at 10.

37. NAT'L SEC. AGENCY, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 1 (2018), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Targeting_27Mar18.pdf [hereinafter NSA, TARGETING PROCEDURES 2018]. *See* INGLIS & KOSSEFF, *supra* note 20, at 10.

38. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 43; *see* NSA, TARGETING PROCEDURES 2018, *supra* note 37, at 1.

in making the foreignness determination.[39] The Privacy and Civil Liberties Oversight Board (PCLOB) has recognized that

> [w]hat constitutes due diligence will vary depending on the target; tasking a new selector used by a foreign intelligence target with whom the NSA is already quite familiar may not require deep research into the target's (already known) U.S. person status and current location, while a great deal more effort may be required to target a previously unknown, and more elusive, individual.[40]

The NSA has specifically used an Internet Protocol (IP) filter with at least "upstream" collection to limit acquisition "to Internet transactions that originate and/or terminate outside the United States."[41] If there is conflicting information regarding whether the target is located inside the United States or is a United States person, the conflict "must be resolved," and the analysts must determine that the potential target is a "non-U.S. person reasonably believed to be located outside the United States prior to targeting."[42] In making the foreign intelligence purpose determination, NSA analysts must determine "that the target is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory."[43] NSA analysts must document their foreignness determinations and foreign intelligence purpose determinations, and two senior NSA analysts must approve the request before a service provider may be compelled to provide the communications associated with a tasked selector.[44]

After a selector has been tasked, the selector is sent to an electronic communications service provider so that acquisition can occur.[45] Two collection programs comprise Section 702 acquisition: "downstream" collection (which was formerly referred to as PRISM) and "upstream" collection. With

---

39. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 43.

40. *Id.* at 43–44.

41. NAT'L SEC. AGENCY, PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 2 (2017), https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf [hereinafter NSA, TARGETING PROCEDURES 2017].

42. INGLIS & KOSSEFF, *supra* note 20, at 10. *See* PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 44; PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., TRANSCRIPT OF PUBLIC HEARING REGARDING THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 40–42 (2014) (statement of Raj De, Gen. Counsel, Nat'l Sec. Agency), https://www.pclob.gov/library/20140319-Transcript.pdf [hereinafter PCLOB, TRANSCRIPT OF PUBLIC HEARING].

43. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 4.

44. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 45–46; INGLIS & KOSSEFF, *supra* note 20, at 11.

45. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 7.

downstream collection, the government compels an electronic communications service provider to turn over the communications that are sent "to" or "from" a specific selector.[46] Under upstream collection, the government compels companies that operate "the telecommunications 'backbone' over which telephone and Internet communications transit" to turn over communications that are sent "to" or "from" (and formerly "about") a specific selector.[47]

The NSA's targeting procedures also require post-tasking analysis to ensure that the person targeted remains a non-United States person overseas and that acquisition against the tasked selector only continues to the extent that the government assesses the tasking is likely to acquire foreign intelligence information.[48] Analysts must review content for indications that a target is a United States person, has entered the United States, or intends to enter the United States.[49] To ensure that analysts conduct this review, "[t]he NSA has developed automated systems to remind analysts to review collection from email addresses and comparable selectors within five business days after the first instance that data is acquired for a particular tasked selector, and at least every 30 days thereafter."[50] If the NSA determines that a person that was first "reasonably believed to be located outside the United States" was actually inside the United States after targeting, or if the NSA determines that a person "believed to be a non-United States person" was actually a United States person after targeting, the NSA must promptly detask the selectors used by that individual, which terminates the acquisition directed at those selectors.[51] The data acquired from a selector that the NSA learned after targeting was used by a United States person or person located inside the United States is destroyed unless the Director of the NSA determines—on a communication-by-communication basis—that the sender or intended recipient had been properly targeted and the "communication is reasonably believed to contain significant foreign intelligence information," "is

---

46. *See id.* (explaining PRISM collection); s*ee also NSA Stops Certain Section 702 "Upstream" Activities*, NAT'L SEC. AGENCY (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/ (explaining that PRISM collection is now referred to as "downstream" collection).

47. *See* PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 7 (explaining "upstream" collection). Upstream collection previously included the acquisition of "about" communications where the selector of a target was contained in the communication, but the NSA ended "about" collection in April 2017 because of trouble complying with FISC regulations. Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html; *NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702*, NAT'L SEC. AGENCY (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activites.shtml; *NSA Stops Certain Section 702 "Upstream" Activities*, *supra* note 46.

48. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 6–8.

49. *Id.* at 7.

50. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 48.

51. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 9–10.

reasonably believed to contain evidence of a crime," is reasonably believed to contain data to be used for cryptanalytic purposes or technical information necessary to understand a communications security vulnerability, or "contains information pertaining to an imminent threat of serious harm to life or property."[52] The NSA may notify "the FBI [Federal Bureau of Investigation] that a target has entered the United States so that the FBI may seek [a] traditional FISA [Title I order] or take other lawful investigative steps."[53]

C. The Importance of Section 702

Section 702 is likely the most important statutory tool for intelligence collection, particularly on terrorism, and is vital for protecting United States national security.[54] In 2018, there were more than 164,000 Section 702 targets.[55] Section 702 enables the Intelligence Community to collect intelligence on non-United States persons that it reasonably believes are overseas when it reasonably believes it will acquire foreign intelligence from surveilling these individuals. The Intelligence Community is not required to establish probable cause that the targeted individual is an agent of a foreign power, nor that each facility is being used or is about to be used by a foreign power or agent of a foreign power, nor that the information could not be reasonably obtained by normal investigative methods.[56] The probable cause requirement in FISA Title I is a protection derived from the Fourth Amendment, but non-United States persons that are

---

52. 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 10–12 (2018), https://www.intel.gov/assets/documents/702%20Documents/declassified/2018_Cert_NSA_Minimization_18Sep18.pdf [hereinafter NSA, MINIMIZATION PROCEDURES 2018].

53. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 50; *see* NSA, MINIMIZATION PROCEDURES 2018, *supra* note 52, at 12.

54. Press Release, Nat'l Sec. Agency, *The National Security Agency: Missions, Authorities, Oversight and Partnerships* (Aug. 9, 2013), https://www.nsa.gov/news-features/press-room/statements/2013-08-09-the-nsa-story.shtml (stating "[t]he collection under FAA Section 702 is the most significant tool in the NSA collection arsenal for the detection, identification, and disruption of terrorist threats to the U.S. and around the world"); *see* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE & DEP'T OF JUSTICE, THE INTELLIGENCE COMMUNITY'S COLLECTION PROGRAMS UNDER TITLE VII OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 6 (2012), https://www.dni.gov/files/documents/Ltr%20to%20HPSCI%20Chairman%20Rogers%20and%20Ranking%20Member%20Ruppersberger_Scan.pdf (summarizing the importance of SIGINT collection under Section 702).

55. DNI, TRANSPARENCY REPORT 2018, *supra* note 4, at 13.

56. *Compare* FISA § 702, 122 Stat. at 2438 (authorizing SIGINT collection targeting non-United States persons reasonably believed to be overseas to acquire foreign intelligence information), *with* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, §§ 102, 104–05, 92 Stat. 1783, 1786–90 (codified as amended at 50 U.S.C. §§ 1802, 1804–05 (2018)) (authorizing foreign intelligence collection under FISA Title I and establishing the legal requirements for conducting such SIGINT activities).

reasonably believed to be overseas are not entitled to Fourth Amendment protections.[57] Without Section 702, the Intelligence Community would likely be unable to amass sufficient information to establish probable cause against many of these targets and the United States would lose a significant amount of critical intelligence because it extended privacy protections to non-United States persons that were never intended for their protection. Even if the Intelligence Community could establish probable cause against some of these targets, the Intelligence Community would need to expend significant resources to meet this high standard, and such resource expenditure would take away from other critical national security missions and the entire process would cause delays in collection that could be harmful.[58] The Intelligence Community would simply not be able to maintain nearly the same level of intelligence collection without Section 702.[59]

Further, Section 702 allows for collection to occur in a stable and safe domestic environment. Under downstream collection, the communications "to" and "from" a selector are even provided to the NSA in a manner that is highly likely to yield intact copies of the entirety of the communications.[60] While Executive Order 12333 authorizes the NSA to collect SIGINT abroad on non-United States persons and accounts for the vast majority of SIGINT collected globally, collection under Executive Order 12333 is often accomplished in a more difficult and less safe environment, and often results in obtaining packets of communications instead of entire communications.[61] Therefore, Section 702 provides a more precise, complete, and safe collection authority than Executive Order 12333. Also, Section 702 collection occurs by the compelled assistance of United States electronic communications service providers, which means that the government does not have to risk exposing its sensitive sources and methods to obtain such information, which it risks exposing under Executive Order 12333 collection.[62] Finally, the PCLOB has found that

---

57. U.S. CONST. amend. IV; United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

58. *See* James Comey, Dir., Fed. Bureau of Investigation, Keynote Address at the Intelligence Studies Project Conference: Intelligence in Defense of the Homeland (Mar. 23, 2017), *in Strauss Ctr. for Int'l Sec. & Law*, UNIV. OF TEX. AT AUSTIN (Mar. 30, 2017), at 4:05, 7:29–8:05, https://intelligencestudies.utexas.edu/events/item/560-isp-spring-conference (describing that FISA Title I applications are lengthy documents and undergo significant internal oversight and external judicial oversight).

59. Interview with Benjamin A. Powell, Former Gen. Counsel, Office of the Dir. of Nat'l Intelligence, in D.C. (Feb. 12, 2018).

60. INGLIS & KOSSEFF, *supra* note 20, at 4.

61. Exec. Order No. 12,333, 3 C.F.R. § 200 (1981), *as amended by* Exec. Order No. 13,284, 68 Fed. Reg. 4075 (Jan. 28, 2003), *as amended by* Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Sept. 1, 2004), *as amended by* Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (Aug. 4, 2008); INGLIS & KOSSEFF, *supra* note 20, at 4; PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 107.

62. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 107.

> acquiring communications with the compelled assistance of U.S. companies allows service providers and the government to manage the manner in which the collection occurs. By helping to prevent incidents of overcollection and swiftly remedy problems that do occur, this arrangement can benefit the privacy of people whose communications are at risk of being acquired mistakenly.[63]

II. TECHNOLOGICAL DEVELOPMENTS THAT COULD CHANGE HOW THE UNITED STATES CONDUCTS SIGINT

Section 702 was a critical intelligence collection reform that belatedly addressed technological developments to enable the Intelligence Community to acquire important foreign intelligence to protect United States national security interests and inform policymakers. While the collection programs under Section 702 have produced a great deal of valuable intelligence over the last decade, the United States must begin to think about foreseeable technological developments and strategically consider how to conduct SIGINT collection in the future.

Individuals now have access to sophisticated technologies that formerly only governments seemed capable of creating. This decentralization of capabilities is a trend that will likely only increase in the future. While access to new technologies produces innovation, improves daily life, and aides human rights activists living under oppressive regimes, these same technologies can be utilized by malign actors to conduct illicit activities.[64] Two trends that may benefit individual users while creating difficulties for the United States Intelligence Community are the increased prevalence of anonymity and location-spoofing technologies.

Also, the United States' home field advantage is shrinking.[65] This trend means that the United States will have a smaller share of the world's communications traffic transit its physical infrastructure, which will reduce the Intelligence Community's ability to acquire precise and intact communications by serving directives on United States companies.[66] The possible balkanization of the Internet through data localization laws may exacerbate this trend threatening the United States' home field advantage.

Further, technology companies have begun to innovate in a manner that reduces their capability to respond to lawful orders. Technology companies have increasingly adopted encryption technologies and may shift data overseas

---

63. *Id.*

64. *See* BENJAMIN WITTES & GABRIELLA BLUM, THE FUTURE OF VIOLENCE 20 (2015) ("By delivering dramatic new capabilities to humanity in general—and to individual humans in particular—technological developments creates the certainty that some of those individuals will use those capabilities to do evil.").

65. David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SEC. L. & POL'Y 377, 417 (2016).

66. *Id.*; PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 107.

to try to avoid complying with lawful surveillance orders in the United States.[67] Following Snowden's unauthorized disclosures regarding United States intelligence activities, United States based technology companies have viewed it as being in their interest to take more adversarial stances in their relationships with the United States government to protect market share and maintain consumer confidence, especially among foreign consumers.[68] Decisions by major private sector technology companies, who may view themselves primarily as global enterprises and may not necessarily be predisposed to serve the United States government's interests, have the remarkable ability to shape how SIGINT is collected.

A. Anonymity Technologies

The increased prevalence and advancement of anonymity technologies may create difficulties for the Intelligence Community in its foreignness determinations and post-tasking analysis. Anonymity tools intentionally hide users' real identities and locations, and provide individuals with ways to circumvent censorship.[69] These products can be enormously useful to human rights activists, dissidents, and journalists living under oppressive regimes, as well as provide privacy protections for individuals.[70] At the same time, the information about a user's true identity and location that are masked by anonymity tools can be critical for the NSA's ability to lawfully target individuals under Section 702.

Tor is one of the most prominent anonymity technologies and serves as a good example for understanding how these technologies operate. Tor enables users to access the Internet anonymously and browse the Internet in such a way that the computer the user is ultimately communicating with does not know who the user is or where the user is physically located—the user's Internet traffic instead appears to originate from the Tor server.[71] Individuals connect to Tor and the packets of data that travel from the user's computer to the recipient computer travel an encrypted path through relay nodes.[72] Relay nodes are computers that are scattered across the world whose owners have also installed Tor and

---

67. Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. 99, 134–35, 138 (2018).

68. Rozenshtein, *supra* note 67, at 115–16.

69. Jim Finkle, *Web Tools Help Protect Human Rights Activists*, REUTERS (Aug. 19, 2009, 4:33 AM), https://www.reuters.com/article/us-column-pluggedin/web-tools-help-protect-human-rights-activists-idUSTRE57I4IE20090819.

70. David D. Clark & Susan Landau, *Untangling Attribution*, 2 HARV. NAT'L SEC. J. 531, 546 (2011); Finkle, *supra* note 69; *Who Uses Tor?*, TOR, https://www.torproject.org/about/torusers.html.en (last visited Sept. 7, 2019).

71. *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Sept. 8, 2019).

72. *Id.*

volunteered their computers to serve as proxies that route data packets.[73] Users connecting to Tor randomly select a path of Tor nodes to perform communications.[74] When the user sends their message over the Tor network, the message first travels to an entry node over an encrypted link.[75] The entry node only knows that the user is connecting to that entry node and that the user has a message that the entry node must pass along to the middle node, but the entry node does not know the content of the message or the message's final recipient because this information is encrypted.[76] Next, the middle node receives the message from the entry node, but only knows that the message came from the entry node and that it must pass the message to the exit node.[77] The middle node does not know who the message originated with, the message's final recipient, or the content of the message because this information is encrypted. [78] Subsequently, the exit node receives the message from the middle node, but only knows that the message came from the middle node and that it must pass the message to the recipient.[79] The exit node does not know who the message originated with or the content of the message—as long as the connection between the exit node and ultimate recipient is also encrypted.[80] Finally, the recipient receives the message from the exit node and can decrypt the content of the message.[81] This means that the user's Internet traffic appears to originate from the exit node, which is a proxy computer, rather than from the original user's computer.[82] This hides the user's IP address, which is a unique identifier that identifies the user's computer and can be used with a high degree of accuracy to determine the location of the user.[83] Also, the traffic emanating from the user's computer appears to be going only to the entry node—a proxy computer—rather than the actual final destination from the perspective of the Internet service provider (ISP).[84] Tor updates its circuits frequently so the user connects to different entry nodes and different exit nodes send the Internet traffic to its final destination.[85]

---

73. *What is Tor?*, TOR, https://www.eff.org/torchallenge/what-is-tor.html (last visited Sept. 8, 2019).

74. *Tor: Overview*, *supra* note 71.

75. *Id.*

76. *Id.*

77. *Id.*

78. *Id.*

79. *Id.*

80. *Id.*

81. *Id*.

82. *Id.*

83. Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1091 (2017).

84. *Id.* at 1088.

85. *Tor FAQ: How Often Does Tor Change its Paths?*, TOR, https://www.torproject.org/docs/faq.html.en#ChangePaths (last visited Sept. 8, 2019) ("Tor will

An individual that is located in the United States and using an anonymity technology, such as Tor, will appear to be located in another country from the perspective of the destination computer—which is likely a webpage—if the exit node is located in another country. Similarly, an individual using this technology that is located outside of the United States will appear to be located inside the United States from the perspective of the destination computer if the exit node is located inside the United States. An individual will appear to the ISP to be communicating only with the entry node and the ISP will not know that the individual ultimately communicated with the destination computer.

Further, individuals can "host content or services without exposing the physical location of their servers" by using Tor's onion services, which were formerly known as hidden services.[86] Onion services are only accessible on the Tor network and users can only communicate with an onion service through a rendezvous point on the Tor network.[87]

Anonymity technologies have become more prevalent in recent years. The number of Tor users increased from under one million users prior to the Snowden disclosures to nearly six million users just after the disclosures, and is currently about two million users as of March 2020.[88] In 2014, a survey of Internet users across twenty-four countries conducted by the Centre for International Governance Innovation showed that 60% of Internet users had heard about Edward Snowden and that 39% of those aware of Snowden reported taking steps to protect their security and privacy online as a result of the disclosures.[89] Bruce Schneier, an American security technologist, calculated that the data from this survey indicated that over 700 million people across the world may have taken steps to try to improve their security and privacy online in the aftermath of the Snowden disclosures.[90] Many of these people are likely not sophisticated technology users, but this demonstrates that there is growing awareness of the surveillance activities that intelligence services engage in, and there is a significant segment of the global population that desires greater

---

reuse the same circuit for new TCP streams for 10 minutes, as long as the circuit is working fine. (If the circuit fails, Tor will switch to a new circuit immediately.)").

86. Ghappour, *supra* note 83, at 1088; *see also Tor: Onion Service Protocol*, TOR, https://www.torproject.org/docs/onion-services.html.en (last visited Sept. 8, 2019) (explaining onion services).

87. *Tor: Onion Service Protocol*, *supra* note 86.

88. *Users*, TOR METRICS, https://metrics.torproject.org/userstats-relay-country.html?start=2013-06-01&end=2020-03-30&country=all&events=off (last visited Mar. 30, 2020) (showing user data for Tor between June 1, 2013 and March 30, 2020).

89. CTR. FOR INT'L GOVERNANCE INNOVATION & IPSOS, 2014 CIGI-IPSOS GLOBAL SURVEY ON INTERNET SECURITY AND TRUST 3 (2014), https://www.cigionline.org/sites/default/files/documents/internet-survey-2014-factum.pdf.

90. Bruce Schneier, *Over 700 Million People Taking Steps to Avoid NSA Surveillance*, LAWFARE (Dec. 15, 2014, 9:02 AM), https://www.lawfareblog.com/over-700-million-people-taking-steps-avoid-nsa-surveillance.

protections against such activities. People's desire for greater security and privacy online is likely also driven by the increased awareness of the extent of information that private companies collect about users to use for advertising purposes and the increased awareness of cybercrime.[91] This may drive more people to use anonymity technologies, at least for sensitive online activities. Also, malicious actors, such as terrorist organizations, have learned from the Snowden disclosures and adjusted their tradecraft to attempt to thwart United States intelligence.[92] Guidelines for how to use Tor have been distributed on an al-Qaeda affiliated forum, the Islamic State of Iraq and al-Sham (ISIS) has advised its followers to use Tor when engaging in propaganda activities and communicating with other terrorists, and ISIS has reportedly launched propaganda sites using Tor's onion services.[93]

---

91. *See* Rafi Goldberg, *Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities*, NAT'L TELECOMMS. & INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities (finding that Americans have become increasingly concerned about Internet security and privacy because of prominent data breaches, cybersecurity incidents, and privacy controversies); Mary Madden, *Public Perceptions of Privacy and Security in the Post-Snowden Era*, PEW RESEARCH CTR. (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/ (finding that "91% of adults in the survey 'agree' or 'strongly agree' that consumers have lost control over how personal information is collected and used by companies," "80% of those who use social networking sites say they are concerned about third parties like advertisers or businesses accessing the data they share on these sites," and "[m]ost say they want to do more to protect their privacy").

92. *See* EDWARD JAY EPSTEIN, HOW AMERICA LOST ITS SECRETS: EDWARD SNOWDEN, THE MAN AND THE THEFT 291–98 (2017) (recounting United States intelligence officials' determinations that foreign terrorist targets took steps to avoid NSA SIGINT collection following the Snowden revelations, which led to the NSA losing their ability to collect on these targets); MICHAEL V. HAYDEN, PLAYING TO THE EDGE: AMERICAN INTELLIGENCE IN THE AGE OF TERROR 421 (2016) (stating that intelligence targets were alerted to United States intelligence tactics and techniques by the Snowden disclosures); MICHAEL MORELL, THE GREAT WAR OF OUR TIME 294 (2015) ("Within weeks of the leaks, terrorist organizations around the world were already starting to modify their actions in light of what Snowden disclosed. Communication sources dried up, tactics were changed. Terrorists moved to more secure communication platforms, they are using encryption, and they are avoiding electronic communications altogether.").

93. *See* LAITH ALKHOURI & ALEX KASSIRER, TECH FOR JIHAD: DISSECTING JIHADISTS' DIGITAL TOOLBOX 2–3 (2016), https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (finding that jihadists have sought to leverage Tor and VPNs to improve their internet security and hide from intelligence and law enforcement agencies, and have encouraged fellow terrorists to adopt these technologies on jihadist web forums); JAMIE BARTLETT & ALEX KRASODOMSKI-JONES, ONLINE ANONYMITY: ISLAMIC STATE AND SURVEILLANCE 7–13 (2015), https://www.demos.co.uk/files/islamic_State_and_Encryption.pdf?1426713922 (providing a blog post that was likely posted by an ISIS fighter advising terrorists on how to avoid government surveillance by using technologies such as Tor and VPNs); Joseph Cox, *ISIS Now Has a Propaganda Site on the Dark Web*, MOTHERBOARD (Nov. 16, 2015, 2:20 PM), https://motherboard.vice.com/en_us/article/d7yzy7/isis-now-has-a-propaganda-site-on-the-dark-web (finding that ISIS launched a propaganda website as a Tor hidden service, which is now called an onion service); *Tor Security Guidelines Distributed on AQ-Affiliated Forum*,

Anonymity technologies may present difficulties for the NSA in conducting surveillance under Section 702 because the statute only permits the NSA to target non-United States persons that are reasonably believed to be overseas. Anonymity technologies disguise users' true IP addresses, which are critical pieces of information that can be used to identify individual's locations. The NSA may therefore have difficulty in determining whether a potential target is a United States person or non-United States person and whether the potential target is inside the United States or overseas. There will likely be many occasions when the information that leads analysts to determine that there is a valid foreign intelligence reason to target a person includes information about the person's citizenship and location, which would alleviate the difficulties arising from having to make a foreignness determination based solely on information that is transmitted using anonymity technologies, but this may not always be the case.

For example, targeting may be based on an intelligence officer's interaction with a person on a terrorist chat forum.[94] The person's presence and activities in the chat forum may provide the officer with a reasonable belief that the individual "is expected to possess, receive, and/or is likely to communicate foreign intelligence information."[95] The officer can then analyze the available information regarding the potential target, such as, the language they use and time of day that they log onto the chat forum, as indicators of the person's status and location.[96] The officer may also review information in the NSA's databases to see if information regarding the person's location is already known.[97] Sophisticated actors could use anonymity technologies and employ tradecraft techniques to attempt to hide their identities and locations, which could require NSA analysts to devote significant time and resources to determining whether specific users are legitimate targets under Section 702.

Currently, the NSA is allowed "to make reasonable presumptions regarding a target's foreignness" based on the information that is available.[98] The NSA

SITE INTELLIGENCE GRP. (Dec. 1, 2015), https://news.siteintelgroup.com/Jihadist-News/tor-security-guidelines-distributed-on-aq-affiliated-forum.html (determining that a group distributed a manual on an al-Qaeda affiliated web forum for obtaining anonymity by using Tor); Kim Zetter, *Security Manual Reveals the OPSEC Advice ISIS Gives Recruits*, WIRED (Nov. 19, 2015, 4:45 PM), https://www.wired.com/2015/11/isis-opsec-encryption-manuals-reveal-terrorist-group-security-protocols/ (analyzing an ISIS operational security guide that advises followers on how to protect their communications and location data).

94. Interview with Matt Tait, Cybersecurity Senior Fellow, Robert S. Strauss Ctr. for Int'l Sec. & Law, in Austin, Tex. (Feb. 8, 2018).

95. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 4.

96. Interview with Matt Tait, *supra* note 94.

97. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 3.

98. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 2015 SUMMARY OF NOTABLE SECTION 702 REQUIREMENTS 4 (2015), https://www.dni.gov/files/documents/icotr/51117/

likely makes the presumption that an individual whose actual location cannot be determined is outside the United States and assumes that a person whose location is unknown is a non-United States person unless that person can be positively identified as a United States person "or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person."[99] The FISC has noted that the NSA only makes such presumptions of foreignness after it has exercised due diligence in attempting to determine the potential target's location.[100]

These presumptions are consistent with the statute's requirement that the Attorney General and DNI

> adopt targeting procedures that are reasonably designed to–
>
> > (A) ensure that any acquisition authorized under [Section 702] is limited to targeting persons reasonably believed to be located outside the United States; and
> >
> > (B) prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.[101]

When the NSA cannot determine the location of a potential target, such as when a user consistently uses anonymity technologies, after exercising due diligence then it is reasonable to assume that the person is not inside the United States, as there is no information that indicates the person is inside the United States. Also, the NSA would clearly not be intentionally acquiring communications to or from a person known at the time of acquisition to be located in the United States as the NSA would not know the person's location at the time of acquisition.

The NSA's presumptions are also consistent with the Fourth Amendment. The Fourth Amendment asserts that:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[102]

The Supreme Court has recognized that the warrant clause does not apply in certain circumstances "when special needs, beyond the normal need for law

---

Doc%201%20%E2%80%93%202015%20Summary%20of%20Notable%20Section%20702%20Requirements.pdf.

99. NSA, MINIMIZATION PROCEDURES 2018, *supra* note 52, at 4.

100. In re DNI/AG Certification, No. 702(i)-08-01, at 10 (FISA Ct. Sept. 4, 2008), https://www.dni.gov/files/documents/0315/FISC%20Opinion%20September%204%202008.pdf.

101. 50 U.S.C. § 1881a(d)(1).

102. U.S. CONST. amend. IV.

enforcement, make the warrant and probable-cause requirements impracticable."[103] The Supreme Court has not addressed whether a similar exception applies for foreign intelligence surveillance. In *Katz*,[104] the Court noted in a footnote that its decision requiring the authorization of a magistrate based on a showing of probable cause prior to engaging in electronic surveillance to satisfy the Fourth Amendment did not determine whether the same analysis would extend to situations involving national security, which would include intelligence surveillance.[105] The Court continued to leave open the question of whether the Fourth Amendment requires a warrant when intelligence investigations concern foreign powers even when it determined that domestic surveillance required appropriate prior warrant procedure in *Keith*.[106] Foreign intelligence surveillance serves a purpose beyond traditional law enforcement objectives and is a vital tool for protecting national security. The Supreme Court has noted that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[107] The government's interest is therefore particularly strong in the foreign intelligence context. If the government was required to obtain a warrant prior to engaging in foreign intelligence surveillance, the government would be hindered in its "ability to collect time-sensitive information" and the government's "vital national security interests that are at stake" would be impeded.[108] This has led multiple federal appeals courts and the Foreign Intelligence Surveillance Court of Review (FISCR) to recognize that there is a foreign intelligence exception to the Fourth Amendment's warrant requirement.[109] The government's action must therefore

103. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

104. Katz v. United States, 389 U.S. 347 (1967).

105. *Id.* at 358 n.23; *see* Eric Manpearl & Raheem Chaudhry, *Judicial Oversight of the Intelligence Community*, *in* INTELLIGENCE AND NATIONAL SECURITY IN AMERICAN SOCIETY 71, 71 (2016).

106. United States v. U.S. Dist. Court (Keith), 407 U.S. 297 (1972).

107. Haig v. Agee, 453 U.S. 280, 307 (1981) (quoting Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964)).

108. In re Directives Pursuant to Section 105b of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008).

109. *Id.*; United States v. Truong Dinh Hung, 629 F.2d 908, 912–16 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 604–06 (3d Cir. 1974) (en banc); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973). *But see* Zweibon v. Mitchell, 516 F.2d 594, 632–51 (D.C. Cir. 1975) (en banc) (plurality opinion) (suggesting, in dictum, that no such exception exists, which was not joined by the majority of the court). Subsequently, the D.C. Circuit has recognized that *Zweibon* only determined that "the warrantless electronic surveillance within the United States of persons not suspected of any collaboration with foreign interests adverse to this country violates the [F]ourth [A]mendment," but that "there was no opinion of the court on the question of warrantless surveillance of collaborators or suspected collaborators of foreign interests." Halkin v. Helms, 690 F.2d 977, 1000 n.82 (D.C. Cir. 1982); *see also* Ellsberg v. Mitchell, 709 F.2d 51, 66 n.63 (D.C. Cir. 1983); United States v. Belfield, 692 F.2d 141, 145 (D.C. Cir. 1982); Chagnon v. Bell, 642 F.2d 1248, 1259 (D.C.

comply with the Fourth Amendment's reasonableness requirement to be constitutional.

In determining whether a government action is reasonable, courts must consider the totality of the circumstances.[110] Courts "weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy.'" [111] The government's action is reasonable in the situation where the NSA discovers a potential target that an analyst determines "is expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory," and that potential target is using an anonymity technology like Tor to successfully mask their identity and physical location.[112] The government clearly has an extraordinarily strong interest in collecting foreign intelligence information and the NSA has assessed that surveilling the potential target would likely result in the acquisition of foreign intelligence in this situation. The NSA only makes a presumptions of foreignness after it has exercised due diligence in attempting to determine the potential target's location.[113] Under *Verdugo-Urquidez*,[114] the Fourth Amendment does not apply to the searches of foreigners outside the United States.[115] Thus, an individual presumed to be a non-United States person overseas does not have privacy interests protected by the Fourth Amendment. However, the individual does suffer a severe privacy intrusion that is protected under the Fourth Amendment if the individual is actually a United States person or is located inside the United States. The NSA's Section 702 procedures provide important protections that reduce this intrusiveness. If the NSA discovers that this person was actually inside the United States or was actually a United States person after targeting, the NSA must promptly detask the selectors used by the individual, which terminates the acquisition directed at those selectors.[116] The data acquired from these selectors would be promptly destroyed, too, unless the Director of the NSA made a specific determination that an exception applied.[117] These measures provide back-end privacy protections for United States persons or individuals that are actually located

---

Cir. 1980). While *Truong* stated that the "government should be relieved of seeking a warrant only when the object of the search or the surveillance is a foreign power, its agent or collaborators," courts today would likely expand the foreign intelligence exception beyond this narrow foreign power nexus requirement to foreign intelligence more broadly given the diverse array of threats from both state and non-state actors in the modern world. *Truong*, 629 F.2d at 915.

110. Samson v. California, 547 U.S. 843, 848 (2006).

111. Maryland v. King, 569 U.S. 435, 448 (2013) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

112. *See* NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 4.

113. In re DNI/AG Certification, *supra* note 100, at 10.

114. United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

115. *Id.* at 274–75.

116. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 9–10.

117. NSA, MINIMIZATION PROCEDURES 2018, *supra* note 52, at 8, 10–12.

inside the United States that are presumed to be foreigners and targeted based on their actions warranting a foreign intelligence purpose determination that occur over the Tor network. The NSA's actions are ultimately reasonable and therefore constitutional in such a circumstance.

The real difficulty for the NSA may be in the post-tasking analysis, rather than in targeting. The NSA requires that analysts review information for indications that a target is a United States person, has entered the United States, or intends to enter the United States.[118] When a target uses anonymity technologies like Tor, the target may appear to be located in different locations depending on where the nodes are located at any given time.[119] There may be instances where the communications acquired from an electronic communications service provider under downstream or Internet transactions acquired from companies that operate the "the telecommunications 'backbone' over which telephone and Internet communications transit" under upstream indicate that the target is located inside the United States if the Tor nodes are located inside the United States.[120] NSA analysts must determine if such information indicates that the target is actually a United States person or is actually inside the United States, which would require detasking, or if the target is only appearing to be present inside the United States because they are using an anonymity technology.[121] This may be a resource intensive endeavor for NSA analysts that leads analysts to spend valuable time trying to determine if the target can continue to be lawfully targeted under Section 702. This would inevitably reduce the amount of time that analysts could spend on other important national security matters. The post-tasking analysis may result in detasking selectors that appear to be being used by a target inside the United States. While the NSA may notify the FBI that a target has appeared to enter the United States so that the FBI may seek a traditional FISA Title I order or take other lawful investigative steps, there may not be enough information to meet the higher legal standards to proceed with these other investigative measures.[122]

Although the NSA must have determined the person was "expected to possess, receive, and/or is likely to communicate foreign intelligence information concerning a foreign power or foreign territory"[123] in order to target them under Section 702, there may not be enough information to establish

118. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 6–8.

119. *See supra* Part II.A.

120. *See* PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 7 (explaining how PRISM collection, now called downstream collection, and upstream collection operate).

121. *See* NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 8–10 (explaining that the NSA must promptly detask the selectors used by an individual if the NSA determines that the individual that was reasonably believed to be located outside the United States was actually inside the United States after targeting, or if the NSA determines that the individual that was believed to be a non-United States person was actually a United States person after targeting).

122. NSA, MINIMIZATION PROCEDURES 2018, *supra* note 52, at 12.

123. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 4.

probable cause that the target is an agent of a foreign power to obtain a FISA Title I order, or "probable cause for belief that an individual is committing, has committed, or is about to commit" an enumerated crime to obtain a court order to intercept wire, oral, and electronic communications under Title III of the Omnibus Crime and Safe Streets Act of 1968.[124] This means that the Intelligence Community would lose the ability to collect on the target, and therefore lose potentially important insight into a terrorist group, foreign country, or other illicit actor. Even if there is enough information to obtain probable cause under one of these legal mechanisms, it requires significant resources and time to put together sufficient FISA Title I and Title III applications.[125]

If anonymity tools become more prevalent and such post-tasking problems become more common, this would pose a serious problem for the Intelligence Community. Trying to establish probable cause on a significant number of targets that appear to now be located within the United States after originally appearing to be non-United States persons overseas when they were first targeted would require the government to use a significant amount of resources, which would take way from other important national security missions, and cause delays in intelligence collection. In addition, even if it were later discovered that the target was using an anonymity technology, such as Tor, and not actually inside the United States, which would allow for the selector to be tasked once again, any communications that occurred during the intervening time after the selector was detasked and before the selector was re-tasked would not be collected and would be lost to the Intelligence Community.

However, there is reason to doubt that anonymity technologies will become widespread to the point where they may cause significant problems for the NSA.[126] Anonymity tools like Tor are not simple to use and will always be rather slow because users' traffic must bounce through volunteers' proxy

---

124. Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2518(3) (2012); 50 U.S.C. § 1805(a) (2012); *see* PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 109 (discussing probable cause requirements under FISA Title I); NSA, MINIMIZATION PROCEDURES 2018, *supra* note 52, at 12 (explaining that the NSA may notify the FBI that a target has appeared to enter the United States so that the FBI may seek a traditional FISA Title I order or take other lawful investigative steps).

125. *See, e.g.*, OFFICE OF ENF'T OPERATIONS, ELECTRONIC SURVEILLANCE MANUAL 1–16 (2005), https://www.justice.gov/sites/default/files/criminal/legacy/2014/10/29/elec-sur-manual.pdf (describing the Title III wiretap application process) [hereinafter OEO, ELECTRONIC SURVEILLANCE MANUAL]; *See also* Roberts, *supra* note 17 (quoting former Director of National Intelligence (DNI) Admiral Mike McConnell as stating "[i]t takes about 200 man hours to do [a FISA application for] one telephone number").

126. Telephone Interview with Nicholas Weaver, Researcher, Int'l Comput. Sci. Inst., Professor, Univ. of Cal. Berkley (Feb. 5, 2018) (explaining the performance costs of using Tor).

computers in different parts of the world.[127] There are also bottlenecks caused by the network not having enough nodes, especially exit nodes, to handle all of the traffic.[128] Currently, people volunteer their computers to serve as nodes, but this uses bandwidth and therefore costs these people money to provide a service for others using the network.[129] Middle nodes have no opportunity to see content in anonymity technologies and therefore cannot even try to monetize access to such information by selling it to advertisers as this would defeat the purpose of anonymity technologies.[130] It is difficult to see how a company would monetize an anonymity technology product other than by having users pay for it, which could generate revenue to pay for computers to serve as nodes. But many people may not be willing to pay for such products.[131] Also, it can be especially difficult to get enough people to volunteer to run exit nodes.[132] When illicit actors use Tor to engage in criminal activity, like accessing child pornography websites, it is the exit node's IP address that appears to be connecting to the final website.[133] This means that the person running the exit node can get embroiled in criminal investigations.[134] This risk reduces the number of people that are willing to serve as exit nodes, which exacerbates the bottleneck issue that is part of what slows anonymity technologies. It is still possible that an Internet browser could create an anonymity technology and could compete with other major Internet browsers, such as Google Chrome and Mozilla Firefox, but it seems unlikely

127. *Tor FAQ: Why is Tor so Slow?*, TOR, https://www.torproject.org/docs/faq.html.en#WhySlow (last visited Sept. 8, 2019); *see also* SUSAN LANDAU, SURVEILLANCE OR SECURITY?: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES 199 (2010) (acknowledging that Tor and other anonymity technologies "have high overhead and are not expected to be used by the vast majority of users").

128. *See* ROGER DINGLEDINE & STEVEN J. MURDOCH, PERFORMANCE IMPROVEMENTS ON TOR OR, WHY TOR IS SLOW AND WHAT WE'RE GOING TO DO ABOUT IT 7–11 (2009), https://svn.torproject.org/svn/projects/roadmaps/2009-03-11-performance.pdf (explaining traffic in the Tor network and its capacity).

129. *See* Interview with Matt Tait, *supra* note 94.

130. *Id.*

131. *See* NIC NEWMAN ET AL., REUTERS INST., DIGITAL NEWS REPORT 2017 36 (2017), https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf (finding that video was the form of online media that had the highest proportion of people that paid for it based on a study of 36 markets, and that only 23% of people across the 36 markets stated that they paid for this form of online media); Lee Rainie & Kristen Purcell, *The Economics of Online News*, PEW RESEARCH CTR. (Mar. 15, 2010), http://www.pewinternet.org/2010/03/15/the-economics-of-online-news/ (finding that only about one in five stated they would be willing to pay for online news content).

132. *See* DINGLEDINE & MURDOCH, *supra* note 128, at 7–11; Interview with Matt Tait, *supra* note 94.

133. *See Tor FAQ: How is Tor Different from Other Proxies?*, TOR, https://www.torproject.org/docs/faq.html.en#Torisdifferent (last visited Sept. 8, 2019).

134. *Id.*

that anonymity technologies will become as ubiquitous as encryption technologies have become.[135]

Further, people often reveal information about themselves even when using anonymity technologies.[136] People have a natural desire to want to be connected with others and therefore often use social media and email, which can provide information regarding a person's true identity and location.[137] Many people do not necessarily want to remain anonymous all the time.[138]

Nonetheless, these technologies can still currently pose problems for the NSA and the increased prevalence of anonymity technologies will likely make the NSA's work more difficult, especially with malign actors who use sophisticated tradecraft. Also, these bad actors will become more difficult to surveil as other innocent users decide to use anonymity technologies because this enables the malicious actors to hide among innocent users.

B. Location-Spoofing Technologies

The increased prevalence of location-spoofing technologies, such as virtual private networks (VPNs), may create more severe difficulties for the NSA than anonymity technologies. VPNs encrypt and relay Internet communications from a user's computer to another computer, where the communications are then decrypted and sent on to their final destination.[139] This makes it appear as if the communications are actually coming from the intermediary computer, which can be run by a VPN service, instead of the original user.[140] Thus, "the user's apparent IP address corresponds to the VPN server, which may or may not be in the same country as the user."[141] VPNs are used by businesses so that employees can securely access internal resources; by ordinary people to protect their privacy and protect their personal data from being stolen by cyber criminals; and to defeat censorship through geo-blocking, which is a location-based restriction

---

135. *See* Stephen Shankland, *Want True Privacy, You Need to Check Out This Browser*, CNET (Apr. 6, 2017, 5:00 AM), https://www.cnet.com/news/privacy-browser-brave-tor-trump/ (describing a new web browser, Brave, that is using Tor's anonymizing technology for its "private browsing" mode).

136. *See* Interview with Benjamin A. Powell, *supra* note 59.

137. *See, e.g.*, Roy F. Baumeister & Mark R. Leary, *The Need to Belong: Desire for Interpersonal Attachments as a Fundamental Human Motivation*, 117 PSYCHOL. BULL. 497, 522 (1995) (concluding that human beings have a strong desire for interpersonal attachments).

138. *See id.* at 520–21 (finding strong evidence of human desire to form social attachments, and that lack of belonging led to negative effects).

139. JAMES A. LEWIS ET AL., THE EFFECT OF ENCRYPTION ON LAWFUL ACCESS TO COMMUNICATIONS AND DATA 11 (2017), https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf; *Surveillance Self-Defense*, VPN, https://ssd.eff.org/en/glossary/vpn (last visited Sept. 8, 2019).

140. *See Tor FAQ: How is Tor Different from Other Proxies?*, *supra* note 133; *Surveillance Self-Defense*, *supra* note 139.

141. Kris, *supra* note 65, at 413.

on the access to certain Internet content that depends on IP addresses to filter users.[142]

Location-spoofing technologies like VPNs are much more common than anonymity technologies and are becoming more widely adopted. VPNs are more user-friendly than anonymity technologies and we may very well see a trend in the adoption of VPNs that mirrors the adoption of encryption technologies, which have increasingly become the default on many devices.[143] In the fourth quarter of 2016, a Global Web Index survey found that 30% of global Internet users stated that they used a VPN or proxy server when accessing the Internet, which was an increase from a Global Web Index survey in the first quarter of 2016 that found that nearly 25% of global Internet users stated that they used a VPN or proxy server when accessing the Internet.[144] A 2015 Global Web Index survey also found that 70% of VPN users reported using VPNs at least once a week.[145] The worldwide VPN market was expected to grow from $45 billion in 2014 to $70 billion in 2019.[146] This indicates that VPNs are becoming increasingly popular.[147]

Adversaries may specifically use location-spoofing technologies to hide their true locations. ISIS and al-Qaeda have advised their followers to use VPNs, and have even published detailed manuals to educate their followers about location-

---

142. *See id*.; Max Eddy, *The Best VPN Services of 2019*, PC MAGAZINE (Sept. 10, 2019, 11:25 AM), https://www.pcmag.com/article2/0,2817,2403388,00.asp; *Surveillance Self-Defense*, *supra* note 139.

143. *See* Eric Manpearl, *Preventing "Going Dark": A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate*, 28 U. FLA. J.L. & PUB. POL'Y 65, 72–73 (2017) (discussing the trend of widespread encryption adoption); *4 Reasons Behind VPN Apps Rising Popularity Among Mobile Users*, PC NEWS (July 27, 2016), http://www.pc-os.org/4-reasons-behind-vpn-apps-rising-popularity-among-mobile-users/; Telephone Interview with Michael Daniel, Former Special Assistant to the President & Cybersecurity Coordinator, White House (Feb. 6, 2018) (expecting VPNs to become widely used in the future); Telephone Interview with David S. Kris, Assistant Attorney Gen. for Nat'l Security, U.S. Dep't of Justice (Feb. 6, 2018) (highlighting the increased prevalence of VPNs); Telephone Interview with Nicholas Weaver, *supra* note 126 (acknowledging that VPNs are much more likely to be used than Tor).

144. Chase Buckle, *Turkey Leads for VPN Usage*, GLOB. WEB INDEX (Jan. 10, 2017), https://blog.globalwebindex.net/chart-of-the-day/turkey-leads-for-vpn-usage/; *see also Number of VPN Users in Selected Global Markets as of 2nd Quarter 2014 (in Millions)*, STATISTA (Sept. 17, 2014), https://www.statista.com/statistics/324982/vpn-users-countries/ (showing the number of VPN users as of the second quarter of 2014 in China, India, Brazil, Indonesia, Mexico, Vietnam, Argentina, Turkey, Thailand, and Saudi Arabia).

145. Katie Young, *1 in 4 VPN Users Accessing Daily*, GLOB. WEB INDEX (Feb. 17, 2016), https://blog.globalwebindex.net/chart-of-the-day/1-in-4-vpn-users-accessing-daily/.

146. *Size of the Virtual Private Network (VPN) Market Worldwide by Type in 2014 and 2019 (in Billion U.S. Dollars)*, STATISTA (Oct. 15, 2015), https://www.statista.com/statistics/542797/worldwide-virtual-private-network-market-by-type/.

147. *See* Thorin Klosowski, *Why is Everyone Talking About VPNs?*, LIFEHACKER (Mar. 29, 2017, 1:09 PM), https://lifehacker.com/why-is-everyone-talking-about-vpns-1793768312 (discussing the increased interest in VPNs).

spoofing technologies and encourage their followers to use VPNs.[148] Also, Russian actors working for the Internet Research Agency that engaged in active measures to meddle in United States politics and the 2016 presidential election "purchased space on computer servers located inside the United States in order to set up virtual private networks ('VPNs')" to make it appear as though they were located inside the United States to carry out their activities and influence operations.[149] These Russian actors "connected from Russia to the U.S.-based infrastructure by way of these VPNs and conducted activity inside the United States—including accessing online social media accounts, opening new accounts, and communicating with real U.S. persons—while masking the Russian origin and control of the activity."[150]

By masking the true location of the user, location-spoofing technologies like VPNs may hinder the NSA's ability to efficiently conduct SIGINT collection under Section 702 because location-spoofing technologies may cause problems for the NSA in making pre-tasking foreignness determinations and in conducting post-tasking analysis regarding an individual's location. These problems would be greatly exacerbated by the widespread adoption of location-spoofing technologies like VPNs.

Under Section 702, the NSA may only target non-United States persons that are reasonably believed to be outside the United States.[151] A potential target may consistently use VPN services that are located inside the United States. The potential target's IP address would appear to be the VPN server's IP address and indicate that the potential target was located wherever the VPN server is, instead of revealing the potential target's true IP address and actual location. If the VPN server is inside the United States, then the potential target will appear to be located inside the United States even if the potential target is really overseas. As discussed *supra*,[152] there will likely be many occasions when the information that leads analysts to determine that there is a valid foreign intelligence reason to target a person includes information about the person's citizenship and location, which would alleviate the difficulties arising from having to make a foreignness determination based solely on information that is transmitted using location-spoofing technologies, but this may not always be the case. The foreign intelligence purpose determination may not be based on the type of information

148. *See* ALKHOURI & KASSIRER, *supra* note 93, at 2–3 (finding that jihadists have sought to leverage Tor and VPNs to improve their Internet security and hide from intelligence and law enforcement agencies, and have encouraged fellow terrorists to adopt these technologies on jihadist web forums); BARTLETT & KRASODOMSKI-JONES, *supra* note 93, at 7–12; Zetter, *supra* note 93 (analyzing an ISIS operational security guide that advised followers on how to protect their communications and location data).

149. Indictment at para. 39, United States v. Internet Research Agency L.L.C., Case No. 1:18-cr-00032-DLF (D.D.C. Feb. 16, 2018), https://www.justice.gov/file/1035477/download.

150. *Id.*

151. 50 U.S.C. § 1881a.

152. *See supra* Part II.

that would allow analysts to make a foreignness determination from this information, and the NSA may not have any prior information regarding a potential new target in its databases to aid in the foreignness determination.[153] Further, NSA analysts are required to "exercise a standard of due diligence" in making the foreignness determination, and make "their determinations based on the totality of the circumstances."[154] The PCLOB has confirmed

> that this is not a "51% to 49% test." If there is conflicting information indicating whether a target is located in the United States or is a U.S. person, that conflict must be resolved and the user must be determined to be a non-U.S. person reasonably believed to be located outside the United States prior to targeting.[155]

This means that NSA analysts must be able to find enough information indicating that a potential target is actually located overseas to overcome the indication from the IP address, which is truly the IP address of the VPN server, that a potential target is located inside the United States based on the totality of the circumstances. If a significant number of potential targets use location-spoofing technologies like VPNs as part of their tradecraft to try to avoid surveillance, this could require NSA analysts to expend a great deal of effort to uncover that a potential target is indeed located overseas. This would limit analysts' ability to engage in their other important intelligence work as foreignness determinations would take longer, and would cause delays in targeting, which means that there would be delays in the ability to actually collect important intelligence on these targets.[156] Delays in collection could have severe consequences when trying to understand fast-moving and dynamic threats, such as terrorist organizations.[157] Also, this may lead to instances in

---

153. *See* NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 3.

154. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 117.

155. PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 44; *see also* PCLOB, TRANSCRIPT OF PUBLIC HEARING, *supra* note 42, at 40–43 (explaining that there is not a 51% rule and that the foreignness determination must be based on the totality of the circumstances); NAT'L SEC. AGENCY, NSA DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 4 (2014), https://www.nsa.gov/about/civil-liberties/reports/assets/files/nsa_report_on_section_702_program.pdf [hereinafter NSA'S IMPLEMENTATION OF FISA § 702]. When identifying and tasking a selector,

> If the analyst discovers any information indicating the targeted person may be located in the U.S. or that the target may be a U.S. person, such information must be considered. In other words, if there is conflicting information about the location of the person or the status of the person as a non-U.S. person, that conflict must be resolved before targeting can occur.

NSA'S IMPLEMENTATION OF FISA § 702, at 4.

156. Kris, *supra* note 65, at 416.

157. *See* Frank J. Cilluffo & Daniel Rankin, *Combating New Security Threats: Fighting Terrorism*, NATO REVIEW, https://www.nato.int/docu/review/2001/Combating-New-Security-

which the NSA cannot resolve the conflict and adequately determine that the potential target is reasonably believed to be outside the United States even though in reality the potential target is a non-United States person overseas because the potential target is using tradecraft to hide the person's true identity and location and using VPNs located inside the United States.[158]

Location-spoofing technologies may also cause especially significant problems for the NSA in post-tasking analysis. NSA analysts must review information to determine whether there is any indication that a target is a United States person, has entered the United States, or intends to enter the United States.[159] When a target uses a VPN that is located inside the United States, the target's IP address may appear to be located inside the United States even if the target remains overseas.[160] If the NSA is heavily dependent on IP addresses to determine location, the use of location-spoofing technologies like VPNs could result in analysts having to spend significant amount of time trying to resolve the conflicting information about the location of the target between the time the person was first targeted and the current information acquired after the person began using the VPN.[161] This could create a major resource problem for the NSA if there is widespread use of location-spoofing technologies like VPNs given the scale of SIGINT collection under Section 702, which had more than 164,000 targets in 2018.[162]

Further, this could result in the NSA having to detask targets when analysts cannot resolve the conflicting information and believe the target has entered the

---

Threats/Fighting-terrorism/EN/index.htm (last visited Sept. 8, 2019) (describing the dynamic nature of the threat from terrorism).

158. *Cf.* Interview with Carrie F. Cordero, Former Senior Assoc. Gen. Counsel, Office of the Dir. of Nat'l Intelligence, Former Counsel to the Assistant Att'y Gen. for Nat'l Sec., U.S. Dep't of Justice, in D.C. (Feb. 12, 2018) (stating that conflicting information regarding a potential target's location or United States person status may result from the use of technologies like VPNs, and that there may be instances in which the NSA cannot resolve the conflict).

159. NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 6–8.

160. Kris, *supra* note 65, at 413.

161. *See* NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 2 (noting the NSA has specifically used an Internet Protocol (IP) filter with at least upstream collection to limit acquisition "to Internet transactions that originate and/or terminate outside the United States"); Kris, *supra* note 65, at 414; Interview with Benjamin Wittes, Senior Fellow, Brookings Inst., Co-Founder & Editor-in-Chief, Lawfare, in D.C. (Feb. 13, 2018) (stating that there may be a problem for the NSA if a target starts using a VPN for the first time after the person has already been targeted and is the subject of ongoing collection after having been initially deemed to be reasonably believed to be outside the United States because the VPN may make it look like the person has travelled from outside the United States to inside the United States, which creates a burden on the NSA analyst to determine if the person indeed entered the United States or not).

162. Kris, *supra* note 65, at 416; Interview with Benjamin Wittes, *supra* note 161; DNI, TRANSPARENCY REPORT 2018, *supra* note 4, at 13; Telephone Interview with David S. Kris, *supra* note 143.

United States.[163] In an increasingly globalized world where a growing number of people travel and use mobile communications devices, it is quite believable that a target could have entered the United States.[164] As discussed *supra*,[165] although the NSA may notify the FBI that a target has appeared to enter the United States so that the FBI may seek a traditional FISA Title I order or take other lawful investigative steps, there may not be enough information to establish probable cause that the target is an agent of a foreign power to obtain a FISA Title I order, or "probable cause for belief that an individual is committing, has committed, or is about to commit" an enumerated crime to obtain a court order to intercept wire, oral, and electronic communications under Title III.[166] This means that the Intelligence Community could lose the ability to collect on the target. Even if there is enough information to obtain probable cause under one of these legal mechanisms, it requires significant resources and time to put together sufficient FISA Title I and Title III applications.[167] Thus, trying to establish probable cause on a significant number of targets that all of the sudden appear to be located within the United States after originally appearing to be overseas when they were first targeted would take way from other important national security missions and cause delays in intelligence collection. Even though the target may be re-tasked if the NSA develops a reasonable belief that the person is outside the United States at a later point in time and the NSA continues to believe that the person possesses or is likely to communicate foreign intelligence information, there will be a gap in collection between the time the target was detasked and re-tasked despite the fact that the person may have been a legitimate target outside the United States the entire time.[168]

C. The Reduction in the United States' Home Field Advantage

The United States' home field advantage in conducting SIGINT collection is diminishing. The Internet is rapidly expanding with more users and data being

163. Kris, *supra* note 65, at 414; *see* NSA, TARGETING PROCEDURES 2017, *supra* note 37, at 2, 7 (noting the NSA has specifically used an IP filter with at least upstream collection to limit acquisition "to Internet transactions that originate and/or terminate outside the United States" and "[i]f the NSA determines that a target has entered the United States" then the NSA must terminate acquisition from the target without delay).

164. Kris, *supra* note 65, at 414.

165. *See supra* Part I.C.

166. 18 U.S.C. § 2518(3)(a) (2012); 50 U.S.C. § 1805(a); NSA, MINIMIZATION PROCEDURES 2018, *supra* note 52, at 12; NSA, TARGETING PROCEDURES 2017, *supra* note 41, at 4; PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 50.

167. *See, e.g.*, OEO, ELECTRONIC SURVEILLANCE MANUAL, *supra* note 125, at 1–7 (describing the Title III wiretap application process); Roberts, *supra* note 17 (quoting former Director of National Intelligence (DNI) Admiral Mike McConnell as stating "[i]t takes about 200 man hours to do [a FISA application for] one telephone number").

168. Interview with Carrie F. Cordero, *supra* note 158; Telephone Interview with David S. Kris, *supra* note 143.

transmitted.[169] In August 2001, just before the September 11 terrorist attacks, the Internet had 513 million users, which constituted 8.6% of the world's population.[170] In December 2019, the Internet had about 4.574 billion users, which constituted 58.7% of the world's population.[171] As Internet growth has occurred, more transmission facilities have been built and are being planned, such as Internet exchange points that transmit local Asian and European traffic and undersea communications cables.[172] For example, Brazil and the European Union have agreed to lay an undersea cable for communications that would connect South America directly to Europe, which would reduce reliance on fiber-optic cables that transit the United States.[173] This agreement was motivated at least in part by the desire to try to avoid U.S. SIGINT activities that were revealed by Edward Snowden.[174] It has been estimated that while 80% of the world's telecommunications traffic transited United States-based routers prior to 2001, only about 20% of the world's telecommunications traffic transited the United States by 2010.[175] Regardless of whether this specific estimate is accurate, there is a very real trend that a smaller share of the world's communications are transiting the United States, which reduces the United States' home field advantage and therefore diminishes the fruitfulness of SIGINT acquired through the programs under Section 702.[176]

This trend may be exacerbated by a push for data localization laws. Numerous countries have considered or enacted data localization rules "that limit the storage, movement, and/or processing of data to specific geographies and

169. Kris, *supra* note 65, at 416.

170. *Internet Growth Statistics*, INTERNET WORLD STATS, https://www.internetworldstats.com/emarketing.htm (last visited Sept. 8, 2019).

171. *Id.*; *Internet Usage Statistics*, INTERNET WORLD STATS, https://www.internetworldstats.com/stats.htm (last visited Mar. 30, 2020).

172. Chris Bryant, *Spying Questions Emerge Over Frankfurt's Data Hub*, FIN. TIMES (July 4, 2013), https://www.ft.com/content/a3e573ce-e3fd-11e2-91a3-00144feabdc0; Jeff Hecht, *The Bandwidth Bottleneck that is Throttling the Internet*, SCI. AM.: THE NATURE MAGAZINE (Aug. 10, 2016), https://www.scientificamerican.com/article/the-bandwidth-bottleneck-that-is-throttling-the-internet/; Kris, *supra* note 65, at 416; Ryan Singel, *NSA's Lucky Break: How the U.S. Became Switchboard to the World*, WIRED (Oct. 10, 2007, 2:00 PM), https://www.wired.com/207/10/nsas-lucky-break-how-the-u-s-became-switchboard-to-the-world/.

173. Robin Emmott, *Brazil, Europe Plan Undersea Cable to Skirt U.S. Spying*, REUTERS (Feb. 24, 2014, 6:52 AM), https://www.reuters.com/article/us-eu-brazil/brazil-europe-plan-undersea-cable-to-skirt-u-s-spying-idUSBREA1N0PL20140224; John Tibbles, *Submarine Cables, Security and the State*, SUBMARINE TELECOMS FORUM, May 2017, at 23, 29.

174. Emmott, *supra* note 173; *Spain, Brazil Plan Subsea Fiber Optic Cable by 2019*, REUTERS (Apr. 24, 2017, 8:02 PM), https://www.reuters.com/article/spain-brazil-telecoms/spain-brazil-plan-subsea-fiber-optic-cable-by-2019-idUSL1N1HW1VO.

175. Marc Ambinder, *How the U.S. Lost its Home Field Surveillance Advantage*, ATL. (Feb. 6, 2010), https://www.theatlantic.com/politics/archive/2010/02/how-the-us-lost-its-home-field-surveillance-advantage/35495/.

176. Kris, *supra* note 65, at 417.

jurisdictions, or [would] limit the companies that can manage data based upon the company's nation of incorporation or principal situs of operations and management."[177] Some authoritarian governments, such as China and Russia, have pursued data localization laws as a way to control the information that is available to citizens and to monitor their citizens' online activities.[178] China famously restricts access to certain websites and Internet services with the "Great Firewall," and limits cross-border data transfers.[179] China has enacted numerous laws and issued rules to store data regarding credit information, personal information, health information, and business information locally; require servers used for an array of publishing services such as "app stores, audio and video distribution platforms, online literature databases, and online gaming" to be located inside China; and try to exclude foreign technology firms from offering cloud-computing services in China.[180] Russia has also enacted requirements for the personal data of Russian citizens to be stored in databases located inside of Russia, and for telecommunications providers and ISPs to store the content and metadata of communications for specific periods of time within Russia.[181]

Recently, democratic countries have also started to push for data localization. Although officials in numerous countries have advocated for data localization

177. Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders*, *in* 3 LAWFARE RESEARCH PAPER SERIES 1, 3 (2014) (analyzing the recent data localization movement and the motivations behind this trend); Myriam Gufflet, *French Senate Proposes Data Localization*, INT'L ASS'N OF PRIVACY PROF'LS (May 12, 2016), https://iapp.org/news/a/french-senate-proposes-data-localization/ (discussing a proposal that was made in the French Senate in May 2016 to require personal data to be stored in the European Union and to prohibit the transfer of personal data to a non-European Union third country); 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 (reporting that Germany, among other countries, has "consider[ed] legislation that would make it costly or even technically impossible for American tech companies to operate inside their borders"); Sam Ball, *Plans to Stop U.S. Spying with European Internet*, FRANCE24 (Feb. 18, 2014, 12:04 PM), http://www.france24.com/en/20140217-european-internet-plans-nsa-spying (revealing that France and Germany have discussed creating a European communications network to enable Europeans to send and receive emails and other data without having the information pass through United States networks and servers).

178. NIGEL CORY, INFO. TECH. & INNOVATION FOUND., CROSS-BORDER DATA FLOWS: WHERE ARE THE BARRIERS, AND WHAT DO THEY COST? 21–22, 28 (May 2017) http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.50788009.1438585138.1567354975-134080276.1567354975; Hill, *supra* note 177, at 3.

179. CORY, *supra* note 178, at 21–22.

180. *Id.*

181. *Id.* at 28; Ksenia Koroleva, *"Yarovaya" Law–New Data Retention Obligations for Telecom Providers and Arrangers in Russia*, GLOB. PRIVACY & SEC. COMPLIANCE LAW BLOG (July 29, 2016), https://www.globalprivacyblog.com/privacy/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/.

by claiming that such policies would better protect privacy in the aftermath of the Snowden disclosures, the trend towards data localization seems to be primarily motivated by the desire "to protect domestic businesses from foreign competition, [and] to support domestic intelligence and law enforcement ambitions."[182] United States technology companies have dominated the global market, and some European business leaders and politicians appear to have taken advantage of the Snowden disclosures and public outcry to promote domestic businesses and enable domestic technology companies to garner greater market share to the detriment of United States companies by portraying United States companies as untrustworthy because of their (lawful and compelled) cooperation with the NSA.[183]

For example, shortly after the initial Snowden disclosures in summer 2013, the German Interior Minister, Hans-Peter Friedrich, stated that "whoever fears their communication is being intercepted in any way should use services that don't go through American servers."[184] In 2014, German Chancellor Angela Merkel suggested that Europe should improve and develop its own Internet infrastructure so that Germany could keep its data inside Europe instead of having it transit the United States.[185] Chancellor Merkel informed the German public that she would work with other European leaders to "discuss which European providers . . . offer security for our citizens . . . [s]o that you don't have to go across the Atlantic with emails and other things, but can build up communications networks also within Europe."[186] The German government terminated its contract with Verizon in June 2014 and announced that it would end all business with Verizon by 2015, largely as a result of Verizon having been implicated in the NSA's SIGINT collection activities.[187] A German telecommunications company, Deutsche Telekom, then received the contract

182. Hill, *supra* note 177, at 22.

183. *See* Kristin Stoller, *The World's Largest Tech Companies 2017: Apple and Samsung Lead, Facebook Rises*, FORBES (May 24, 2017, 7:00 AM), https://www.forbes.com/sites/kristinstoller/2017/05/24/the-worlds-largest-tech-companies-2017-apple-and-samsung-lead-facebook-rises/#e3425ead140d (showing that United States technology companies have become the largest companies in the world and detailing the prominence of United States technology products and services).

184. *German Minister: Drop Google if You Fear US Spying*, U.S. NEWS & WORLD REPORT (July 3, 2013), https://www.usnews.com/news/technology/articles/2013/07/03/german-minister-drop-google-if-you-fear-us-spying.

185. Alison Smale, *Merkel Backs Return to Keep European Data in Europe*, N.Y. TIMES (Feb. 16, 2014), https://www.nytimes.com/2014/02/17/world/europe/merkel-backs-plan-to-keep-european-data-in-europe.html.

186. *Id.*

187. ADAM SEGAL, THE HACKED WORLD ORDER: HOW NATIONS FIGHT, TRADE, MANEUVER, AND MANIPULATE IN THE DIGITAL AGE 155 (2016); Aaron Mamiit, *German Government Drops Verizon Contract in Fear of U.S. Espionage*, TECH TIMES (June 27, 2014, 9:11 AM), http://www.techtimes.com/articles/9292/20140627/german-government-drops-verizon-contract-in-fear-of-u-s-espionage.htm.

that had been terminated with Verizon by the German government.[188] Germany also enacted legislation in 2016 to require telecommunications providers to retain metadata for specific periods of time and store that metadata in servers located in Germany to improve law enforcement effectiveness, but a German regulator suspended enforcement of the data retention provisions in June 2017 just before the new law was to go into effect because of litigation over whether the law complies with European Union law.[189]

France has considered data localization rules that may actually be driven by the country's national economic interests, too. France's former Minister for Small and Medium-Sized Enterprises, Innovation and the Digital Economy, Fleur Pellerin, declared that it was necessary "to locate datacentres and servers in [French] national territory in order to better ensure data security."[190] France has sought to promote French data centers and has stated that it is illegal to use a non-"sovereign" cloud, which is a foreign cloud provider, for data produced by national or local governments to ensure that government data is stored and processed inside of France.[191]

In addition, Brazil has considered data localization rules as a way to promote its own domestic technology sector. Former Brazilian President Dilma Rousseff

---

188. SEGAL, *supra* note 187, at 155; Mamiit, *supra* note 187.

189. Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten [VerkdHSpFruSpPflEG] [Draft Act Introducing a Storage Obligation and a Maximum Storage Retention Period for Traffic Data], Dec. 10, 2015, BUNDESGESETZBLATT, Teil I [BGBL I] at 2218 (Ger.), https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s2218.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s2218.pdf%27%5D__1584838685166 [http://perma.cc/XZK2-Y7D5]; *Free Flow of Data is at the Essence of a True European Digital Single Market*, BUS. EUR. (Nov. 29, 2016), https://www.businesseurope.eu/sites/buseur/files/media/public_letters/imco/2016-11-29_ffd_joint_statement.pdf [hereinafter *Free Flow of Data*]; Joachim Scherer & Caroline Heinickel, *German Data Retention Obligations Suspended*, GLOB. COMPLIANCE NEWS (July 12, 2017), https://www.bakermckenzie.com/en/insight/publications/2017/07/german-data-retention/; Mirko Hohmann, *German Bundestag Passes New Data Retention Law*, LAWFARE (Oct. 16, 2015, 3:40 PM), https://lawfareblog.com/german-bundestag-passes-new-data-retention-law; Maria Sheahan, *German Regulator Suspends Law on Storing Phone and Internet Data*, U.S. NEWS (June 28, 2017), https://www.usnews.com/news/technology/articles/2017-06-28/german-regulator-suspends-law-on-storing-phone-and-internet-data; *Verkehrsdatenspeicherung*, BUNDESNETZAGENTUR (June 28, 2017), https://www.bundesnetzagentur.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Anbieterpflichten/OeffentlicheSicherheit/Umsetzung110TKG/VDS_113aTKG/VDS-node.html.

190. Valéry Marchive, *France Hopes to Turn PRISM Worries into Cloud Opportunities*, ZDNET (June 21, 2013, 9:02 AM), http://www.zdnet.com/article/france-hopes-to-turn-prism-worries-into-cloud-opportunities/.

191. *Free Flow of Data*, *supra* note 189; MINISTÈRE DE LA CULTURA ET DE LA COMMUNICATION, NOTE D'INFORMATION DU 5 AVRIL 2016 RELATIVE À L'INFORMATIQUE EN NUAGE (CLOUD COMPUTING) 1–3 (2016), https://francearchives.fr/file/f7ace4517613a246583fd2dd673a0e6d0f86c039/static_9151.pdf.

had long championed policy initiatives to increase the number of Internet exchange points and increase domestic Internet bandwidth, improve connectivity (in part by building undersea cables and overland fiber-optic cables), encourage Internet content providers to be based in Brazil, and promote the use of domestically produced telecommunications equipment.[192] Following the Snowden disclosures, the Brazilian government announced plans in to abandon its Microsoft Outlook email services, which are from a foreign United States-based provider, and move to a domestic email service that uses data centers inside Brazil.[193] Brazil considered requiring Internet companies to store copies of Brazilian citizens' data in data servers inside Brazil as part of Brazil's Marco Civil da Internet legislation to enable "greater access for Brazilian law enforcement to data stored abroad or belonging to foreign companies," but ultimately removed this provision prior to the legislation being passed.[194] The final law did include a provision that "extends the reach of Brazilian law to any Internet service in the world with Brazilian users," which means that "[a] firm based in the United States whose services are used by Brazilians could, for example, be penalized for adhering to its domestic data-disclosure laws if they conflict with Brazil's."[195] If Brazil aggressively enforces these rules or once again pursues data localization legislation, United States technology companies may find it too costly to continue offering their services and products in Brazil.

These data localization rules create barriers to cross-border data flows and threaten to reduce the ability of United States technology companies to do business overseas. Governments at times seek to use data localization laws to force companies to move data-related jobs to their countries in an effort to help the domestic economies.[196] Governments also promote these rules to protect and promote domestic companies by making it more costly for foreign firms to

---

192. Bill Woodcock, *On Internet, Brazil is Beating U.S. at its Own Game*, AL JAZEERA AM. (Sept. 20, 2013, 2 :45 PM), http://america.aljazeera.com/articles/2013/9/20/brazil-internet-dilmarousseffnsa.html.

193. Hill, *supra* note 177, at 17–18; Angelica Mari, *Brazilian Government to Ditch Microsoft in Favour of Bespoke Email System*, ZDNET (Oct. 14, 2013, 6:13 PM), http://www.zdnet.com/article/brazilian-government-to-ditch-microsoft-in-favour-of-bespoke-email-system/; Miller, *supra* note 177.

194. Hill, *supra* note 177, at 17–18; *see* Anthony Boadle, *Brazil to Drop Local Data Storage Rule in Internet Bill*, REUTERS (Mar. 18, 2014, 11:25 PM), https://www.reuters.com/article/us-brazil-internet/brazil-to-drop-local-data-storage-rule-in-internet-bill-idUSBREA2I03O20140319.

195. Hill, *supra* note 177, at 18.

196. CORY, *supra* note 178, at 5. Nigel Cory has found that

> [t]hese supposed benefits of data-localization policies are misunderstood. Data centers have become more automated, meaning that the number of jobs associated with each facility, especially for technical staff, has decreased. While data centers contain expensive hardware (which is usually imported) and create some temporary construction jobs, they employ relatively few full-time staff.

Id.

do business in their countries.[197] The push for data localization could diminish United States companies' market share by reducing their competitiveness abroad, which would aggravate the trend towards a smaller percentage of the world's communications transiting the United States because of the growth of the Internet. Thus, the United States' home field advantage will likely recede in the future and the advantages in the Intelligence Community's ability to acquire SIGINT through the programs under Section 702 will be diminished.

D. Companies No Longer Cooperating with the Government

SIGINT collection under Section 702 is heavily dependent on a small number of technology companies that have become less cooperative in the post-Snowden environment.[198] Following the September 11 terrorist attacks, technology companies voluntarily aided the government's surveillance programs described in Part I prior to the passage of the PAA and FAA.[199] However, the relationship between the government and technology companies has fractured in recent years, most notably as a result of the Snowden disclosures. Foreign consumers were extremely alarmed by the disclosures, which described United States technology companies' (lawful and compelled) cooperation with the NSA.[200] Thus, foreign consumers became distrustful of American products and online services because they feared that their communications would become accessible to United States law enforcement or intelligence agencies.[201] United States technology companies lost between $35 and $180 billion in revenue over the three-year period following the Snowden disclosures.[202] This increased the

197. *Id.* at 6–7.

198. Interview with Benjamin Wittes, *supra* note 161; Rozenshtein, *supra* note 67, at 112–16.

199. S. REP. NO. 110-209, at 7; CHARLIE SAVAGE, POWER WARS: INSIDE OBAMA'S POST-9/11 PRESIDENCY 183–87 (2015); Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 910–13 (2008).

200. Miller, *supra* note 177.

201. *See, e.g.*, *id.* (discussing the increased skepticism by foreign consumers of United States technology products and services following the Snowden disclosures); Nicholas Weaver, *Band-Aids Can't Fix Bullet Holes: Silicon Valley and the NSA*, LAWFARE (Sept. 30, 2015, 3:55 PM), https://www.lawfareblog.com/band-aids-cant-fix-bullet-holes-silicon-valley-and-nsa ("Silicon Valley can't operate without the trust of their customers, and trust, once lost, is hard to regain. The bad blood will remain for years.").

202. DANIEL CASTRO, THE INFO. TECH. & INNOVATION FOUND., HOW MUCH WILL PRISM COST THE U.S. CLOUD COMPUTING INDUSTRY? 3 (2013), http://www2.itif.org/2013-cloud-computing-costs.pdf (calculating that United States technology companies would lose up to $35 billion between 2013–2016 following Snowden's unauthorized disclosures about the NSA's intelligence programs) (last visited Mar. 16, 2020); James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, FORRESTER (Aug. 15, 2013, 11:02 AM), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects (estimating that United States technology companies could lose up to $180 billion between 2013–2016 because of disclosures about NSA programs).

incentive for these technology companies to adopt a more publicly adversarial relationship with the United States government.[203]

There is also a significant ideological and cultural divide between many leaders in the technology industry and the government, which adds to the friction and desire on the part of technology companies to resist government surveillance. Professor Amy Zegart has described the "yawning cultural divide between policymakers in Washington and engineers in Silicon Valley tech companies" as the "suit-hoodie divide."[204] Many technology leaders have more libertarian political beliefs than those in government and some are even ideologically inclined to thwart surveillance efforts.[205] These major technology companies are also multinational corporations with significant global customer bases, and thus often view themselves as global enterprises that are not necessarily predisposed to serve the United States government's interests.

Technology companies have the ability to innovate in a manner that can frustrate government SIGINT collection efforts.[206] Service providers are increasingly offering encryption by default, especially end-to-end encryption.[207]

---

203. Rozenshtein, *supra* note 67, at 115–22.

204. Amy Zegart, *Policymakers Are From Mars, Tech Company Engineers Are From Venus*, LAWFARE (June 6, 2016, 9:54 AM), https://www.lawfareblog.com/policymakers-are-mars-tech-company-engineers-are-venus; *see* Univ. of Tex. at Austin, *Weapons of Mass Deception: The Changing Cyber Landscape*, STRAUSS CTR. (Mar. 27, 2018, 12:15 PM), https://www.strausscenter.org/event/518-a-conversation-with-amy-zegart.html.

205. *See* Rozenshtein, *supra* note 67, at 118 (characterizing many technologists as subscribing to the "Californian Ideology," which is a "worldview that is simultaneously countercultural in lifestyle, laissez-faire in economics, and libertarian in politics"); PETER SWIRE, NEW AM., THE DECLINING HALF-LIFE OF SECRETS: AND THE FUTURE OF SIGNALS AND INTELLIGENCE 4 (2015), https://static.newamerica.org/attachments/4425-the-declining-half-life-of-secrets/Swire_DecliningHalf-LifeOfSecrets.f8ba7c96a6c049108dfa85b5f79024d8.pdf (describing an anti-secrecy and libertarian culture among technologists); Andy Greenberg, *Meet Moxie Marlinspike, The Anarchist Bringing Encryption to All of Us*, WIRED (July 31, 2016, 6:45 AM), https://www.wired.com/2016/07/meet-moxie-marlinspike-anarchist-bringing-encryption-us/ (discussing Moxie Marlinspike's, a security researcher who developed Signal and helped encrypt WhatsApp, advocacy of encryption and Marlinspike's belief that people should be able to use encryption to break the law because this may inspire social change in some areas); Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016, 11:08 AM), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/ (observing that it is "an article of faith that's commonly held among Silicon Valley engineers" that "online privacy must be protected against surveillance of all kinds" and that "[i]n Silicon Valley, strong encryption isn't really up for debate [since] [a]mong tech's most powerful leaders, it's orthodoxy").

206. *See* Rozenshtein, *supra* note 67, at 134–35 (referring to technology companies' ability to innovate in this way as "technological unilateralism").

207. *See* CHERTOFF GROUP, THE GROUND TRUTH ABOUT ENCRYPTION 1 (2016) https://cdn2.hubspot.net/hubfs/3821841/docs/238024-282765.groundtruth.pdf (observing that users formerly had to take affirmative action to use encryption, but now more devices and products encrypt data by default unless the user takes affirmative action turn this function off); Telephone Interview with Timothy Edgar, Former Dir. of Privacy & Civil Liberties, Nat'l Sec. Council Staff, Former

These products encrypt data and communications in such a way that the service provider does not have the technical ability to decrypt the information.[208] End-to-end encryption improves the security of these products against malicious actors and allows companies to signal that they value customer privacy.[209] Providers that offer unbreakable end-to-end encryption cannot respond to lawful orders under Section 702 with useful information because they do not possess the decrypted information that the government is requesting.[210] In 2016, WhatsApp, an online messaging service on smartphones that is now owned by Facebook, implemented end-to-end encryption to its service, which is used by more than two billion people.[211]

Some have questioned whether end-to-end encryption will be widely adopted by the technology industry because it conflicts with many companies' business models.[212] Many technology companies rely on advertising revenue to subsidize free content and services, and advertising is very dependent on user data to produce targeted advertisements.[213] End-to-end encryption would reduce companies' access to useful user information, which means that companies could risk losing revenue if they employed end-to-end encryption.[214] Access to consumer data can also enhance a product or service's security because this can

---

Nat'l Sec. Counsel, Am. Civil Liberties Union (Feb. 20, 2018) (noting that many companies have begun using encryption to protect users' information); Manpearl, *supra* note 143, at 72 (explaining that "the burden of action formerly favored not using encryption," but it will now favor using encryption because it is often the default setting, and that this will greatly increase the prevalence of at least endpoint encryption).

208. CHERTOFF GROUP, *supra* note 207, at 1.

209. *See* HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS 10 (July 6, 2015) https://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf (arguing against a lawful access requirement because of cybersecurity concerns); Rozenshtein, *supra* note 67, at 138 (stating that companies may use end-to-end encryption to demonstrate that they take user privacy seriously).

210. CHERTOFF GROUP, *supra* note 207, at 1; Manpearl, *supra* note 143, at 72–73; Interview with Robert S. Litt, Former Gen. Counsel, Office of the Dir. of Nat'l Intelligence, in D.C. (Feb. 14, 2018).

211. Andy Greenberg, *WhatsApp Just Switched on End-to-End Encryption for Hundreds of Millions of Users*, WIRED (Nov. 18, 2014, 10:54 AM), https://www.wired.com/2014/11/whatsapp-encrypted-messaging/; Metz, *supra* note 205; *Two Billion Users—Connecting the World Privately*, WHATSAPP (Feb. 12, 2020), https://blog.whatsapp.com/two-billion-users-connecting-the-world-privately.

212. MATTHEW G. OLSEN ET AL., BERKMAN CTR. FOR INTERNET & SOC'Y, DON'T PANIC: MAKING PROGRESS ON THE "GOING DARK" DEBATE 10–12 (2016) https://dash.harvard.edu/bitstream/handle/1/28552576/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf?sequence=1&isAllowed=y.

213. *Id.* at 10–11.

214. *Id.*

allow the company to scan for malware, which would not be possible with end-to-end encryption.[215]

However, the Office of the Director of National Intelligence (ODNI) insists that end-to-end encryption poses a significant problem.[216] ODNI believes that there is already a trend developing of companies implementing end-to-end encryption and United States adversaries using these tools to avoid surveillance.[217] Also, in the aftermath of the NSA announcing the voluntary termination of "about" collection, Julian Sanchez, a senior fellow at the Cato Institute, and Nicholas Weaver, a senior researcher at the International Computer Science Institute and professor in computer science at the University of California Berkley, speculated that the increasing prevalence of encryption of email traffic between servers made it more difficult to scan the contents of email during transit and therefore made "about" collection less useful to the NSA.[218] Nicholas Weaver has even stated that "upstream is dying . . . because everything is getting encrypted."[219]

Further, multinational technology companies have global infrastructure and are building data centers around the world, which enables them to store data overseas.[220] Companies have legitimate business reasons to store data overseas because some foreign customers may prefer having their data be physically located in their own countries and storing a user's data near the physical location of that user may enhance the quality of service.[221] Storing data overseas may

---

215. *See Privacy Policy*, GOOGLE (Mar. 31, 2020), https://www.gstatic.com/policies/privacy/pdf/20200331/acec359e/google_privacy_policy_en_us.pdf (explaining that Google's systems analyze user content, including emails, to provide relevant product features, such as customized search results, tailored advertising, and spam and malware detection) (last visited Apr. 8, 2020); Andy Greenberg, *After 3 Years, Why Gmail's End-to-End Encryption is Still Vapor*, WIRED (Feb. 28, 2017, 11:27 AM), https://www.wired.com/2017/02/3-years-gmails-end-end-encryption-still-vapor/ (acknowledging that end-to-end encryption would make Gmail's spam and malware filtering functions much more difficult).

216. *See* Letter from Deirdre M. Walsh, Chief Operating Officer, Office of the Dir. of Nat'l Intelligence, to Sen. Ron Wyden 1–2 (May 5, 2016) https://www.wyden.senate.gov/download/?id=3F716160-095E-420E-93F3-849453EB61B2&download=1 (asserting that the increased prevalence of encryption has already hampered law enforcement and intelligence collection activities and that the problem is only growing).

217. *Id.*

218. Adam Klein, *The End of "About" Collection Under Section 702*, LAWFARE (May 1, 2017, 10:07 AM), https://www.lawfareblog.com/end-about-collection-under-section-702; Julian Sanchez, *All About "About" Collection*, JUST SEC. (Apr. 28, 2017), https://www.justsecurity.org/40384/ado-about/; Telephone Interview with Nicholas Weaver, *supra* note 126.

219. Telephone Interview with Nicholas Weaver, *supra* note 126.

220. Mark Scott, *U.S. Tech Giants are Investing Billions to Keep Data in Europe*, N.Y. TIMES (Oct. 3, 2016), https://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html.

221. In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014), *rev'd and remanded sub nom.* In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. (In re Microsoft),

make it more difficult for the government to access the data because Section 702 may not empower the government to compel data that is stored overseas.[222] Companies that see a business advantage in opposing government SIGINT collection efforts or have an ideological reason for doing so may be driven to intentionally configure their data storage architecture to have data be stored outside the United States such that the government cannot obtain such information under Section 702. Although the NSA would not have the same difficulties that law enforcement has had in obtaining data stored overseas because the NSA could utilize Executive Order 12333 collection to obtain such information, as discussed *supra* in Part I.C, Section 702 offers unique advantages that Executive Order 12333 lacks so this shift could potentially diminish the quality of intelligence that the NSA could collect.[223]

The government is now extremely dependent on technology companies to facilitate SIGINT collection under Section 702, which means that these private firms wield tremendous power.[224] As Professor Alan Rozenshtein has observed, this is a stark example of "private actors wielding public power: when, by virtue of their opposition to a core government activity, they challenge traditional conceptions of state sovereignty and thereby transform into 'supercitizens.'"[225]

---

829 F.3d 197 (2d Cir. 2016) (stating that "because the quality of service decreases the farther a user is from the datacenter where his account is hosted, efforts are made to assign each account to the closest datacenter"), *vacated and remanded sub nom*. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018); Rozenshtein, *supra* note 67, at 140–41, 143 (asserting that "companies routinely leave the decision where to store data to users, allowing them to forum shop with the ease of a drop-down menu" and that "Microsoft's network may run more efficiently if it can store data physically near the data's user, or even dynamically shift data around the network depending on network congestion"); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 761 (2016) (explaining that data is typically stored close to the user).

222. *See In re Microsoft*, 829 F.3d at 211–22 (concluding that Congress did not intend for the Stored Communications Act's (SCA) warrant provision to apply extraterritorially, and therefore an SCA warrant could not lawfully compel a United States-based service provider, Microsoft, to seize the contents of its customer's communications stored abroad in Ireland), *vacated and remanded sub nom.* Microsoft Corp., 138 S. Ct. at 1186.

223. *See supra* Part I.C.

224. *See* David S. Kris, *Modernizing the Foreign Intelligence Surveillance Act: Progress to Date and Work Still to Come*, *in* LEGISLATING THE WAR ON TERROR 217, 227 (Benjamin Wittes ed., 2009). In 2008, Ken Wainstein, then-Assistant Attorney General for National Security in the Department of Justice, described the government's reliance on technology companies to facilitate surveillance:

> [W]e rely on the communications providers to do our intelligence surveillances. We can't do [the surveillances] without them because . . . we . . . don't own the communications systems. We need to rely on their assistance. . . . Yes, we can compel the phone companies, or compel the communications providers to do a surveillance, and even if they . . . resist a directive . . . we can go to the FISA Court to get our orders enforced. Problem is, throughout that time, we're dark on whatever surveillance it is that we want to go up on.

Id.

225. Rozenshtein, *supra* note 67, at 187.

The relationship between the government and technology companies has become more adversarial in the aftermath of Snowden's unauthorized disclosures. Technology companies have sought to regain consumers' confidence, especially foreign consumers, by innovating technologically in a manner that reduces their capability to respond to lawful orders.[226] The widespread adoption of encryption technologies and possible shift to storing data overseas to avoid complying with lawful surveillance orders may severely diminish the Intelligence Community's ability to conduct fruitful SIGINT under Section 702.

III. STRATEGIES TO ADDRESS THE DIFFICULTIES IN ACCURATELY DETERMINING LOCATION

The United States' current legal regime governing SIGINT activities is predicated on the location of the target. If location becomes significantly more difficult to determine because of the increased prevalence and advancement of location-spoofing and anonymity technologies, the United States may have to reconsider how location should factor into this legal paradigm.

A. Fourth Amendment Doctrine and the Difficulty in Determining Location

The Fourth Amendment is territorial in nature and a person's connections to the United States dictate whether the individual is protected under the Fourth Amendment. Social contract theory pervaded American political philosophy prior to the Constitution, and the United States Constitution was drafted as a social contract between the American people and the United States government.[227] The social compact stressed that a government's legitimacy stems from the consent of the governed.[228] Formerly free individuals willingly

226. *Id.* at 134–43.

227. *See Mayflower Compact 1620*, *in* SOURCES OF OUR LIBERTIES: DOCUMENTARY ORIGINS OF INDIVIDUAL LIBERTIES IN THE UNITED STATES CONSTITUTION AND BILL OF RIGHTS 55, 60 (Richard L. Perry ed., rev. 1978) (declaring that "[w]e . . . solemnly and mutually . . . covenant and combine ourselves together into a civil Body Politick, for our better Ordering and Preservation"); THOMAS HOBBES, LEVIATHAN 103–05 (George Routledge & Sons, 2d ed. 1886) (asserting that individuals agreed to abandon their natural rights and subject themselves to the sovereign to impose laws and maintain peace); JOHN LOCKE, TWO TREATISES OF GOVERNMENT, *in* THE WORKS OF JOHN LOCKE IN NINE VOLUMES 207, 312–13 (12th ed. 1824) (arguing that formerly free people parted with unrestricted freedom to form commonwealths to enable governments to protect the rights that individuals cherished); Eric Manpearl, *The Privacy Rights of Non-U.S. Persons in Signals Intelligence*, 29 FLA. J. INT'L L. 303, 311 (2018) (detailing the Constitution's basis in social contract theory).

228. *See* THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776). The Declaration of Independence states:

> We hold these truths to be self-evident: that all men are created equal; that they are endowed, by their Creator with certain unalienable rights; that among these are life, liberty, and the pursuit of happiness. That to secure these rights, governments are instituted among men, deriving their just powers from the consent of the governed.

united to establish communities by undertaking obligations to the government in exchange for the protection of certain rights.[229]

The Supreme Court has held that the Fourth Amendment does not apply to the searches of foreigners outside of the United States in *Verdugo-Urquidez*.[230] Rene Martin Verdugo-Urquidez, a citizen and resident of Mexico, was a leader of a violent drug cartel in Mexico and was involved in the kidnapping, torture, and murder of a United States Drug Enforce Administration (DEA) Special Agent.[231] Verdugo-Urquidez was apprehended in Mexico and transported to the United States border where he was transferred to United States custody.[232] DEA Agents, working with Mexican police, then searched Verdugo-Urquidez's properties in Mexico and seized documents to use as evidence.[233] The Supreme Court determined that the Fourth Amendment does not apply to the search and seizure by United States agents of property owned by a nonresident alien and located in a foreign country.[234] The Court reasoned that the phrase "the people" in the Fourth Amendment "refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[235] Therefore, the Fourth Amendment likely protects individuals who are lawfully present in the United States because these individuals are either part of the United States' national community or likely have sufficient connections to the United States by virtue of their lawful presence in the country.[236] This means that location must be part

---

Id.

ALEXANDER HAMILTON, *The Farmer Refuted*, *in* 1 THE PAPERS OF ALEXANDER HAMILTON 81, 88 (Harold C. Syrett & Jacob E. Cooke eds., 1961) ("the origin of all civil government, justly established, must be a voluntary compact, between the rulers and the ruled; and must be liable to such limitations, as are necessary for the security of the *absolute rights* of the latter").

229. *See* McCulloch v. Maryland, 17 U.S. 316, 404–05 (1819) (declaring that "[t]he government of the Union . . . is, emphatically and truly, a government of the people . . . it emanates from them. Its powers are granted by them, and are to be exercised directly on them, and for their benefit"); Chisolm v. Georgia, 2 U.S. 419, 471 (1793) (stating that "[e]very State Constitution is a compact . . . and the Constitution of the United States is likewise a compact made by the people of the United States to govern themselves").

230. United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

231. *Id.* at 262.

232. *Id.*

233. *Id.*

234. *Id.* at 274–75.

235. *Id.* at 265.

236. *See* Kwong Hai Chew v. Colding, 344 U.S. 590, 596 n.5 (1953) ("The Bill of Rights is a futile authority for the alien seeking admission for the first time to these shores. But once an alien lawfully enters and resides in this country he becomes invested with the rights guaranteed by the Constitution to all people within our borders."); Martinez-Aguero v. Gonzalez, 459 F.3d 618, 620, 624–25 (5th Cir. 2006) (holding that a foreign resident's regular visits to the United States and reliance on a United States consular office's statement that the person could continue to rely on an expired visa until a new visa arrived established sufficient contacts with the United States to provide Fourth Amendment rights). *But see* Am. Immigration Lawyers Ass'n v. Reno, 18 F. Supp.

of the legal regime governing SIGINT activities under current Fourth Amendment jurisprudence, but this may raise serious difficulties as a person's true location may become increasingly more difficult to ascertain. This raises the question of how the law should adapt to the uncertainty of location.

Some have argued that technological advancements have made the world much more interconnected and that national borders have become less significant so the Fourth Amendment's protections should apply to all individuals—regardless of location or non-United States person status. Professor Jennifer Daskal has proposed a "presumptive" Fourth Amendment in which the Fourth Amendment is presumed to apply "regardless of whether the collection takes place inside or outside the United States, and regardless of whether the target is a U.S. person or not" unless "the government establishes that none of the parties to the communication is a U.S. person."[237] A more security-oriented approach may be that in a world in which location becomes extremely difficult to determine accurately, the FISA legal regime governing SIGINT activities should create a new category for non-United States persons appearing to be located in the United States. These individuals, who the Intelligence Community could not develop a reasonable belief that they were outside the United States, but still reasonably believed were non-United States persons, could still be targeted if the Intelligence Community has reasonable suspicion that these individuals are likely to possess, receive, and/or communicate foreign intelligence information rather than forcing the NSA or FBI to establish probable cause that these individuals are agents of a foreign power as long as the Intelligence Community has not conclusively determined that these individuals are physically located inside the United States. The FISC would be required to make this reasonable suspicion determination on an individualized basis. Further, if the Intelligence Community gained conclusive evidence that the target was actually physically located inside the United States, then the Intelligence Community would have one week to shift collection to FISA Title I. Finally, another security-oriented approach would be that if technology develops and is widely adopted such that determining location becomes an extreme problem for the NSA and SIGINT collection under Section 702 is severely hindered, it could be necessary to amend FISA by creating two categories: one for United States persons and one for non-United States persons. These more security-oriented approaches would each rely heavily on the foreign intelligence exception to the warrant clause in the Fourth Amendment.

2d 38, 59–60, 60 n.17 (D.D.C. 1998), *aff'd*, 199 F.3d 1352 (D.C. Cir. 2000) (holding that a person who regularly visited the United States to visit her daughter and grandchild did not have sufficient "substantial connections" to the United States to satisfy the standard set forth in *Verdugo-Urquidez*).

237. Daskal, *supra* note 5, at 383.

1. Extend Fourth Amendment Protections in a Universal Manner

Extending Fourth Amendment protections in a universal manner would reduce the difficulty presented by not being able to determine accurately a target's location because this factor would no longer matter as even non-United States persons overseas would receive Fourth Amendment protections.[238] This embrace of universal privacy rights would be a major break with the United States' social compact tradition and would be an explicit rejection of the holding in *Verdugo-Urquidez*.[239] The approach would also mean that the United States would be accepting the enormous security costs that would come from such a decision. The United States could not maintain nearly the same level of intelligence capabilities as the Intelligence Community currently has if the United States adopted the universalist approach. This would inevitably mean that the Intelligence Community would lose visibility into malicious actors and threats because the United States—as with all countries—has fewer resources to identify threats from foreigners abroad compared with its ability to identify threats from citizens inside the country.[240] Ultimately, pursuing this path would greatly diminish the United States' capacity to gain intelligence to protect the United States' national security interests, the American people, and the Homeland.

---

238. *See* David Cole, *More on the Rights of Others—Ben Wittes' Failure of Imagination*, JUST SEC. (Nov. 12, 2013), https://www.justsecurity.org/3128/rights-ben-wittes-failure-imagination/ (taking a more global view of governance and advocating for universal privacy rights regardless of nationality); David Cole, *More on Wittes and the Rights of Others*, JUST SEC. (Nov. 13, 2013), https://www.justsecurity.org/3148/wittes-rights/; David Cole, *The New U.S. "Red Line"—No Privacy Rights for Foreigners*, JUST SEC. (Nov. 21, 2013), https://www.justsecurity.org/3567/red-line-privacy-rights-foreigners/?print; David Cole, *Time to End the Spying Game*, THE NATION (Nov. 13, 2013), https://www.thenation.com/article/time-end-spying-game/; Cole, *We Are All Foreigners: NSA Spying and the Rights of Others*, *supra* note 5; David Cole, *We Are All Foreign Nationals—Even Orin Kerr*, JUST SEC. (Nov. 1, 2013), https://www.justsecurity.org/2817/foreign-nationals-orin-kerr/.

239. *Compare* Joseph A. Cannataci (Special Rapporteur on the Right to Privacy), *Report of the Special Rapporteur on the Right to Privacy*, ¶ 52, U.N. Doc. A/HRC/34/60 (Sept. 6, 2017) (advocating that "[s]tates [should] prepare themselves to ensure that both domestically and internationally, privacy be respected as a truly universal right and that, especially when it comes to surveillance carried out on the Internet, privacy [should] not [be] a right that depends on the passport in your pocket"), *with Verdugo-Urquidez*, 494 U.S. at 274–75 (holding that the Fourth Amendment does not apply to the searches of foreigners outside of the United States).

240. *See* Ryan Goodman, *Should Foreign Nationals Get the Same Privacy Protections Under NSA Surveillance—or Less (or More)?*, JUST SEC. (Oct. 29, 2014), https://www.justsecurity.org/16797/foreign-nationals-privacy-protections-nsa-surveillance-or-or-more/ (citing national security risks from abroad as a potential reason to offer less privacy protections to foreigners abroad); Peter Margulies, *Sweeping Claims and Casual Legal Analysis in the Latest U.N. Mass Surveillance Report*, LAWFARE (Oct. 20, 2014, 4:11 PM), https://www.lawfareblog.com/sweeping-claims-and-casual-legal-analysis-latest-un-mass-surveillance-report.

2. A Presumptive Fourth Amendment

Professor Daskal rejects the universalist approach, but still argues for more expansive privacy protections under a presumptive Fourth Amendment approach.[241] Professor Daskal argues that the rules that govern data collection activities "should presumptively apply to U.S. persons and non-U.S. persons alike, regardless of whether the target of the acquisition or the data being acquired is based in the United States—absent a determination that all parties to the communication are non-U.S. persons."[242] This position is based on the desire to protect United States persons' communications that may be implicated in collection activities, especially through incidental collection.[243]

In practice, this proposal would mean that Fourth Amendment protections would be extended to most foreign intelligence surveillance targets as it would be extremely difficult to show that no one in a communication was a United States person or located inside the United States, especially if location becomes difficult to ascertain in the future. The approach is certainly contrary to current practice and would extend Fourth Amendment protections to many foreigners abroad who are not part of the United States' social compact and have therefore not been granted the same privacy protections under law as United States persons.[244]

Professor Daskal's vast extension of Fourth Amendment protections to non-United States persons overseas would hinder the Intelligence Community's ability to gather intelligence and create a culture of diminished aggressiveness, which could result in troubling security harms—especially at a time when the United States faces an exceptionally complex threat environment. The NSA already employs minimization procedures that dictate how the agency limits the accessibility, retention, and dissemination of "nonpublicly available information concerning unconsenting United States persons" who are not the target of the surveillance.[245] These minimization procedures help protect United States persons' privacy interests and diminish the intrusiveness of incidental or inadvertent collection.

241. Daskal, *supra* note 5, at 383–87.

242. *Id.* at 385–86.

243. *Id.* at 385; PCLOB, REPORT ON SURVEILLANCE PROGRAM, *supra* note 11, at 114 (explaining that under Section 702, "the term 'incidental collection' is used to refer to situations in which United States persons or people located in the United States have their communications acquired because they were in contact with a targeted foreigner located overseas").

244. *See* Manpearl, *supra* note 227, at 320 (explaining that "U.S. intelligence efforts have focused on protecting U.S. persons' privacy rights and have not been concerned with the privacy interests of non-U.S. persons outside of the United States").

245. 50 U.S.C. § 1801(h).

3. Amend FISA to Create a New Category for Non-United States Persons Appearing to be Located Inside the United States

If location becomes burdensome and extremely difficult to determine accurately for the NSA, a more security-oriented reform would be to reform the FISA legal regime governing surveillance to create a new category for non-United States persons that the NSA is not able to establish a reasonable belief that they are outside of the United States, but still has a reasonable suspicion that such persons are likely to possess, receive, and/or communicate foreign intelligence information. Under this reform, there would be three primary FISA categories: (1) United States persons and individuals conclusively determined to be physically located inside the United States, (2) non-United States persons appearing to be located inside the United States, and (3) non-United States persons reasonably believed to be outside the United States.

FISA has various provisions that distinguish between United States persons that are inside the United States and United States persons that are reasonably believed to be outside the United States, but all of these provisions require probable cause findings that the United States person is "a foreign power or an agent of a foreign power"[246] (in the case of United States persons inside the United States) or "a foreign power, an agent of a foreign power, or an officer or employee of a foreign power"[247] (in the case of United States persons that are reasonably believed to be outside the United States).[248] There are subtle differences in the way FISA treats these subcategories of United States persons, but for the purposes of this Article I group these sub-categories of United States persons together as one category because FISA requires that the FISC make an individualized probable cause finding prior to the Intelligence Community targeting any United States persons—regardless of whether they are inside or outside the United States—under the statute.[249] This reform would continue to require a probable cause finding prior to targeting any United States person or person conclusively determined to be inside the United States under FISA.

The second category—non-United States persons appearing to be located inside the United States—would currently not be covered by Section 702 and the government would likely need to obtain a FISC order based on a probable cause finding that the person is a foreign power or agent of a foreign power to target such individuals. Under this reform, the government would only need to establish reasonable suspicion that a person in this new category is likely to possess, receive, and/or communicate foreign intelligence information despite the fact that the person appears to be located inside the United States. This reform would include the privacy protective measure of requiring that the FISC make an individualized reasonable suspicion determination prior to the

246. 50 U.S.C. § 1805(a).

247. 50 U.S.C. § 1881b(b).

248. 50 U.S.C. §§ 1805, 1881b, 1881c, 1881d.

249. 50 U.S.C. §§ 1805, 1881b, 1881c, 1881d.

Intelligence Community targeting individuals in this category. Further, this reform would require that if the Intelligence Community gained conclusive evidence that the target is actually physically located inside the United States then the Intelligence Community would have one week to shift collection to FISA Title I.

The final category of non-United States persons reasonably believed to be outside the United States would remain the same as currently exists under Section 702.

In a world in which advanced anonymity and location-spoofing technologies are more prevalent, and cause problems for the NSA in making pre-tasking foreignness determinations and in conducting post-tasking analysis regarding an individual's location, this reform can alleviate some of the difficulties. The government would be able to target non-United States persons that successfully use these technologies to hide their true locations and appear to be located inside the United States as long as the government can meet the less stringent legal standard of reasonable suspicion instead of requiring the government to establish probable cause that the target is a foreign power or agent of a foreign power under FISA Title I.[250] The government would also have an easier time maintaining SIGINT collection against individuals that were originally targeted as non-United States persons reasonably believed to be overseas, but during post-tasking analysis appear to have entered the United States. The government could transition its collection efforts against such individuals from the non-United States persons reasonably believed to be outside the United States category to the non-United States persons appearing to be located inside the United States category as long as the government maintained a reasonable suspicion that the target is likely to possess, receive, and/or communicate foreign intelligence information. This could help reduce the post-tasking analysis resource problem that could be created by these technologies and diminish the number of targets that the government would have to cease collecting on when it appeared that the individual had entered the United States. The reasonable suspicion standard in this reform is a less demanding legal hurdle than the probable cause determination in FISA Title I, which should reduce the potential for situations in which the government was able to collect on a target under Section 702, but did not have enough information to target the person under FISA Title I. Also, it would not require as much time to establish reasonable suspicion as is currently needed for FISA Title I applications.[251] The reasonable

250. *See* 50 U.S.C. § 1805(a) (giving the FISA Title I legal standards); Terry v. Ohio, 392 U.S. 1, 19–27 (1968) (finding that a law enforcement officer may conduct a brief investigatory stop, consistent with the Fourth Amendment, when the officer has reasonable, articulable suspicion that criminal activity is afoot, which is a less demanding hurdle than probable cause).

251. *Compare* Comey, *supra* note 58 (describing that FISA Title I applications are lengthy documents and undergo significant internal oversight and external judicial oversight), *and* Roberts, *supra* note 17 (quoting former Director of National Intelligence (DNI) Admiral Mike McConnell

suspicion determination would be made by the FISC on an individualized basis because of the privacy concerns that are implicated by the fact that some of these targets that are non-United States persons appearing to be located inside the United States will indeed actually be located inside the United States and not just using technologies to try to thwart NSA SIGINT collection that make this appear to be the case.

This reform would also require that if the Intelligence Community gained conclusive evidence that the target is actually physically located inside the United States then the Intelligence Community would have one week to shift collection to FISA Title I. There will certainly be some instances in which the non-United States person appearing to be located inside the United States target will indeed truly be located inside the United States and intelligence will reveal this information. For example, an FBI agent may positively identify a non-United States person foreign intelligence target inside the United States while conducting physical surveillance or biometrics may establish that a non-United States person foreign intelligence target has entered the United States. These examples would both meet the conclusive evidence standard under this reform to require that the Intelligence Community shift collection to FISA Title I. The information required to meet this conclusive evidence standard does not need to be as concrete as these examples, but solely having email content that says that a target is inside the United States would not be sufficient enough under this reform to require the Intelligence Community to shift collection to FISA Title I because this information could be manipulated as part of tradecraft to complement the use of anonymity or location-spoofing technologies. Analysts would be required to assess whether a non-United States person appearing to be located inside the United States target can actually be conclusively determined to be physically located inside the United States whenever new information regarding location is acquired, and analysts would be required to document their assessments. These assessments would be periodically reviewed to ensure that the Intelligence Community is adhering to the reformed legal regime.

This reform relies heavily on the foreign intelligence exception to the warrant requirement. Non-United States persons appearing to be located inside the United States are likely entitled to Fourth Amendment protections because these individuals likely have sufficient connections (or appear to have sufficient connections in regard to individuals that only appear to be located inside the United States by virtue of their use of anonymity or location-spoofing technologies) to the United States by virtue of their lawful presence in the country.[252] The government's action in regard to this new category must comply with the Fourth Amendment's reasonableness requirement to be

---

as stating "[i]t takes about 200 man hours to do [a FISA application for] one telephone number"), *with* Arizona v. Hicks, 480 U.S. 321, 326 (1987) (recognizing that "reasonable suspicion … means something less than probable cause").

252. *See* cases cited *supra* note 236.

constitutional.[253] The government has an extremely strong interest in collecting foreign intelligence information and the Supreme Court has noted that "[i]t is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."[254] This new legal regime would only be created as a result of significant problems for the government in accurately determining location because of the advances and prevalence of anonymity and location-spoofing technologies, which means that the government's ability to conduct speedy SIGINT collection for foreign intelligence purposes would potentially be diminished without the reform. This adds to the gravity of the threat the reform is intended to address.[255] Further, this new legal regime would have the protection of requiring prior judicial review, as a FISC judge would be required to make the determination that there is reasonable suspicion that the target is likely to possess, receive, and/or communicate foreign intelligence information. The legal regime would also continue to have the protections of requiring that targeting procedures, minimization procedures, and certifications be approved by the FISC. In addition, this reform would have the significant protection of requiring the Intelligence Community to shift collection to FISA Title I if it gained conclusive evidence that the target is actually physically located inside the United States. The government's interest and the protections granted to the targeted persons' privacy rights must be weighed against the privacy intrusion that occurs.[256] Surveillance constitutes a significant intrusion into the privacy rights of the individual who is targeted. SIGINT collection can reveal intimate information about an individual, such as one's political association, religious belief, and sexual habits.[257] Despite this intrusion, "the ultimate touchstone of the *Fourth Amendment* is 'reasonableness'" and the protections put in place under this

253. *See* U.S. CONST. amend. IV.

254. Haig v. Agee, 453 U.S. 280, 307 (1981) (quoting Aptheker v. Sec'y of State, 378 U.S. 500, 509 (1964)).

255. Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 451 (1990) (determining that the severity of the drunk driving problem and state's interest in eliminating drinking and driving were significant factors in making sobriety checkpoints constitutional).

256. *See* Maryland v. King, 569 U.S. 435, 448 (2013) (the '"traditional standards of reasonableness' requires a court to weigh 'the promotion of legitimate governmental interests' against 'the degree to which [the search] intrudes upon an individual's privacy'" (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

257. *See* Riley v. California, 573 U.S. 373, 396–99 (2014) (describing the significant privacy intrusion of searching cell phones, and observing that

> a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is);

United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (asserting that GPS surveillance "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations").

regime should be deemed reasonable in view of the significant government interest at stake to uphold the government's action as reasonable.[258]

The primary concerns with this reform are that SIGINT collection targeting non-United States persons appearing to be located inside the United States will implicate more United States persons in incidental collection than currently occurs under Section 702 and that collecting on targets appearing to be located inside the United States based solely on reasonably suspicion, not probable cause, increases the potential for domestic political abuse. While this reform would be intended to address the difficulties in accurately determining location because of technological advancements that hinder the Intelligence Community's ability to determine accurately and quickly that a target that appears to be inside the United States is actually just using technological tools to make it appear that way and is not truly inside the United States, the new category of non-United States persons appearing to be located inside the United States would inevitably encompass people who actually are present in the United States, such as foreign diplomats. That is why this reform would require the Intelligence Community to shift collection to FISA Title I if it gained conclusive evidence that the target is actually physically located inside the United States. People who are actually present in the United States are much more likely to be in contact with Americans, which means that there will be a significant likelihood that SIGINT collection targeting these individuals will result in quite a lot of incidental collection on Americans. This raises the potential for domestic political abuse, which was a core concern that led to the original FISA statute being passed in 1978. The passage of the original FISA in 1978 expressed "a deep concern about potential government abuse *within our own political system*."[259] FISA prohibits reverse targeting, too, which is a significant protection against the government taking advantage of a lesser legal hurdle to collect on a non-United States person as a pretext for the actual purpose of acquiring information about United States persons that have not separately been deemed appropriate targets by the FISC.[260] These protections help to ensure that the original FISA's intent to provide "special protections for United States persons . . . as a crucial safeguard of democratic accountability and effective self-governance within the American political system" would continue to exist under this reform.[261]

Further, this reform could take advantage of minimization at the point of collection to enhance privacy protections for the United States persons who communicate with the non-United States person appearing to be located inside

---

258. *Riley*, 134 S. Ct. at 2482 (quoting Brigham City v. Stuart, 547 U. S. 398, 403 (2006)).

259. CLARKE ET AL., *supra* note 18, at 154 (describing the original FISA statute's stringent legal restrictions on surveillance of United States persons as reflecting "not only a respect for individual privacy, but also—and fundamentally—a deep concern about potential government abuse *within our own political system*").

260. 50 U.S.C. § 1881a(b).

261. CLARKE ET AL., *supra* note 18, at 154.

the United States target. Data acquired under this new category could also be tagged and treated as a special category of information that has a relatively short retention period. There is obviously increased risk by imposing enhanced minimization requirements and subjecting this data to shorter retention periods because information that might become important later on would have been deleted, which creates the potential that an important relationship connection or illicit activity could be missed. Nonetheless, the privacy concerns regarding the increased incidental collection of United States person communications may be significant enough to warrant these measures. These back-end privacy protections enhance the reasonableness of this reform proposal under the Fourth Amendment, too.

4. Amend FISA to Distinguish Based Only on United States Person vs. Non-United States Person Status

Another security-oriented reform would be to remove location as a statutory factor in determining what legal standard should apply, and solely distinguish based on whether a target is a United States person or non-United States person. This reform would go even further than the proposal discussed in Part III.A.3, but could be necessary if technology develops to the point that location can no longer be accurately determined for a significant number of targets to the extent that collection efforts under Section 702 are severely hindered. Under this approach, SIGINT collection targeting United States persons would continue to have to be based on a probable cause finding by a FISC judge that the person is a foreign power or agent of a foreign power. SIGINT collection targeting non-United States persons would only be based on a finding made by government officials that there is reasonable suspicion that the person is likely to possess, receive, and/or communicate foreign intelligence information. Intelligence Community officials would make this determination based on targeting procedures, minimization procedures, and certifications that are approved by the FISC such that this category would function the way Section 702 currently operates, and not require individualized findings of reasonable suspicion by the FISC. Section 702 currently has more than 164,000 targets,[262] so it would likely not be practically possible to require the FISC to make a reasonable suspicion determination on each one of these targets plus the other non-United States person targets that would now be included in this reformed category that were previously not targeted under Section 702.

This would simplify the government's efforts because the Intelligence Community would no longer have to make a determination regarding a target's location under the statute. The Intelligence Community would only have to make determinations regarding the target's status as a United States person or non-United States person and the foreign intelligence purpose. In practice, a target's location has significant intelligence value so analysts will likely still try

262. DNI, TRANSPARENCY REPORT 2018, *supra* note 4, at 13.

to determine this piece of information, but this determination would not have legal significance because of the extreme technical challenges in accurately obtaining this information. The government would be able to target non-United States persons that successfully use these technologies to hide their true locations and appear to be located inside the United States as long as the government can meet the less stringent legal standard of reasonable suspicion instead of requiring the government to establish probable cause that the target is a foreign power or agent of a foreign power under FISA Title I.[263] Also, the Intelligence Community would not face problems in conducting post-tasking analysis because it would not be legally significant if the target appeared to have entered the United States during post-tasking analysis as long as the government still had the reasonable belief that the person was a non-United States person and reasonable suspicion that the person is likely to possess, receive, and/or communicate foreign intelligence information.

This reform proposal places a significant amount of weight on the foreign intelligence exception. Some of the individuals in the non-United States persons category will surely be present inside the United States and therefore likely have Fourth Amendment rights by virtue of likely having sufficient connections to the United States.[264] The government's action would therefore need to be reasonable to be constitutional under the Fourth Amendment. As discussed *supra*, the government's interest in collecting foreign intelligence information to protect national security is a compelling interest of the upmost importance.[265] This new legal regime would only be created if location was no longer a practically useful factor to consider because of the evolutions in technology, which would transform the location factor in the current FISA legal regime into a significant and dangerous hindrance. This means that the reform proposal would only be enacted if maintaining the status quo posed a significant threat.

Unlike the proposal in Part III.A.3, this proposal would not have the added protection of requiring individualized judicial review prior to SIGINT collection against non-United States person targets because prior individualized judicial review would not be possible given the scale of collection efforts against more than 164,000 non-United States person targets. This legal regime would continue to have the protection of requiring that targeting procedures, minimization procedures, and certifications be approved by the FISC as with the current Section 702 design. The government's interest and the protections granted to the targeted persons' privacy rights must be weighed against the

263. *See* 50 U.S.C. § 1805(a) (giving the FISA Title I legal standards); Terry v. Ohio, 392 U.S. 1, 20–27 (1968) (finding that a law enforcement officer may conduct a brief investigatory stop, consistent with the Fourth Amendment, when the officer has reasonable, articulable suspicion that criminal activity is afoot, which is a less demanding hurdle than probable cause).

264. *See* cases cited *supra* note 236.

265. *See supra* Part II.

privacy intrusion that occurs.[266] Surveillance constitutes a significant intrusion into the privacy rights of the individual who is targeted. SIGINT collection can reveal intimate information about an individual.[267] The reasonableness of the government's activities under this reform proposal is less certain because of the lack of individualized prior judicial review, even for those non-United States persons that are located inside the United States and therefore have Fourth Amendment rights. The significance of the government's interests and protections provided by the targeting procedures, minimization procedures, and certifications may be sufficient to make the government's action reasonable. Further, the technological developments that would necessitate this type of reform could force significant Fourth Amendment doctrinal developments, which may place this reform proposal on stronger constitutional footing.

This reform proposal presents the same concerns as discussed in Part III.A.3 because solely distinguishing based on United States person and non-United States person status will lead to SIGINT collection targeting non-United States persons located inside the United States. This implicates more United States persons in incidental collection than currently occurs under Section 702 and collecting on targets inside the United States based solely on reasonably suspicion, not probable cause, increases the potential for domestic political abuse. Reverse targeting would still be prohibited, which is a significant protection. However, there is less of an upside in creating strict minimization procedures with relatively short retention periods for information collected on non-United States persons under this reform because the vast majority of individuals in this category would be non-United States persons overseas, and therefore would not have Fourth Amendment rights. The security costs that can result by deleting information that may be useful at a later point in time would also be greater under this reform than the reform in Part III.A.3 because the category of all non-United States person targets is much larger than the category of non-United States persons located inside the United States. Nonetheless, it may be necessary to have strict minimizations procedures despite the security costs to increase the reasonableness of the reform proposal under the Fourth Amendment. This proposal goes much further than the reform proposal in Part III.A.3 and would likely only be desirable under the most extreme circumstances.

B. Reforming Procedures to be More Forward Leaning

It may be prudent to create more forward leaning procedures to ease some of the difficulties that could be caused by increased uncertainty of the location of targets. One approach would be to build "lists of IP addresses [that are]

266. Maryland v. King, 569 U.S. 435, 448 (2013) (quoting Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

267. *See supra* note 257 and accompanying text.

associated with known VPN providers."[268] This would ensure that when a target uses one of the United States-based VPNs that the NSA is aware of, the analysts can immediately learn that the target is using a location-spoofing device and has not actually entered the United States—or at least know that this piece of information does not indicate that the target has entered the United States. Creating lists of IP addresses that are associated with known VPN providers would also enhance privacy protections for United States persons because United States persons located inside the United States may use VPN providers that are based overseas, and therefore the United States person's IP address would indicate that they were abroad. If the NSA had knowledge that the specific IP address was associated with a VPN, this piece of information would be given no weight in the foreignness determination that is based on the totality of the circumstances, which would diminish the potential for inadvertent collection on a United States person. The NSA could bring the "lists of IP addresses [that are] associated with known VPN providers" to the FISC's attention to ensure that the FISC is aware that the NSA is taking such measures to deal with the problem of determining location when targets use location-spoofing technologies.[269]

If procedures allow for greater collection of communications on the front-end, the Intelligence Community can develop greater back-end privacy protections to ensure that collection efforts remain reasonable under the Fourth Amendment. The Intelligence Community can tag the data collected from targets that appear to have entered the United States and have shorter retention periods and stricter dissemination limits on this data if the Intelligence Community is authorized to continue collecting on these targets, either because one of the reforms proposed above in Parts III.A.3 or III.A.4 were adopted or because the NSA gained approval to ignore indicators from the IP addresses that are associated with known United States-based VPN providers. Although these SIGINT programs and databases are already extremely complex and adding in more complexity increases the potential for compliance issues, data tagging seems to be an increasingly useful tool in helping the Intelligence Community place special rules on certain data.[270]

Finally, the Intelligence Community should be proactive in explaining the technological challenges that it faces to the FISC.[271] This will help to better inform FISC judges of impending problems and avoid situations in which in

---

268. Kris, *supra* note 65, at 414.

269. *Id.*

270. *See* Frank R. Konkel, *Managing the Deluge*, GOV'T EXEC. (Nov. 11, 2014), https://www.govexec.com/magazine/magazine-analysis/2014/11/managing-deluge/98579/ (describing the NSA's process of tagging data to implement access controls to different data).

271. *See* Interview with Carrie F. Cordero, *supra* note 158 (stating that the NSA can develop a positive relationship with the DOJ and FISC by keeping the DOJ and FISC better informed about the technological changes that the Intelligence Community is facing).

which technological challenges become compliance problems.[272] It is in the NSA's interest to avoid situations in which it has to report compliance problems to the FISC after they have occurred to try to explain why it has not been able to implement the collection as originally presented to the FISC in the application, and as approved in the court order.[273] Ideally, a more proactive approach would create a more collaborative environment where the NSA, Department of Justice (DOJ), and FISC develop rules and procedures that allow for flexibility to adjust to new technical challenges while providing adequate privacy protections.[274]

IV. WHAT'S PAST IS PROLOGUE: THE NECESSITY TO RELY HEAVILY ON EXECUTIVE ORDER 12333 TO DEAL WITH A DIMINISHED HOME FIELD ADVANTAGE AND REDUCED COMPLIANCE BY TECHNOLOGY COMPANIES

As the Internet continues to grow, more transmission facilities will be built around the world, which will diminish communications networks' reliance on United States-based physical infrastructure.[275] This means that a smaller percentage of the world's communications will transit the United States. The reduction in the United States' home field advantage will diminish the usefulness of Section 702 in the future.[276] The push towards data localization could diminish United States companies' market share and could exacerbate the trend towards a smaller percentage of the world's communications transiting the United States.[277] Further, United States-based multi-national technology companies have innovated technologically, especially in the aftermath of the Snowden disclosures, in a manner that reduces their ability to respond to lawful surveillance orders and makes intelligence collection more difficult. The widespread adoption of encryption has created difficulties for the Intelligence Community—and will likely create significant problems in the future—and the possible shift to storing data overseas to avoid complying with lawful orders may also reduce the usefulness of Section 702.[278] As Section 702 becomes less useful in the future, the Intelligence Community must assess how it can improve collection under Executive Order 12333 to ensure that the government continues to acquire vital intelligence to protect United States national security interests.[279]

---

272. *Id.*

273. *Id.*

274. *See id.* (arguing that it is a better approach for the NSA to work with the FISC to adjust procedures to match the technology changes as the NSA sees them occurring and as the NSA initially starts to grapple with the developments, rather than after developments have created more significant hardships that result in compliance issues).

275. Hecht, *supra* note 172; Kris, *supra* note 65, at 416–17; *see* Bryant, *supra* note 172; Singel, *supra* note 172.

276. *See supra* Part II.C.

277. *See supra* Part II.C.

278. *See supra* Part II.D.

279. *See supra* Part II.D.

There are a number of areas that the Intelligence Community should focus on to enhance Executive Order 12333 SIGINT collection. The Intelligence Community should continue to invest significant resources in decrypting communications, especially in technologies that can assist in being able to decrypt communications at scale; continue to conduct outreach to technology companies whose cooperation will always be helpful in SIGINT collection because these private companies own the communications systems; and increase the focus on obtaining cooperation from foreign entities and compromising key strategic targets. Further, beyond enhancing SIGINT collection capabilities, the Intelligence Community must concentrate on how to develop and improve technological tools that can assist in conducting intelligence analysis at scale to be able to sift through and make sense of the massive quantities of data that are collected.

A. Obtain Decrypted Communications and Invest in Decrypting Communications

The increased prevalence of encryption creates a serious impediment to the Intelligence Community being able to obtain useful information. Although the NSA may have the technical and cryptographic skills to be able to decrypt a lot of data, the widespread adoption of encryption technologies still poses a significant problem because the NSA may not be able to decrypt the information at the scale that is needed. One approach to alleviating the difficulties that encryption poses for Section 702 would be for Congress to enact a lawful access requirement.[280] Encryption would still pose a problem for SIGINT collection that occurs under Executive Order 12333, which will become more important as the United States' home field advantage diminishes, regardless of whether Congress enacts a lawful access requirement because technology companies outside of the United States are also adopting encryption technologies.[281] The NSA must therefore continue to invest resources in being able to decrypt communications and acquiring unencrypted communications.

There is a currently a robust debate over whether there should be a lawful access requirement to mandate that companies maintain access to users' communications and data, and provide law enforcement or intelligence agencies with access upon receipt of a lawful order.[282] If Congress enacted a lawful

---

280. *See* Manpearl, *supra* note 143, at 93; Eric Manpearl, *The International Front of the Going Dark Debate*, 22 VA. J.L. & TECH. 158, 161–69 (2019) [hereinafter Manpearl, *International Front of the Going Dark Debate*].

281. *See* BRUCE SCHNEIER ET AL., A WORLDWIDE SURVEY OF ENCRYPTION PRODUCTS 2 (2016), https://www.schneier.com/academic/paperfiles/worldwide-survey-of-encryption-products.pdf (finding that there are "546 encryption products from outside the [United States]").

282. *See, e.g.*, Stewart Baker, *How Long Will Unbreakable Commercial Encryption Last?*, LAWFARE (Sept. 20, 2019, 8:00 AM), https://www.lawfareblog.com/how-long-will-unbreakable-

access requirement, the NSA would be able to acquire targets' plaintext communications from technology companies upon issuing a directive under Section 702 because the companies would be required to maintain access to their users' communications. This would alleviate the difficulties that encryption poses to Section 702 collection.

However, the private sector and some cryptographers fear that the technological architecture that would guarantee law enforcement and intelligence agencies access would compromise user security and privacy.[283] Building in lawful access would increase systems' complexities, which would increase vulnerabilities because the new feature could interact with existing features in unintended and unknown ways.[284] Also, the encryption keys that would need to be retained by the companies, government, or third party would become targets for illicit actors to attack.[285] Thus, user security could be put at greater risk with a lawful access requirement. This could result in increased theft of intellectual property through cybercrime, which already costs United States companies about $250 billion per year.[286]

Also, surveillance by governments that have less robust legal processes as the United States would be made easier by the new technological architecture because United States products are used around the world.[287] A lawful access requirement may conflict with the United States' foreign policy interests at times when unbreakable encryption could be favored because dissidents could use it to challenge authoritarian regimes.[288] Further, sophisticated illicit actors would be able to encrypt their communications regardless of whether the United States mandated lawful access because they could switch to foreign technology services and products that would continue to offer unbreakable encryption because they would not be affected by the United States' lawful access

---

commercial-encryption-last; *see generally* Manpearl, *supra* note 143; Manpearl, *International Front of the Going Dark Debate*, *supra* note 280.

283. *See, e.g.*, ABELSON ET AL., *supra* note 209, at 10 (arguing against a lawful access requirement because of cybersecurity concerns).

284. *Id.* at 15–16.

285. *Id.*

286. Keith B. Alexander, U.S. Cyber Command Commander & NSA Dir., Cybersecurity and American Power, Address at the American Enterprise Institute 15:57–16:02 (July 9, 2012), http://www.aei.org/events/cybersecurity-and-american-power/.

287. *See* Lu Wang, *Tech Giants Are Now Global Stock Leaders*, BLOOMBERG (Feb. 2, 2016, 11:00 AM), http://www.bloomberg.com/news/articles/2016-02-02/facebook-ascent-cements-reign-of-u-s-tech-in-global-stock-ranks (discussing how the demand for United States technology products around the world has spurred United States technology companies to become the largest companies in the world).

288. *See, e.g.*, Andrea Peterson, *The NSA is Trying to Crack Tor. The State Department is Helping Pay for It*, WASH. POST (Oct. 5, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/10/05/the-nsa-is-trying-to-crack-tor-the-state-department-is-helping-pay-for-it/?utm_term=.8c9b8767725f (reporting on the State Department's efforts to teach activists and journalists to use Tor and other counter-surveillance technologies during the Arab Spring).

requirement.[289] Finally, requiring lawful access could further diminish the market share and economic viability of United States companies because this requirement could reinforce foreign consumers' beliefs that using American products or online services would make their communications accessible to United States law enforcement or intelligence agencies.[290] This could contribute even more to the erosion of the United States' home field advantage and diminish the United States' economic strength, which is an important aspect of the United States' role in the world.[291]

Some of the concerns that caution against a lawful access requirement may not be as severe as some have argued. Several major Internet companies currently have the ability to decrypt information and have not suffered major security problems, which indicates that these companies' services may not be made insecure by having the ability to decrypt information. For example, Google has the ability to decrypt Gmail and Gchat communications because this allows Google to target users for advertisements.[292] Also, Gmail is able to filter spam, which can contain malware, because Google can read emails' plaintext, which would not be possible with end-to-end encryption.[293] Google offers the full text search of files stored in the cloud, which requires access to plaintext, too, and could not occur with end-to-end encryption.[294] There have not been security issues with Google's services thus far.[295]

Further, consumers may care more about being able to be connected to friends, having easy to use and reliable products, and having sleek interfaces and useful applications, and may be willing to sacrifice some privacy and security in exchange. A recent study surveying 1,510 participants, including both information technology security experts and non-experts, from the United States, United Kingdom, and Germany found that privacy and security only play a minor role in people's decisions to use a particular mobile instant messenger.[296] The primary reason that participants gave for using a mobile instant messenger "was whether friends were using the messenger."[297] Of those surveyed, 46.1% of participants from the United States, 48.2% of participants

289. SCHNEIER ET AL., *supra* note 281, at 6.

290. *See, e.g.*, Miller, *supra* note 177 (discussing the increased skepticism by foreign consumers of United States technology products following the Snowden disclosures).

291. Manpearl, *supra* note 143, at 83 (recognizing that "[e]conomic strength enables countries to have political and military power and to have strong geopolitical influence").

292. Benjamin Wittes, *Five Hard Encryption Questions*, LAWFARE (Aug. 7, 2015, 2:14 PM), https://lawfareblog.com/five-hard-encryption-questions.

293. Greenberg, *supra* note 215.

294. OLSEN ET AL., *supra* note 212, at 11.

295. Wittes, *supra* note 292.

296. ALEXANDER DE LUCA ET AL., USENIX, EXPERT AND NON-EXPERT ATTITUDES TOWARDS (SECURE) INSTANT MESSAGING 147–51 (2016) https://www.usenix.org/system/files/conference/soups2016/soups2016-paper-de-luca-.pdf.

297. *Id.* at 149.

from the United Kingdom, and 54.9% of participants from Germany stated this was the main reason they used a particular mobile instant messenger.[298] On the other hand, only a small percentage of participants stated the main reason they used a mobile instant messenger was because of privacy and security.[299] Only 5.6% of participants from the United States, 3.4% of participants from the United Kingdom, and 13.1% of participants from Germany stated this was the main reason that they used a particular mobile instant messenger.[300] If consumers are not driven to select products and services based on whether they offer unbreakable encryption, then perhaps the fear that United States companies will lose market share and that the economic viability of United States companies would be hurt by a lawful access requirement is overstated. A full discussion of the arguments in the "going dark" debate, which is a complex issue, is beyond the scope of this Article. I have previously advocated for a lawful access requirement and believe that pursuing this policy would help to maintain the usefulness of SIGINT collection under Section 702.[301]

Regardless of whether Congress enacts a lawful access requirement, it is important for the Intelligence Community to develop strategies to address widespread encryption. Acquiring communications is most useful if the Intelligence Community can decrypt the information or get the information in plaintext form. Continuing to invest in technologies that can aid in decryption is extremely important, especially technologies that can assist in the decryption of large quantities of information. Quantum computing may be an enormous breakthrough in being able to decrypt information at scale. The Intelligence Community may need to devote more resources towards compromising major foreign ISPs, discussed more *infra*,[302] to collect traffic as it transits the companies' infrastructure. If the company has access to plaintext communications for its own business reasons, then compromising that company will allow the Intelligence Community to collect unencrypted communications. Nonetheless, the Intelligence Community may still have to devote more resources towards decryption if the company's internal traffic is encrypted in this scenario.

End-to-end encryption poses another problem. The Intelligence Community will have to devote resources to conducting man-in-the-middle attacks and compromising end-users to obtain desired communications when it encounters end-to-end encryption. If the government is interested in a particular conversation between two individuals, the government can relay the messages between the users to trick the users into thinking that they are connecting directly with each other when in reality the government has inserted itself into the

298. *Id.*
299. *Id.*
300. *Id.*
301. Manpearl, *supra* note 143, at 93–99.
302. *See infra* Part IV.C.

communications as an attacker.[303] For example, if the government is interested in a particular conversation between two individuals, Alice and Bob, the government can attempt to replace the Bob's public encryption key with its own Intelligence Community public key to conduct an active man-in-the-middle attack because Alice will now be sending her messages to the Intelligence Community and not Bob.[304] The Intelligence Community can then forward Alice's messages to Bob so as not to tip off Bob to the fact that the Intelligence Community has inserted itself into Alice and Bob's communications.[305] The Intelligence Community could even change messages that Alice sends to Bob so that Bob sees the manipulated messages if this would be useful for an intelligence operation.[306] Often times, the Intelligence Community will first need to compromise the private key of a trusted intermediary company that serves as a broker of public keys in order for the Intelligence Community to be able to send Alice the Intelligence Community's public key as a replacement for Bob's public key and successfully trick Alice into thinking she has actually been given Bob's public key.[307] Conducting narrowly targeted man-in-the-middle attacks and compromising specific end-users may be quite resource intensive because these types of attacks do not generally provide for broad collection opportunities.[308] Therefore, these attacks against end-to-end encryption may only be feasible against higher value targets.[309] Finally, the Intelligence Community will need to continue to exploit metadata with technical analysis because metadata is often unencrypted. While metadata can be "a valuable source of information" and help map networks, "it does not replace the definitive value of content."[310]

B. Improved Cooperation from Companies

Despite the rather adversarial relationship between some companies and the United States government that has developed in the aftermath of the Snowden disclosures, this environment may not persist forever. The United States government should continue to work to develop strong relationships with United States technology companies and seek to mend to fissures that have been created. Technology companies have been great innovators for our society and are extremely important to the United States economy. In 2014, Internet-related

303. Tanmay Patange, *How to Defend Yourself Against MITM or Man-in-the-Middle Attack*, HACKERSPACE (Nov. 10, 2013, 8:37 AM), https://hackerspace.kinja.com/how-to-defend-yourself-against-mitm-or-man-in-the-middl-1461796382.

304. *Id.*

305. *Id.*

306. *Id.*

307. *Id.*

308. Interview with Eric Greenwald, Former Senior Dir. for Cybersecurity, Nat'l Sec. Council Staff, in Austin, Tex. (Mar. 21, 2018).

309. *Id.*

310. Letter from Deirdre Walsh to Sen. Ron Wyden, *supra* note 216, at 2.

companies in the United States generated $966.2 billion in revenue, which accounted for six percent of real Gross Domestic Product.[311] "Economic strength enables countries to have political and military power and to have strong geopolitical influence."[312] Therefore, the government should continue to champion the innovations that occur at these companies. Further, these private-sector technology companies will develop many of the technological tools that the Intelligence Community will use in the future as an increasing amount of technology is being produced in the private sector rather than inside the government.[313] For example, Amazon has contracted with the Central Intelligence Agency (CIA) to provide cloud computing for the Intelligence Community, and the National Geospatial-Intelligence Agency (NGA) has contracted with private firms "to enhance artificial intelligence and automation to improve geospatial-intelligence analysis."[314] Working to maintain and improve relationships across the board with technology companies can pay dividends in obtaining better cooperation in the future. Cooperation from technology companies will always be very helpful to SIGINT collection because private companies own the communications systems.[315]

---

311. STEPHEN E. SIWEK, INTERNET ASS'N, MEASURING THE U.S. INTERNET SECTOR 5 (2015), https://internetassociation.org/wp-content/uploads/2015/12/Internet-Association-Measuring-the-US-Internet-Sector-12-10-15.pdf.

312. Manpearl, *supra* note 143, at 83; Manpearl, *International Front of the Going Dark Debate*, *supra* note 280, at 169.

313. *See* Noel Calhoun, *Private and Government Defense and Intelligence Agencies Must Work Together*, THE HILL (Jan. 26, 2018, 10:15 AM), http://thehill.com/opinion/technology/370852-private-and-government-defense-and-intelligence-agencies-must-work (acknowledging that the private sector possesses state of the art technological tools and can develop innovative technologies rapidly, and providing advice on how the government and private sector can work together to better leverage private industry's capabilities to serve national security needs).

314. *NGA Awards Four Contracts to Enhance Artificial Intelligence and Automation*, NAT'L GEOSPATIAL-INTELLIGENCE AGENCY (Feb. 15, 2017), https://www.nga.mil/ProductsServices/Pages/NGA-awards-four-contracts-to-enhance-artificial-intelligence-and-automation.aspx. *See* Frank Konkel, *The Details About the CIA's Deal with Amazon*, ATL. (July 17, 2014), https://www.theatlantic.com/technology/archive/2014/07/the-details-about-the-cias-deal-with-amazon/374632/; Stew Magnuson, *Geospatial Agency to Share Historical Data with Private Sector, Start-Ups*, NAT'L DEF. (June 5, 2017), http://www.nationaldefensemagazine.org/articles/2017/6/5/geospatial-agency-to-share-historical-data-with-private-sector-start-ups.

315. Kris, *supra* note 224, at 227. In 2008, Ken Wainstein, then-Assistant Attorney General for National Security in the Department of Justice, described the government's reliance on technology companies to facilitate surveillance:

> [W]e rely on the communications providers to do our intelligence surveillances. We can't do [the surveillances] without them because . . . we . . . don't own the communications systems. We need to rely on their assistance. . . . Yes, we can compel the phone companies, or compel the communications providers to do a surveillance, and even if they . . . resist a directive . . . we can go to the FISA Court to get our orders enforced. Problem is, throughout that time, we're dark on whatever surveillance it is that we want to go up on.

C. Cooperation with Foreign Entities and Compromising Key Strategic Targets

As SIGINT collection under Executive Order 12333 becomes more important, the Intelligence Community must increase its focus on obtaining the cooperation of foreign entities and compromising key strategic targets. Partner arrangements between governments and intelligence services to facilitate intelligence sharing and access to key collection platforms and facilities is an incredibly important aspect of intelligence collection.[316] As Section 702 becomes less useful in the future, the United States will need to rely more on foreign governments to share intelligence and encourage technology companies within those foreign nations to cooperate with the United States. These intelligence-sharing relationships will help the United States Intelligence Community gain access to pristine and complete communications in a safer environment, which are important factors that have made Section 702 such a vital intelligence gathering authority.[317] Relationships and deals between intelligence services and allied governments can always entail certain limitations, though, such as the need to provide more robust privacy protections to citizens of another country in the SIGINT that is obtained as a result of an arrangement than would otherwise be provided or use restrictions on the intelligence that is shared.[318] Nonetheless, the tradeoffs typically favor engaging in these intelligence relationships unless the same information can be collected in another manner because the United States will almost certainly always be better off with more intelligence.[319]

The United States must increase the amount of resources that it devotes to effectively compromising key strategic targets. Some of this will be accomplished by human intelligence (HUMINT) operations—this can be thought of as HUMINT enabled SIGINT. Intelligence officers may be able to recruit assets inside foreign technology companies that can provide access to those communications systems or develop fruitful relationships with the leaders of key strategic foreign technology companies.[320]

The Intelligence Community will also need to increase its exploitation of vulnerabilities (*i.e.*, conduct more remote hacking operations) for SIGINT collection as the amount of fruitful intelligence obtained under Section 702 diminishes. It takes significant time and resources to find vulnerabilities and

---

Id.

316. Ashley S. Deeks, *A (Qualified) Defense of Secret Agreements*, 49 ARIZ. ST. L.J. 713, 741–44 (2017); Ashley Deeks, *Intelligence Communities, Peer Constraints, and the Law*, 7 HARV. NAT'L SEC. J. 1, 6–10 (2016).

317. *See supra* Part I.C.

318. Deeks, *Intelligence Communities, Peer Constraints, and the Law*, *supra* note 316, at 10–11; Interview with Robert S. Litt, *supra* note 210.

319. Interview with Eric Greenwald, *supra* note 308.

320. Interview with Eric Greenwald, *supra* note 308; Interview with Benjamin Wittes, *supra* note 161.

money to purchase vulnerabilities, as well as significant effort to develop the tools to exploit these vulnerabilities.[321] These vulnerabilities are transient, though, as eventually they are discovered and patched or new products and services are developed that do not have the same vulnerabilities.[322] This means that the Intelligence Community will constantly need to innovate to exploit vulnerabilities to be able to collect SIGINT at scale. Many of these capabilities will depend on investing in research and development, talented personnel, and the necessary infrastructure to conduct these intelligence operations.[323]

Increased aggressiveness in exploiting vulnerabilities to conduct SIGINT operations could result in diplomatic blowback when operations are discovered. The foreign policy challenges and strained alliance relationships that can result from disclosed intelligence operations are important factors to consider at the outset of deciding whether to conduct intelligence operations.[324] The risk of blowback can therefore be a key limitation on intelligence operations. While there was a great deal of diplomatic backlash following the Snowden disclosures, there is a general understanding among nations that countries spy on one another.[325] The key question of whether to proceed with an operation or whether the risks are too great to proceed will always be a context dependent inquiry. Intelligence officials will have to weigh the value of the target, the country or countries that will be affected by the operation and their relationship with the United States, the threat environment and diplomatic challenges that are present at a given point in time, and other factors when deciding whether to conduct operations while being mindful that operations seldom stay secret forever.

This increased reliance on exploiting vulnerabilities will lead to increased debate over when the government should disclose vulnerabilities to vendors or hold onto these vulnerabilities. The Vulnerabilities Equities Process (VEP), which is the process that the United States government has created to decide

---

321. Susan Hennessey, *Lawful Hacking and the Case for a Strategic Approach to "Going Dark"*, BROOKINGS INST. (Oct. 7, 2016), https://www.brookings.edu/research/lawful-hacking-and-the-case-for-a-strategic-approach-to-going-dark/; Interview with Robert S. Litt, *supra* note 210.

322. *See* HAYDEN, *supra* note 92, at 421 (acknowledging that SIGINT advantages are temporary).

323. Interview with Eric Greenwald, *supra* note 308.

324. *See* Manpearl, *supra* note 227, at 354 (describing the intense foreign policy backlash to the Snowden disclosures that led the United States to institute voluntary surveillance reforms); Courtney Weldon, Steve Brackin & Eric Manpearl, *National Security Council Oversight of U.S. Intelligence Activities*, *in* INTELLIGENCE AND NATIONAL SECURITY IN AMERICAN SOCIETY 3, 8–9 (discussing the importance of developing contingency plans for managing the unauthorized disclosure of sensitive intelligence collection programs).

325. *See* Ashley S. Deeks, *Confronting and Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 609–10 (2016) (detailing several instances of government leaders openly talking about the importance of intelligence).

when the government should disclose previously unknown (zero-day) vulnerabilities, has already sparked rigorous debate on this topic.[326] While the government has important intelligence, military, and law enforcement interests in discovering and keeping vulnerabilities to exploit, there are also valid cybersecurity reasons for disclosing some vulnerabilities and United States technology companies that may benefit from vulnerability disclosure are an important part of the United States economy. In addition to the important intelligence that will increasingly be gathered through the exploitation of vulnerabilities—and likely will not be able to be collected through other means—which weigh in favor of holding onto vulnerabilities, disclosing vulnerabilities may risk potentially informing adversaries about the United States Intelligence Community's sources and methods.[327] Further, the United States' adversaries do not engage in similar vulnerability disclosure programs, which could potentially put the United States in an intelligence gathering and military disadvantage in the future relative to adversary countries that are able to continuously stockpile vulnerabilities without disclosing them.[328]

On the other hand, there are salient arguments in favor of disclosure. Disclosing vulnerabilities enables companies to patch the vulnerabilities, thus fixing their products.[329] This improves cybersecurity overall and helps these companies to have more secure products.[330] For the last several years, the United States Intelligence Community has listed the cyber threat as the top threat in its worldwide threat assessment report and United States companies lose hundreds of billions of dollars in intellectual property theft per year.[331] Further,

---

326. WHITE HOUSE, VULNERABILITIES EQUITIES POLICY AND PROCESS FOR THE UNITED STATES GOVERNMENT 1 (2017), https://www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF.

327. Dave Aitel & Matt Tait, *Everything You Know About the Vulnerabilities Equities Process is Wrong*, LAWFARE (Aug. 18, 2016, 2:46 PM), https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

328. *Id.*

329. Michael Daniel, *Heartbleed: Understanding When We Disclose Cyber Vulnerabilities*, WHITE HOUSE (Apr. 28, 2014, 3:00 PM), https://obamawhitehouse.archives.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities; ARI SCHWARTZ & ROB KNAKE, BELFER CTR. FOR SCI. & INT'L AFFAIRS, GOVERNMENT'S ROLE IN VULNERABILITY DISCLOSURE 1, 3, 5 (2016), https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf.

330. Daniel, *supra* note 329.

331. DANIEL R. COATS, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 5–7 (2019), https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR—-SSCI.pdf; DANIEL R. COATS, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 5–6 (2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA—-Unclassified-SSCI.pdf; DANIEL R. COATS, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1–3

adversary nations may discover the same vulnerability as the United States has discovered and may seek to use the vulnerability to target United States interests, which would weigh heavily in favor of disclosure in such situations.

There will certainly be situations in which it is an easy call not to disclose. For example, the United States should obviously not disclose a vulnerability when the United States discovers a vulnerability in a foreign adversary government's system that the foreign country contracted for with a foreign company in that country. A vulnerability that has little intelligence value yet exists on systems that many Americans use would be an obvious example of a situation in which the government should disclose. The more difficult decisions are those that implicate important offensive and defensive interests. United States officials will have to consider the likelihood that another group will also discover the vulnerability, the risk of a leak of the vulnerability, how quickly a vendor could develop a patch for the vulnerability and how widespread the adoption of the patch would be, the importance of the target the vulnerability is being used on, and the susceptibility of United States interests to the same vulnerability among other important considerations when deciding whether to hold onto or disclose a vulnerability.

D. Technical Investments to Improve Analysis Capabilities

Beyond enhancing SIGINT collection capabilities, the Intelligence Community must focus on improving the ability to conduct intelligence analysis at scale. As numerous observers have noted, "the increase in the total amount of data also creates problems in the form of ever-larger haystacks in which the government must find the needles."[332] Perhaps a more apt analogy is that it is

(2017), https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf; JAMES R. CLAPPER, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1–4 (2016), https://www.dni.gov/files/documents/SASC_Unclassified_2016_ATA_SFR_FINAL.pdf; JAMES R. CLAPPER, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1–4 (2015), https://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf; JAMES R. CLAPPER, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1–3 (2014), https://www.dni.gov/files/documents/Intelligence%20Reports/2014%20WWTA%20%20SFR_SSCI_29_Jan.pdf; JAMES R. CLAPPER, OFFICE OF THE DIR. NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD, WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 1–3 (2013), https://www.dni.gov/files/documents/Intelligence%20Reports/UNCLASS_2013%20ATA%20SFR%20FINAL%20for%20SASC%2018%20Apr%202013.pdf.

332. Kris, *supra* note 65, at 417.

"like looking for a needle in a stack of needles"[333] as important pieces of intelligence do not necessarily stand out in the sea of information—analysts must sift through the massive quantities of information to determine what is important.[334] The great value in SIGINT collection can only be realized if analysts are able to find the useful pieces of information.

Unlike downstream collection under Section 702 in which the communications "to" and "from" a selector are provided to the NSA in a manner that is highly likely to yield intact copies of the entirety of the communications, Executive Order 12333 collection cannot necessarily provide such tailored acquisition. The Intelligence Community must invest in developing and purchasing the technological tools, such as artificial intelligence, that can assist in conducting intelligence analysis at scale to be able to sift through massive quantities of data.[335] These tools will play an increasingly critical role in sorting through data to find useful intelligence, and can be leveraged to improve the usefulness of SIGINT collection under Executive Order 12333.[336] Further, the Intelligence Community should continue to invest in machine translation tools. Linguistic analysis has been a limiting factor for all intelligence agencies, and this problem will only get worse as more data is generated.[337] There will not be

---

333. CTR. FOR DIG. CONTENT, UNTANGLING THE WEB: A GUIDE TO INTERNET RESEARCH 12 (2007); Interview with Eric Greenwald, *supra* note 308.

334. Calhoun, *supra* note 313; CTR. FOR DIG. CONTENT, *supra* note 333 at 12; Interview with Eric Greenwald, *supra* note 308.

335. GREG ALLEN & TANIEL CHAN, BELFER CTR. STUDY, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY 27–28 (2017), https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf; Magnuson, *supra* note 314.

336. Melissa Drisko, the former Deputy Director of the Defense Intelligence Agency (DIA), has stated that "[w]e have to be much more data-centric, much more savvy in how we handle data . . . . There are secrets there that we got to find. It's how do you find those." Lauren C. Williams, *Spy Chiefs Set Sights on AI and Cyber*, FCW (Sept. 7, 2017), https://fcw.com/articles/2017/09/07/intel-insa-ai-tech-chiefs-insa.aspx. Drisko concluded that "algorithmic analysis, artificial intelligence, [and] machine learning" will play a key role in finding important intelligence. *Id. See* Amaani Lyle, *National Security Experts Examine Intelligence Challenges at Summit*, U.S. DEP'T OF DEF. (Sept. 9, 2016), https://www.defense.gov/News/Article/Article/938941/national-security-experts-examine-intelligence-challenges-at-summit/ (summarizing Intelligence Community leaders' discussion of the necessity of using artificial intelligence); Jenna McLaughlin, *Artificial Intelligence will Put Spies Out of Work, Too*, FOREIGN POLICY (June 9, 2017, 2:37 PM), http://foreignpolicy.com/2017/06/09/artificial-intelligence-will-put-spies-out-of-work-too/ (discussing NGA's push to utilize artificial intelligence); Mark Pomerleau, *Here's How Technology Can Help Unburden DIA Analysts*, C4ISRNET (Aug. 4, 2017), https://www.c4isrnet.com/intel-geoint/isr/2017/08/04/heres-how-technology-can-help-unburden-dia-analysts/ (reporting on DIA's plan to adopt artificial intelligence to help analysts sift through a flood of data).

337. *See, e.g.*, H.R. PERMANENT SELECT COMM. ON INTELLIGENCE, INTELLIGENCE AUTHORIZATION ACT FOR FISCAL YEAR 2002, H.R. REP. NO. 107-219, at 19 (2001) ("The principle agencies dealing with foreign intelligence—CIA, NSA, FBI, DIA and the military services—have all admitted they do not have the language talents, in breadth or in depth, to fully

enough human-hours to be able to translate communications by human linguists. Instead, machine translation, though imperfect, can dramatically increase the Intelligence Community's efficiency in this area. Finally, the Intelligence Community must invest in technologies that can work to piece packets of communications together to form complete communications automatically by drawing on data packets across multiple streams of SIGINT acquisition. A tremendous advantage of Section 702 has been the ability to obtain precise and complete communications, but as Section 702 becomes less useful, Executive Order 12333 will need to make up for this lost intelligence.

V. CONCLUSION

Section 702 was a critical intelligence collection reform that addressed technological developments to enable the Intelligence Community to acquire vital foreign intelligence to protect United States national security interests and inform policymakers.[338] Section 702 enables the Intelligence Community to collect intelligence on non-United States persons that are reasonably believed to be overseas when the Intelligence Community reasonably believes it will likely acquire foreign intelligence from surveilling these individuals without having to undergo the significant step of establishing probable cause that the target is an agent of a foreign power, probable cause that each facility is being used or is about to be used by a foreign power or agent of a foreign power, and that the information could not be reasonably obtained by normal investigative methods.[339] The Intelligence Community would simply not be able to maintain nearly the same level of intelligence collection without Section 702 if it were forced to rely on FISA Title I. Also, Section 702 allows for collection to occur in a stable and safe domestic environment. Under downstream, the communications "to" and "from" a selector are even provided to the NSA in a manner that is highly likely to yield intact copies of the entirety of the communications.[340]

While the collection programs under Section 702 have produced a great deal of valuable intelligence over the last decade, the United States must begin to think about impending technological developments and strategically consider how to conduct SIGINT collection in the future. The United States' current legal regime governing SIGINT activities is predicated on the location of the target. If location becomes significantly difficult to determine because of the increased

---

and effectively accomplish their missions."); *see also* Interview with Eric Greenwald, *supra* note 308.

338. INGLIS & KOSSEFF, *supra* note 20, at 4–8.

339. *Compare* Foreign Intelligence Surveillance Act of 1978 Amendments Acts of 2008 § 702 (authorizing SIGINT collection targeting non-United States persons reasonably believed to be overseas to acquire foreign intelligence information), *with* Foreign Intelligence Surveillance Act of 1978 §§ 104-105 (authorizing foreign intelligence collection under FISA Title I and establishing the legal requirements for conducting such SIGINT activities).

340. INGLIS & KOSSEFF, *supra* note 20, at 4.

prevalence and advancement of location-spoofing and anonymity technologies, the United States may have to reconsider how location should factor into this legal paradigm. Anonymity tools mask information about a user's true identity and location that can be critical for the NSA's ability to lawfully target individuals under Section 702. Although anonymity tools may not become widespread, these technologies can still currently pose problems for the NSA and the increased prevalence of illicit actors using anonymity technologies will make the NSA's work more difficult, especially in regard to illicit actors that use sophisticated tradecraft. Location-spoofing technologies are very likely to be widely adopted and may cause substantial problems for the NSA. Location-spoofing technologies make it appear as if communications are actually coming from an intermediary computer instead of the original user, which can hide the user's true location. These technologies may hinder the NSA's ability to target individuals under Section 702 and could create a major resource problem for the NSA in its post-tasking analysis or cause the NSA to have to detask targets and lose the ability to gather intelligence on these targets.

In a world in which location becomes extremely difficult to accurately determine, the United States should reform FISA to create a new category for non-United States persons appearing to be located in the United States. These individuals, who the Intelligence Community could not develop a reasonable belief that they were outside the United States, but still reasonably believed were non-United States persons, could still be targeted if the Intelligence Community has reasonable suspicion that these individuals are likely to possess, receive, and/or communicate foreign intelligence information rather than forcing the NSA or FBI to establish probable cause that these individuals are agents of a foreign power as long as the Intelligence Community has not conclusively determined that these individuals are physically located inside the United States. The FISC would be required to make this reasonable suspicion determination on an individualized basis because of the privacy concerns that are implicated by the fact that some of these targets that are non-United States persons appearing to be located inside the United States will indeed actually be located inside the United States and not just using technologies that make this appear to be the case. If the Intelligence Community gained conclusive evidence that the target is actually physically located inside the United States, then the Intelligence Community would have one week to shift collection to FISA Title I. This reform could take advantage of minimization at the point of collection to enhance privacy protections for the United States persons that communicate with the non-United States person appearing to be located inside the United States target, and data acquired under this new category could be tagged and treated as a special category of information that has a relatively short retention period.

If this reform would still not be sufficient to address the significant problems created by technological developments and the adoption of these technologies such that SIGINT collection under Section 702 was severely hindered, it could be necessary to reform FISA by creating two categories: one for United States

persons and one for non-United States persons. Both of these reforms would rely heavily on the foreign intelligence exception to the warrant clause in the Fourth Amendment.

It may be prudent to create more forward leaning procedures to ease some of the difficulties that could be caused by increased uncertainty of the location of targets. One approach would be to build lists of IP addresses that are associated with known VPN providers. If procedures allow for greater collection of communications on the front-end, the Intelligence Community can develop greater back-end privacy protections to ensure that collection efforts remain reasonable under the Fourth Amendment. Finally, the Intelligence Community should be proactive in explaining the technological challenges that it faces to the FISC. Ideally, a more proactive approach can create a more collaborative environment where the NSA, DOJ, and FISC can find the proper balance of rules and procedures that allow for the needed flexibility to adjust to new technical challenges while providing adequate privacy protections for those who are protected by the Fourth Amendment.

Further, Section 702 will likely become less useful in the future. The United States' home field advantage is receding, which means that the United States will have a smaller share of the world's communications traffic transit its physical infrastructure.[341] This will reduce the Intelligence Community's ability to acquire precise and intact communications by serving directives on United States companies. The push towards data localization could diminish the market share of United States companies and could exacerbate the trend towards a smaller percentage of the world's communications transiting the United States. In addition, technology companies have begun to innovate in a manner that reduces their capability to respond to lawful orders. Technology companies have increasingly adopted encryption technologies and may shift data overseas to try to avoid complying with lawful surveillance orders. As Section 702 becomes less useful in the future, the Intelligence Community must assess how it can improve collection under Executive Order 12333 to ensure that the government continues to acquire vital intelligence to protect United States national security interests.

One approach to alleviating the difficulties that encryption poses for Section 702 would be for Congress to enact a lawful access requirement.[342] Encryption would still pose a problem for SIGINT collection that occurs under Executive Order 12333, which will become more important as the United States' home field advantage diminishes, regardless of whether Congress enacts a lawful access requirement because technology companies outside of the United States are also adopting these technologies. The NSA must therefore continue to invest resources in being able to decrypt communications and acquiring unencrypted communications. The United States government should continue to work to

341. Kris, *supra* note 65, at 416–17.

342. *See, e.g.*, Manpearl, *supra* note 143, at 73–74.

develop strong relationships with United States technology companies and seek to mend to fissures that have been created in the aftermath of the Snowden disclosures.

Also, as SIGINT collection under Executive Order 12333 becomes more important, the Intelligence Community must increase its focus on obtaining the cooperation of foreign entities and compromising key strategic targets. The United States will need to rely more on foreign governments to share intelligence and encourage technology companies within those foreign nations to cooperate with the United States. The United States must increase the amount of resources that it devotes to compromising key strategic targets effectively. Some of this will be accomplished by HUMINT enabled SIGINT. The Intelligence Community will also need to increase its exploitation of vulnerabilities for SIGINT collection.

Finally, beyond enhancing SIGINT collection capabilities, the Intelligence Community must focus on improving the ability to conduct intelligence analysis at scale. The Intelligence Community must invest in developing and acquiring technological tools that can assist in conducting intelligence analysis at scale to be able to sift through massive quantities of data.

These reforms and strategic investments can help ensure that United States SIGINT activities evolve to meet future technological developments and continue to provide the necessary intelligence to protect United States national security interests, the American people, and the Homeland.