Michigan Telecommunications and Technology Law Review

Volume 21 | Issue 2

2015

Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad

Axel Arnbak
University of Amsterdam

Sharon Goldberg
Boston University

LOOPHOLES FOR CIRCUMVENTING THE CONSTITUTION: UNRESTRAINED BULK SURVEILLANCE ON AMERICANS BY COLLECTING NETWORK TRAFFIC ABROAD

*Axel Arnbak and Sharon Goldberg**

Cite as: Axel Arnbak and Sharon Goldberg,
Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad,
21 MICH. TELECOMM. & TECH. L. REV. 317 (2015).
This manuscript may be accessed online at repository.law.umich.edu.

ABSTRACT

This Article reveals interdependent legal and technical loopholes that the US intelligence community could use to circumvent constitutional and statutory safeguards for Americans. These loopholes involve the collection of Internet traffic on foreign territory, and leave Americans as unprotected as foreigners by current United States (US) surveillance laws. This Article will also describe how modern Internet protocols can be manipulated to deliberately divert American's traffic abroad, where traffic can then be collected under a more permissive legal regime (Executive Order 12333) that is overseen solely by the executive branch of the US government. Although the media has reported on some of the techniques we describe, we cannot establish the extent to which these loopholes are exploited in practice.

An actionable short-term remedy to these loopholes involves updating the antiquated legal definition of "electronic surveillance" in the Foreign Intelligence Surveillance Act (FISA), that has remained largely intact since 1978. In the long term, however, a fundamental reconsideration of established principles in US surveillance law is required, since

* Axel Arnbak is a Faculty Researcher at the Institute for Information Law, University of Amsterdam and a Research Affiliate at the Berkman Center for Internet & Society, Harvard University. Sharon Goldberg is Associate Professor of Computer Science, Boston University and a Research Fellow, Sloan Foundation. She gratefully acknowledges the support of the Sloan Foundation. Both authors thank Timothy H. Edgar, Ethan Heilman, Susan Landau, Alex Marthews, Bruce Schneier, Haya Shulman, Marcy Wheeler and various attendees of the PETS'14 and TPRC'14 conferences for discussions and advice that have greatly aided this work. Alexander Abdo, David Choffnes, Nico van Eijk, Edward Felten, Daniel K. Gillmore, Jennifer Rexford, Julian Sanchez and the anonymous reviewers for HotPETS'14 each provided insightful comments on drafts of this Article. Views and errors expressed in this Article remain the sole responsibility of the authors. This Article was submitted on September 1, 2014 and a brief update was concluded on December 26, 2014. All URLs have been checked on this date. An earlier version of this Article was first posted online on June 27, 2014.

these loopholes cannot be closed by technology alone. Legal issues that require reconsideration include the determination of applicable law by the geographical point of collection of network traffic, the lack of general constitutional or statutory protection for network-traffic collection before users are "intentionally targeted," and the fact that constitutional protection under the Fourth Amendment is limited to "US persons" only. The combination of these three principles results in high vulnerability for Americans when the US intelligence community collects Americans' network traffic abroad.

Introduction

Although the string of revelations on surveillance operations conducted by the United States (US) intelligence community has overloaded the general public and the media, we are only beginning the process of precisely describing the legal and technical details behind these operations. This multi-disciplinary Article discusses interdependent legal and technical loopholes that US intelligence agencies could use to circumvent Fourth Amendment protections and statutory safeguards for Americans.

There are several loopholes in current US surveillance law that allow for largely unrestrained surveillance on Americans by collecting their network traffic abroad while not intentionally targeting a US person. Because the US legal framework regulating intelligence operations has not been updated to account for new technical realities, the loopholes we identify could leave Americans' Internet traffic as exposed to network surveillance and as unprotected, from a legal perspective, as foreigners' Internet traffic.

This Article aims to broaden the understanding of how technical realities of the Internet impact US surveillance law and suggest remedies that can close the loopholes identified. This Article focuses on surveillance operations conducted by US government agencies but does not speculate on the extent to which the intelligence community is exploiting the loopholes identified. This Article also does not address the morality of surveillance based on the (assumed) nationality of Internet users.

This analysis fits into a recurring regulatory conundrum. The application of any law is, ultimately, tied to jurisdiction. For centuries, jurisdiction has been determined primarily by geographic borders, or the physical space that states consider sovereign territory. Because global communication networks do not necessarily respect such borders, regulators and courts across the globe are struggling to adapt law to this new technical reality. Transnational surveillance (i.e., surveillance conducted from one country, directed towards users in another country) on global communications networks presents us with one of the most urgent examples of this conundrum.[1]

Although short term technical and legal solutions are available to address some of the issues outlined in this Article, they are no panacea. In the end, safeguarding the privacy of American Internet users requires a reconsideration of three legal principles underlying US surveillance law. First, the geographical point of collection determines which legal regime applies to a surveillance operation. Second, the collection of network traffic, before processing and analysis, is not firmly protected by the Fourth Amendment of

1. *See generally* Joris van Hoboken, Axel Arnbak, & Nico van Eijk, Obscured by Clouds, or How to Address Governmental Access to Cloud Data from Abroad (June 7, 2013) (conference paper), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103 (discussing the issue of transnational surveillance on global communications networks extensively).

the US Constitution. Third, constitutional protection is limited to "US persons," a term that is not defined uniformly across different regimes of US surveillance laws. These principles emerged in different times than ours. If they are maintained, loopholes in antiquated law—particularly Executive Order (EO) 12333—will work in conjunction with ever-advancing technical capabilities to enable largely unrestrained surveillance on Americans from abroad.

This Article focuses on network traffic surveillance conducted from abroad in the data collection phase, although at times we point to policies for data retention and subsequent analysis as well. Part I describes the three legal regimes that form the core regulatory framework for network traffic collection by intelligence agencies. Part II discusses the technical details of how network protocols can be exploited to conduct surveillance from abroad, thus circumventing the legal protections in place for Americans when operations are conducted on US soil. Part III briefly reflects on possible legal and technical remedies.

METHODOLOGY. Our research combines descriptive, internal legal analysis with threat-modeling from computer science. In addition to reaching inter-disciplinary conclusions, we aim to offer academics a new analytical framework to conduct similar research. Our method should be particularly helpful for conducting research on the interdependency of the laws and technologies for network surveillance and conducting evaluations of surveillance law as part of policymaking.

LEGAL ANALYSIS. Part I describes the current US regulatory framework for intelligence gathering. Three legal regimes are most relevant to this Article:

1. Surveillance of domestic communications records conducted on US soil under § 215 of the Patriot Act;[2]
2. Surveillance of international communications conducted on US soil under the Foreign Intelligence Surveillance Act (FISA);[3] and
3. Surveillance conducted entirely abroad under Executive Order 12333 (EO 12333)[4] and underlying policies, notably

2. *See generally* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, 50 U.S.C. § 1861 (2012).

3. *See generally* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. § 1881a (2012).

4. *See generally* Intelligence Authorization Act for Fiscal Year 2015, H.R. 4681, 113th Cong. § 309 (2014); Exec. Order No. 12,333, 3 C.F.R. § 200 (1981); Exec. Order No. 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003); Exec. Order No. 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004); Exec. Order No. 13,470, 73 Fed. Reg. 45,325 (July 30, 2008).

the US Signals Intelligence Directive SP0018 (USSID 18).[5]

Distinguishing factors include where the surveillance is conducted and whom a surveillance operation targets. All three branches of the US government oversee the first two regimes, and have been discussed at length by the government, media, and general public. The third regime, however, is solely the domain of the executive branch and has only recently begun to receive some attention in policy, media, and academic arenas. EO 12333, adopted in 1981 by the Reagan Administration and not substantially updated since, forms the cornerstone of this legal analysis; indeed, the NSA states that EO 12333 is the "primary legal authority" for its operations.[6]

Working with primary legal sources, many of which have only recently been made public and are still redacted on key issues, we make the following central observation: if an intelligence agency can construct plausible presumptions that surveillance does not "intentionally target" a US person and when the surveillance is conducted abroad, the permissive legal regime under EO 12333 applies. Under EO 12333, operations from abroad can be presumed to affect foreigners rather than Americans. Since the Supreme Court has consistently held that foreigners do not enjoy constitutional protection under US law,[7] the legal incentives to conduct surveillance under EO 12333 are substantial.

The legal notion of "targeting a US person" does not rule out bulk collection of Internet traffic, even in situations where the traffic actually contains millions of Americans' communication records. By collecting the traffic abroad, authorities can presume the traffic belongs to foreigners. Any US person's traffic that happens to be captured during bulk collection is considered "incidentally collected" and may be retained for further processing. Users are only "targeted," in the legal sense, once collection is complete and the surveillance operation moves into its retention and analysis phases. Indeed, documents revealed on August 25, 2014 indicate that metadata from retained traffic can be shared between multiple intelligence agencies, including domestic law enforcement and the Drug Enforcement Agency, and used for purposes that include "target development."[8]

---

5. *See generally* National Security Agency, U.S. Signals Intelligence Directive SP 0018, Legal Compliance and U.S. Persons Minimization (2011) [hereinafter "USSID 18"].

6. National Security Agency, Memorandum: The National Security Agency: Missions, Authorities, Oversight and Partnerships at 2–3 (2013), *available at* https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf.

7. Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138 (2013); United States v. Verdugo-Urquidez 494 U.S. 259 (1990).

8. Ryan Gallagher, *Sharing Communications Metadata Across the U.S. Intelligence Community*, The Intercept, at slide 6, August 25, 2014, https://firstlook.org/theintercept/document/2014/08/25/sharing-communications-metadata-across-u-s-intelligence-community;

Thus, collecting Americans' network traffic abroad creates a legal loophole for surveillance on them. A surveillance operation acting in a manner consistent with EO 12333 allows foreignness to be presumed for data that is intercepted abroad. This circumvents Americans' Fourth Amendment protections that are assumed (in the legal sense) to be US persons under FISA and § 215 of the Patriot Act during domestic surveillance operations.[9]

As of July 2014, the lack of public scrutiny of EO 12333 seems to have shifted. When the first public version of this Article was posted online prior to its presentation at the 2014 Privacy Enhancing Technologies Symposium, a range of media outlets reported on our findings. Coverage on *CBS News*[10] spurred an inadequate official response from the NSA compliance department; we discuss this response further in Part I.C.4 of this Article. A few weeks later, a *Washington Post* editorial by John Napier Tye, who served in the State Department from 2011 to 2014, argued:

> Based in part on classified facts that I am prohibited by law from publishing, I believe that Americans should be even more concerned about the collection and storage of their communications under Executive Order 12333 than under Section 215. . . . Consider the possibility that Section 215 collection does not represent the outer limits of collection on US persons but rather is a mechanism to backfill that portion of US person data that cannot be collected overseas under 12333.[11]

On July 23, 2014, the executive agency's Privacy and Civil Liberties Oversight Board ("PCLOB") confirmed that it will investigate surveillance policy and operations based on EO 12333.[12] Given the complexity of US surveillance law and especially EO 12333, the investigation is expected to take months and underscores the necessity of inter-disciplinary research on EO 12333 policy and operations.

TECHNICAL REALITIES. Part II explores why network traffic can easily be routed or stored abroad where it can then be collected under the permissive legal regime of EO 12333. We already know of surveillance programs that

---

Ryan Gallagher, *The Surveillance Engine: How the NSA Built its Own Secret Google*, THE INTERCEPT, August 25, 2014, https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.

9. *See* 50 U.S.C. § 1861 (2012); 50 U.S.C. § 1881a(b)(5) (2012).

10. *See* Zack Whittaker, *Legal Loopholes Could Allow Wider NSA Surveillance, Researchers Say*, CBS NEWS (June 30, 2014, 4:02 PM), http://www.cbsnews.com/news/legal-loopholes-could-let-nsa-surveillance-circumvent-fourth-amendment-researchers-say/.

11. John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets The NSA Spy On Americans*, THE WASHINGTON POST (July 18, 2014), http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html.

12. *See* Transcript, Public Meeting 202-220-4158, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD (July 23, 2014), https://www.pclob.gov/library/20140723-Transcript.pdf.

have exploited this loophole. The MUSCULAR/TURMOIL program, for example, illustrates how the NSA assumed authority under EO 12333 to acquire traffic between Google and Yahoo! servers located on foreign territory; this program allegedly collected up to 180 million user records (including those of Americans) per month abroad.[13]

Part II also discusses other technical means an intelligence agency, using the legal loopholes in EO 12333, might exploit. Instead of eavesdropping on intradomain traffic (i.e., data sent within a network belonging to a single organization, as in the MUSCULAR/TURMOIL program), these loopholes can be exploited in the interdomain setting, where traffic traverses networks belonging to different organizations. Interdomain routing with Border Gateway Protocol (BGP) can naturally cause traffic originating in a US network to be routed abroad, even when it is destined for an endpoint located on US soil. Additionally, core Internet protocols—BGP and the Domain Name System (DNS)—can be deliberately manipulated to force traffic originating in American networks to be routed abroad. These deliberate manipulations can fall within the permissive EO 12333 regime and used to collect, in bulk, all Internet traffic (including metadata and content) sent between a pair of networks, even if both networks are located on US soil.

REMEDIES. Part III explores possible legal and technical remedies. Reform of the Patriot Act and FISA will not close the international surveillance loopholes identified in this Article. The focus on the Patriot Act and FISA may be attributed to the legal fact that the legislative and judicial branches of the US government have little authority over EO 12333 reform, since EO 12333 authority falls solely under the executive branch. Thus, surveillance operations conducted abroad under EO 12333 have thus far been overlooked by reform efforts, despite the fact that they may affect millions of Americans' privacy.

I. LOOPHOLES IN THE LEGAL FRAMEWORK

In this Part, we use recently revealed and declassified primary legal sources to describe and contextualize the US legal framework for network surveillance by intelligence agencies. This discussion highlights the differences in legal protection under the different legal regimes for network traffic collection and reflects on the outlook for reform.

Before we analyze specific legal regimes, it is critical to emphasize that non-US persons do not enjoy the protections of the Fourth Amendment of the US Constitution. The Supreme Court first established this in *United*

13. *See* Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links To Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, THE WASHINGTON POST (October 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

States v. Verdugo-Urquidez[14] and recently confirmed it in *Clapper v. Amnesty International USA a.o.*[15] The legal and technical loopholes we identify fundamentally rely on this principle because it profoundly impacts the statutory regimes for network surveillance.

Under the current US legal framework, two main inquiries determine which of the three legal regimes regulate network traffic collection: *where the communication is taking place* (inside or outside the US) and *who is targeted*. This analysis is focused on the poorly-understood third regime, EO 12333, which primarily regulates intelligence community operations on foreign territory.[16]

We start by analyzing the types of operations that fall under the legal regimes of the Patriot Act and FISA, since EO 12333 covers operations that are not addressed by the first two legal regimes.[17] EO 12333 (and its underlying policies) are then examined in detail. The Order applies when surveillance does not "intentionally target a US person" and is conducted abroad, regardless of whether or not the operation actually affects the communications records of Americans.

Our legal analysis is consistent with a recently released NSA slide titled "SIGINT Authority decision tree," revealed by the Washington Post on July 23, 2014 (after an earlier version of this Article was first posted online) and shown in Figure 1, below:[18]

14. United States v. Verdugo-Urquidez, 494 U.S. 259, 261 (1990). The case concerned a warrantless search of a Mexican citizen's house, in Mexico, suspected of drug trafficking. *See also infra* note 232.

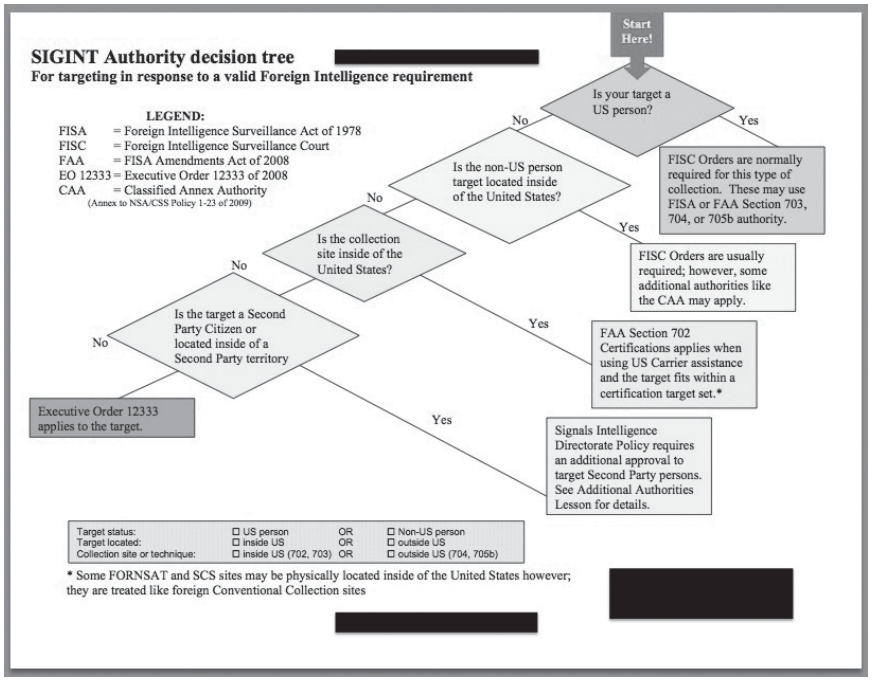
15. Clapper v. Amnesty Int'l USA, 133 S.Ct. 1138, 1154 (2013); *see supra* note 10. The case was brought by several civil society groups, claiming the unconstitutionality of warrantless bulk surveillance of their international communications. *See also* van Hoboken et al., *supra* note 1 at 8; *infra* note 232.

16. We focus on operations conducted abroad. But as we note in Part I.C.2, *infra*, EO 12333 also seems to have been interpreted to enable *domestic* operations not covered by the other two legal regimes.

17. *See* discussion *infra* Parts I.B.2, I.C.2.

18. *See* Ellen Nakashima & Ashkan Soltani, *Privacy Watchdog's Next Target: the Least-Known but Biggest Aspect of NSA Surveillance*, The Washington Post (July 23, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/. Most elements of the flowchart are discussed throughout this section. We will not, however, further discuss the "Second Party" reference, understood to point at the so-called "Five Eyes" nation coalition: the US, United Kingdom, Canada, Australia and New Zealand. For earlier analysis on how allied nations allow one another to conduct surveillance on each other's citizens under lowered legal standards, and subsequently obtain or share the information under classified bilateral agreements, *see* van Hoboken et al., *supra* note 1, at 17–18.

FIGURE 1. FLOWCHART SHOWING NSA SURVEILLANCE OPERATIONS



The location of the collection site and the target's nationality are key elements that determine the applicable legal regime. The less explicit elements of targeting and presumed foreignness, however, are essential to understanding the flowchart and are discussed throughout the remainder of this Article.

First, surveillance operations that collect network traffic in bulk do not necessarily "intentionally target a US person" in the legal sense. Put differently, "targeting" a person (as noted in the decision tree depicted in Figure 1) often occurs after the collection phase (i.e., after network traffic has already been intercepted). Upon collection, surveillance operations move into the retention and analysis phases; it is in these phases that users are actually "targeted" in the legal sense. Most of this discussion centers on the collection phase. The collection phase is crucially important, since large volumes of Americans' communications records can be captured during collection and subsequently stored, searched, or shared with other government agencies.[19]

Second, under the current US surveillance framework, conducting network traffic collection operations from abroad creates the presumption that

19. *See* Tye, *supra* note 11. The revelations of August 25, 2014 indicate that searches of these records is not limited to the N.S.A, but can also be performed by agencies including domestic law enforcement and the Drug Enforcement Agency. *See supra* note 8.

traffic belongs to foreigners: a presumption that holds even though the traffic might, in fact, belong largely to Americans.[20]

A. *Patriot Act § 215: Domestic Communications and Surveillance on US Soil*

Some intelligence operations target and surveil domestic communications on US soil. Under § 215 of the Patriot Act, intelligence agencies can request a warrant at the FISA Court for "tangible things" that are "relevant" to authorized terrorism or counterintelligence investigations.[21] The current form of § 215 was adopted shortly after the 9/11 attacks and broadened the legal authority for domestic surveillance.[22]

One program operating under this authority is the production of Americans' telephone records—the so-called "Verizon Metadata Program." Immediately after 9/11, President Bush arranged for the voluntary provisions of communication records by major US telecommunications providers.[23] Upon a 2005 disclosure of the program in the press, one company asked the government to obtain a warrant from the FISA Court.[24] Since 2006, the Court has granted the warrants on a rolling basis, which include so-called "gag" orders that prevent the companies from disclosing the requests to customers or the public.[25]

With the details of the telephony metadata programs revealed after nearly twelve years, scholars have argued that the program violates both the Constitution and provisions of the Patriot Act.[26] Proposals to reform this legal regime have also been initiated in Congress. Thus far, these proposals have failed.[27] In June 2015, § 215 expires, setting the scene for a new round

---

20. *See infra* Part II.C.

21. 50 U.S.C. § 1861 (2012).

22. *See* USA PATRIOT Improvement and Reauthorization Act of 2005 § 105, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended in scattered sections of 50 U.S.C.); *see* The PATRIOT Sunsets Extension Act of 2011 § 2, Pub. L. No. 122-14, 125 Stat. 216 (codified as amended in scattered sections of 50 U.S.C.).

23. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The Guardian (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order. *See* Offices of Inspectors General of the Dep't of Defense, Dep't of Justice, Cent. Intelligence Agency, Nat'l Sec. Agency & Office of the Dir. of Nat'l Intelligence, Unclassified Report on the President's Surveillance Program (2009), *available at* http://fas.org/irp/eprint/psp.pdf.

24. Greenwald, *supra* note 23.

25. *Id.*

26. *See* L. K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 Harv. J.L. & Pub. Pol'y 757, 763 (2014); *see* R. Levinson-Waldman, Brennan Center for Justice, What The Government Does With Americans' Data (2013).

27. Several bills are being proposed. The bill introduced by Congressman Sensenbrenner and Senator Leahy appeared among those most likely to be adopted, but narrowly failed by a 58 to 42 vote, needing 60 votes in the Senate. *Text of H.R. 3361: USA FREEDOM Act (Referred to Senate Committee Version)*, GovTrack.us, https://www.govtrack.us/congress/bills/113/hr3361/text (last visited May 3, 2015).

of legislative debates in the near future.[28] Furthermore, court cases are pending in several circuits with vastly varying outcomes,[29] suggesting that the Supreme Court may eventually rule on the issue. It is too early to report on the final outcomes of these legal and political debates. Regardless of the outcomes, all three branches of government are involved in establishing the legal protections under this first regulatory regime. As we will see, the other two legal regimes discussed in this Article feature diminished legal protection and, consequently, prospects for reform.

B. *The Foreign Intelligence Surveillance Act: International Communications and Surveillance on US Soil*

The second regulatory regime covers a class of surveillance operations on international communications conducted on US soil, regulated by the 1978 Foreign Intelligence Surveillance Act (FISA). This Part describes this second regime, the scope of surveillance operations covered under FISA, the legal protections afforded to Americans under FISA, and the prospect of FISA reform.

1. Overview

FISA and the FISA Court were introduced in 1978 in response to domestic surveillance overreach and the Church Committee's reform proposals.[30] In 2008, Congress amended and broadened FISA with the FISA Amendments Act (FAA).[31] The FAA broadened the definition of "foreign intelligence information" to include information "relating to the foreign affairs of the United States."[32] With the new definition, surveillance of foreign governments, corporations, media organizations, and citizens was explicitly allowed.[33] The FAA also introduced § 702, which enables warrantless surveillance of foreign communications conducted on US soil, as long as the operations do not "intentionally target US persons."[34] Ever since, authorities have not required warrants for specific cases based on a particularized probable cause; instead, the FISA Court issues generalized certifications for sur-

28. *See* USA PATRIOT Improvement and Reauthorization Act of 2005 § 105, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended in scattered sections of 50 U.S.C.); The PATRIOT Sunsets Extension Act of 2011 § 2, Pub. L. No. 122-14, 125 Stat. 216 (codified as amended in scattered sections of 50 U.S.C.).

29. Klayman v. Obama, 957 F. Supp. 2d 1, 66 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

30. *See supra* notes 1 & 15 for references containing detailed analysis of the legal provisions under FISA and its policy history.

31. *See generally* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, 50 U.S.C. § 1881a (2012).

32. 50 U.S.C. §1801(e)(2) (2012). *See also supra* note 1 at 10–12.

33. *See* 50 U.S.C. §1801(f), (i), (m) (2012).

34. *See* 50 U.S.C. §1881a(b)(1) (2012).

veillance operations aimed at gathering foreign intelligence information.[35] In addition, the FISA Court has approved generalized "targeting" and "minimization" procedures to govern the processing of data after it has been collected.[36] These procedures are intended to ameliorate concerns about US citizens' privacy, and have remained classified until recently.

Since 2005, when reports of bulk wiretapping from the Internet backbone at an AT&T switch came to light, public awareness of bulk surveillance operations on Americans has increased.[37] Nonetheless, even after the AT&T program was revealed, Congress passed the Protect America Act in 2007, which contained many of the provisions adopted in the FAA just one year later.[38] In late 2012, the FAA was extended for another five years.[39] Two months later, the Supreme Court denied several US organizations legal standing in their claim that the privacy of their international communications was violated by § 702.[40] In what appeared to be the final ruling on the constitutionality of § 702, a 5-4 majority held that the civil society groups filing suit lacked standing because they could not prove that their communications had actually been intercepted.[41] The details of the relevant programs remained classified.[42]

---

35. USA PATRIOT Improvement and Reauthorization Act of 2005 § 105, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended in scattered sections of 50 U.S.C.).

36. U.S. Dep't of Justice, Procedures Used by the National Security Agency for Targeting Non-United States Pesrons 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 (2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document [hereinafter Exhibit A]; U.S. Dep't of Justice, 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 (2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document [hereinafter Exhibit B].

37. Declaration of Mark Klein in Support of Plaintiffs' Motion for Preliminary Injunction, Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) (No. C-06-0672-VRW), *available at* https://www.eff.org/node/55051; *See, e.g.*, 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/16program.html?pagewanted=all&_r=0.

38. *See* Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (repealed July 10, 2008). For a comparison between the provisions of the Protect America Act and FAA, *see* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol'y 117, 135–137 (2015).

39. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238.

40. *See* Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1138 (2013).

41. *Id.* at 1150.

42. *See* Press Release, American Civil Liberties Union, Supreme Court Dismisses ACLU's Challenge to NSA Warrantless Wiretapping Law (Feb. 26, 2013), *available at* https://www.aclu.org/national-security/supreme-court-dismisses-aclus-challenge-nsa-warrantless-wiretapping-law.

The political debate and the issue of legal standing have shifted considerably since the first Snowden leaks in June 2013. Today, it has become clear that § 702 serves as the legal basis for surveillance operations like UPSTREAM and PRISM.[43] The NSA has also confirmed that § 702 is used to compel US Internet companies to assist with warrantless surveillance.[44] In addition, several of the classified targeting and minimization procedures under § 702 have been leaked or declassified,[45] providing unique insights into classified interpretations of the legal provisions in FISA as made by the FISA Court and intelligence community.[46] Ongoing lawsuits filed in 2008 to challenge the constitutionality of the AT&T wiretapping operations under the "Terrorist Surveillance Program" have also altered the political landscape.[47]

Before describing § 702 in more detail, it is worth noting that FISA §§ 703, 704 and 705b regulate surveillance to intentionally target US persons.[48] These provisions are outside the scope of this Article—our focus is on surveillance operations conducted on foreign territory that do not intentionally target US persons in the collection phase but affect Americans nonetheless.[49]

2. Scope: The 1978 Definition of "Electronic Surveillance"

All communications surveillance operations that constitute "electronic surveillance" as defined in FISA fall within its scope.[50] The FISA definition has remained largely intact since 1978[51] and fails to account for the technical realities of today's global communications networks.

To collect the content or metadata of "wire communication[s]," surveillance only falls within the FISA definition when authorities "intentionally target a US person," or when the acquisition is conducted on US territory.[52] If authorities conduct targeted surveillance from abroad, even if they know

43. *See* Donohue, *supra* note 38, at 195; *Cf.* Donohue, *supra* note 26.

44. NATIONAL SECURITY AGENCY, *supra* note 6, at 4.

45. *See, e.g.*, EXHIBIT A, *supra* note 36; EXHIBIT B, *supra* note 36.

46. For the most comprehensive analysis to date, *see* Donohue, *supra* note 38 at 195; Donohue, *supra* note 26.

47. *See, e.g.*, Jewel v. NSA, 673 F.3d 902, 912 (9th Cir. 2011). The Electronic Frontier Foundation, one of the organizations involved in the court proceeding, maintains an updated case document repository at https://www.eff.org/cases/jewel.

48. Depicted in Fig. 1: Flowchart Showing NSA Surveillance Operations, *supra* note 18.

49. Laura Donohue has observed that the warrant requirements in §§ 703 & 704 can be circumvented by applying § 702 criteria to the collection phase and deciding after the fact if data collected is of use for further processing. *See* Donohue, *supra* note 38, at 193.

50. *See* 50 U.S.C. §§ 1801(f), 1812(a) (2012); 18 U.S.C. § 2511(2)(f) (2012).

51. 50 U.S.C. § 1801(f) (2012).

52. *See* 50 U.S.C. § 1801(f)(1),(2) (2012). The FISA definition only explicitly mentions communications "content," but also covers "metadata" (location, time, duration, identity of communicants, etc.).

that both "sender and all intended recipients are located in the United States," then only radio (i.e., wireless) communications fall within the FISA definition of "electronic surveillance."[53]

INTENTIONALLY TARGETING US PERSONS. "Intentionally targeting a US person" constitutes "electronic surveillance" under FISA.[54] However, neither "intentionally" nor "targeting" are defined in FISA; instead, these concepts are open to interpretation in classified "targeting" and "minimization" procedures.[55] The recent disclosure of these "targeting" and "minimization" procedures illuminates several areas of concern. For instance, bulk surveillance is not regarded as "intentional targeting;" we discuss this further when we look at legal protections afforded to US persons under FISA in the next sub-Part.

Moreover, the "minimization" and "targeting" procedures reveal two important new facts related to surveillance operations conducted abroad. First, conducting surveillance abroad creates the presumption that the target is a "non-US person."[56] Second, the "targeting procedures" do not provide any due diligence requirement or duty of care to establish the identity of parties on either side of a communication.[57] This implies that unless a communicant is known to be a US person, the communicant is considered to be a non-US person. Thus, authorities have a strong incentive to conduct surveillance abroad: legal protections offered to US persons under FISA can be circumvented, and a more permissive legal regime applies to data collection under EO 12333.

INSTALLING A DEVICE. Preparing a communications infrastructure for surveillance is of particular interest to this analysis.[58] An example of such infrastructure is the use of network protocol manipulations that modify the flow of network traffic, as described in Part II. FISA contains a clause on "the installation . . . of . . . surveillance device[s] in the United States," which can be understood as making a communications infrastructure ready for surveillance.[59] However, this clause only covers electronic surveillance "other than wire or radio communication." The US Congressional Research Service gives "a hidden microphone" as an example of such "other communication."[60]

---

53. *Id.* § 1801(f)(3).

54. *Id.* § 1801(f)(1).

55. *Cf.* Klayman v. Obama, 957 F. Supp. 2d 1, 17–18 (D.D.C. 2013); ACLU v. Clapper, 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013).

56. *See* EXHIBIT B, *supra* note 36.

57. *Cf.* EXHIBIT A, *supra* note 36.

58. For example, as described in Part II, surveillance personnel could use network protocol manipulations to modify the flow of network traffic.

59. *See* 50 U.S.C. § 1801(f)(4) (2012).

60. EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 7 (2013).

Under the current definition, most modern methods of preparing a networked communications infrastructure for surveillance do not constitute "electronic surveillance" under FISA and are, therefore, regulated only by EO 12333. In 1978, when these FISA provisions were adopted, the "installation of a device" was perhaps necessary to divert traffic to a network location where it could be collected.[61] Today, no device installation is necessary: one can exploit vulnerabilities in existing network devices (routers, web proxies, etc.) and network protocols (BGP, DNS, etc.) to alter the flow of network traffic and divert it towards a specified point of collection.[62]

It is possible that the intelligence community has secretly expanded the scope of the 1978 "installing a device" definition to cover newer technologies. But even if this were true, "wired communications" fall outside this part of the FISA definition altogether. Therefore, except when US persons are intentionally targeted, operations for the purpose of "installing a device" that eavesdrop on Internet communications do not constitute "electronic surveillance" under the 1978 FISA definition. Moreover, under the current definition, it is irrelevant whether the "installation of a device" is conducted on US soil or abroad, a relevant factor for our technical analysis in Part II.B.

Without full access to classified surveillance policies fully implementing the directives of FISA and EO 12333, it is impossible to conclusively determine how the intelligence community interprets US surveillance statutes. But recent revelations on untargeted malware operations seem to support our textual analysis.[63] These revelations indicate that NSA analysts perform compliance checks against EO 12333 (but, importantly, not against FISA) when singling out targets for more sophisticated malware operations on the target's machine.[64] Based on these revelations, it seems likely that advanced *active* attacks,[65] which use modern technological capabilities to prepare an infrastructure for a subsequent targeted surveillance operation, are regulated under EO 12333.

3. Legal Protections for US Persons under FISA

Applicability of FISA to a surveillance operation is relevant for Americans because the statute contains important legal protections for US persons that are intentionally targeted. For instance, the statute states that the Fourth

61. *Cf.* 50 U.S.C. § 1801(f)(4) (2012).

62. *See infra* Part II.B on "How Deliberate Manipulations Can Divert US Traffic Abroad."

63. Jacob Applebaum et al., *NSA Secret Toolbox: ANT Unit Offers Spy Gadgets for Every Need*, DER SPIEGEL, Dec. 30, 2013, http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html; *NSA Documents*, DER SPIEGEL (Dec. 30, 2013), http://www.spiegel.de/fotostrecke/nsa-dokumente-so-knackt-der-geheimdienst-internetkonten-fotostrecke-105326-13.html

64. *Id.*

65. *E.g.*, advanced network protocol manipulations, described in Part I.C.3, and injecting malware and installing backdoors in software or hardware.

Amendment applies to surveillance operations under FISA and prohibits a narrow set of four surveillance operations.[66] Surveillance under § 702 may not intentionally target a US person; § 703 of FISA regulates those operations instead. Another example is the "reverse-targeting" prohibition,[67] which states that authorities may not target a non-US person under § 702 when the goal of the operation targets a US person. By contrast, as discussed in Part I.C.3, *infra*, EO 12333 explicitly allows for intentional targeting of US persons under certain conditions.

Vast opportunities for surveillance overreach exist within the bounds of FISA.[68] Other scholars have already offered a comprehensive analysis of the FISA targeting and minimization procedures, along with a critical assessment of the role of the FISA Court. For example, Laura Donohue argued that these procedures allow for the creation of a "foreign intelligence" interest in the data sometime after its collection.[69] Despite the concerning aspects of FISA, at least all three branches of government are involved in FISA, either directly (by amending the statute or the executive measures enacting it) or through the opportunity for judicial review.

4. FISA Reform: Three Branches of Government

FISA and FAA have serious implications for Americans' privacy rights. In response to the recent disclosures, proposals such as the USA Freedom Act seek to reform current legal and regulatory schemes, for instance, by introducing a "civil liberties advocate" that defends privacy interests to make FISA Court hearings adversarial.[70] These proposals, which thus far have failed, pay little attention to the loopholes described in this Article. In the long run, all three branches of government must be involved in regulating such surveillance. FISA and FAA are statutes approved by Congress; the executive branch regulates the operational details of surveillance; and targeting and minimization procedures are approved by the FISA Court.[71]

---

66. *See* 50 U.S.C. § 1881a(b) (2012).

67. *Id.* § 1881(b)(2).

68. *See, e.g.*, EXHIBIT B, *supra* note 36. One of the most-discussed loopholes is when US persons are not "intentionally targeted" but still affected by a surveillance operation. A well-known example is the bulk interception on the Internet backbone on US soil of international communications under the UPSTREAM program. Instead of promptly destroying such data, generous exemptions exist to use the "incidentally" or "inadvertently" collected information of the affected Internet users, American and non-American alike. *See also* Barton Gellman, Julie Tate, & Ashkan Soltani, *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, THE WASHINGTON POST (July 5, 2014), *available at* http://www.washingtonpost.com/world/national-_security/in-_nsa-_intercepted-_data-_those-_not-_targeted-_far-_outnumber-_the-_foreigners-_who-_are/2014/07/05/8139adf8-_045a-_11e4-_8572-_4b1b969b6322_story.html.

69. *See* Donohue, *supra* note 38, at 170–74.

70. *See supra* note 27 at § 401.

71. 50 U.S.C. § 1881a(b)(i)(1)(A) (2012).

C. *Executive Order 12333: Surveillance Conducted on Foreign Soil*

The legal protections afforded to Americans, and the prospects for reform, are significantly lowered under EO 12333. Electronic surveillance conducted abroad is largely regulated by Executive Order (EO) 12333. Surveillance policies regulated under this regime are designed and adopted solely within the executive branch. The NSA recently acknowledged that EO 12333 is "the foundational authority by which NSA collects, retains, analyzes, and disseminates foreign signals intelligence information."[72]

Until recently, the public's ability to analyze the full extent of US surveillance policies has been limited. Many relevant policies were completely classified.[73] Secrecy might explain why EO 12333 and its underlying policies have seen little discussion in policy and scholarly circles; understanding was simply obstructed by classification.

Over the last year, leaks and government releases have enabled a deeper understanding of EO 12333 surveillance policies. But many relevant sentences, paragraphs, sections and even entire documents containing surveillance policy (not actual operations) remain classified. The issue of classified law and policy remains a critical subject for policymakers to address.[74]

This sub-Part analyzes what is publicly known about EO 12333 and flags remaining knowledge gaps relevant to our analysis, focusing on the US Signals Intelligence Directive SP0018 (USSID 18). After providing an overview of EO 12333, we discuss the scope of the document and its application to advanced network surveillance methods. We then describe how US intelligence authorities enjoy broad and largely unchecked legal authority when conducting surveillance abroad and how legal protections offered to Americans under EO 12333 are weaker than under the other two regimes discussed in this Article. Part I.C.4 explores the NSA's official response to an earlier version of this Article—one that fails to address the main issues raised here. Finally, we point to fundamental structural issues in the US Constitution that could serve as barriers to the long-term reform of EO 12333 policies. Here, we briefly examine a new legal authority created by Congress in December 2014: § 309 of the Intelligence Authorization Bill 2014–15,[75] introduced and voted on within forty-eight hours.[76] The exact implications of this provision remain opaque, apparently even to the majority of lawmakers in Congress, and are subject to speculation by lawmakers, the media, and the public.[77]

---

72. NATIONAL SECURITY AGENCY, *supra* note 6, at 2.

73. *See infra* Part I.C.1.

74. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 12, at 9–10, 47–70.

75. Intelligence Authorization Act for Fiscal Year 2015, Pub. L. 113-293, 128 Stat. 3990.

76. *See* Facebook Page of Rep. Justin Amash, FACEBOOK (Dec. 10, 2014, 9:10 PM), https://www.facebook.com/repjustinamash/posts/812569822115759.

77. *Id.*

The President signed the bill into law shortly after it was congressionally approved.

This Article is not an exhaustive analysis of EO 12333's loopholes; it focuses, instead, on bulk surveillance on Americans by collecting network traffic abroad. Other types of surveillance operations are also authorized under EO 12333, including malware deployment.[78] With regard to actual bulk surveillance operations, the public has learned how the NSA assumed authority under EO 12333 to acquire communications (including those of US persons) within Google and Yahoo! networks because the operation was conducted on foreign territory under the MUSCULAR program;[79] we discuss MUSCULAR in Part II.A.

1. Overview

EO 12333 is a broad document, readily available to the public.[80] The complex web of instructions and directives implementing EO 12333 contain even more detailed rules for intelligence conduct.

Two Department of Defense (DoD) Directives fall immediately beneath EO 12333 in the legal hierarchy and contain more detailed principles on "DoD activities that may affect US persons."[81] EO 12333 and these DoD Directives form the basis of US Signals Intelligence Directive 18 (USSID 18).[82] USSID 18 was drafted by intelligence community executives in the Defense Department and approved by the Attorney General in the Justice Department.[83] USSID 18 contains fairly specific surveillance principles.[84] But many sentences and some complete paragraphs in USSID 18 remain classified. Prior to the MUSCULAR revelations on October 30, 2013, only a redacted 1993 version of USSID 18 had been released. On November 18, 2013, a 2011 version of USSID 18 was released.[85] We focus our analysis on this recently declassified, but heavily redacted, 2011 version of the document.

USSID 18 § 2 references several legal documents that further specify intelligence activities governed by the aforementioned DoD Directives, as well as a document establishing oversight procedures titled "NSA/CSS Pol-

78. *See* NATIONAL SECURITY AGENCY, *supra* note 6, at 2–3; Applebaum et al., *supra* note 63; *NSA Documents*, *supra* note 63.

79. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 12.

80. Exec. Order No. 12,333, 3 C.F.R. (1981).

81. U.S. DEP'T OF DEF. Directive 5240.01, *DOD Intelligence Activities* (Aug. 2007); U.S. DEP'T OF DEF. Directive 5240.1-R, *Procedures Governing the Activities of DOD Intelligence Components That Affect United States Persons* (Dec. 1982).

82. *See* USSID 18, *supra* note 5, § 2.1.

83. *Id.* (while the procedures of approval are still unclear due to the classified documents, USSID 18 was approved by Attorney General Janet Reno in 1997).

84. *See id.* §§ 4–9.

85. *See* USSID 18, *supra* note 5, at 1 (approved for release by the NSA on Nov. 13, 2013).

icy No. 1-23, procedures governing NSA/CSS Activities that affect US persons."[86] Interestingly, the latter document references a classified Annex A of EO 12333.[87] Some commentators have pointed toward the existence of this Annex, which sits right at the top of the legal hierarchy.[88] It appears that the same Annex is mentioned in a redacted public version of NSA/CSS Policy No. 1-23.[89] Although we are not in a position to further reflect on the classified content of this Annex, its existence serves as a reminder that additional loopholes may exist beyond those identified in this Part.

2. Scope of FISA: Surveillance Abroad is Not "Electronic Surveillance"

Internet surveillance falls within the EO 12333 regime when it is conducted on foreign soil and does not fall within the 1978 FISA definition of "electronic surveillance."[90] As the NSA recently put it, EO 12333 applies when surveillance is "conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA."[91]

While FISA surveillance is conducted on US soil, EO 12333 surveillance is mostly conducted abroad.[92] EO 12333 presumes that network traffic, intercepted on foreign soil, belongs to non-US persons.[93] Companies and associations are also considered in the EO 12333 definition of "US persons."[94] These entities may be assumed to be non-US persons if they have their headquarters outside the United States. Even when it is known to the NSA that a company is legally controlled by a US company, EO 12333 does not prohibit the NSA to assume such an entity to be a non-US person under USSID 18. Taken together, the hurdles for presuming that surveillance does not affect a US person under EO 12333 are low. By contrast, FISA minimi-

86. *Id.* § 2.1.

87. *See* NSA / CENT. SEC. SERV., NSA/CSS POLICY NO. 1-23 - PROCEDURES GOVERNING NSA/CSS ACTIVITIES THAT AFFECT U.S. PERSONS § 8(f) (Mar. 2004), *available at* http://cryptome.org/nsa-css-1-23.pdf.

88. *See* Marcy Wheeler, *Snowden: "A Classified Executive Order"*, EMPTYWHEEL (May 30, 2014), https://www.emptywheel.net/2014/05/30/snowden-a-classified-executive-order.

89. *See* NSA, *supra* note 87, annex.

90. *See supra* Part I.B.2.

91. *See* NATIONAL SECURITY AGENCY, *supra* note 6, at 2. The statement seems to suggest that all surveillance operations, even domestic ones, that do not fall with the 1978 FISA definition are regulated by EO 12333. In this Article, we focus on advanced network surveillance operations conducted from abroad, but how to exactly draw the line between FISA and EO 12333 applicability, and how EO 12333 might regulate domestic operations, is an important subject for public debate and further research.

92. *See supra* Part I.B.2.

93. USSID 18, *supra* note 5, § 9.8 (defining "foreign communications").

94. *Id.* at § 9.18.e.2 (defining "U.S. person").

zation policies direct authorities to presume that surveillance operations conducted on US soil affect US persons.[95]

INSTALLING A DEVICE. To understand how EO 12333 regulates the network protocol manipulations described in Part II.B, we now return to the question of "installing a device."[96] These manipulations fall under EO 12333. However, on top of the 1978 FISA definition of "electronic surveillance," neither EO 12333 nor the 2011 update of USSID 18 further specify what "installing a device" means today.[97] It is not covered in the definitions of "collection,"[98] "interception,"[99] or "electronic surveillance."[100] The definition of "installing a device" to enable surveillance could possibly be redacted in USSID 18 or further specified in a still-classified guideline. A post-Snowden NSA memorandum does not provide any clarity. To the contrary:

> N.S.A. uses EO 12333 authority to collect foreign intelligence from communications systems around the world. Due to the fragility of these sources, providing any significant detail outside of classified channels is damaging to national security.[101]

One recently leaked document seems to suggest that EO 12333 governs untargeted malware attacks and strategies. The revealed slide on the VALIDATOR program indicates that the VALIDATOR malware is deployed in an untargeted fashion on many machines. Once the VALIDATOR malware infects a given machine, the infected machine contacts a "listening post" server. Finally, analysts at the listening point perform a "USSID-18 check" to "validate the targets identity and location" and thus decide whether "a more sophisticated . . . implant" may be deployed on the infected machine.[102] Importantly, the USSID 18 check is only performed *after* the untargeted VALIDATOR malware has been deployed.[103] In other words, legal protection comes into play only after the NSA knows who it is targeting, based on the identity of a target or the location of his/her machine. This is consistent with our contention that the 1978 FISA definition of "installing a device" does not cover the advanced network manipulations presented in Part II.B.[104]

---

95. *See supra* Part I.B.3.
96. *See also supra* Part I.B.2.
97. Exec. Order No. 12,333, 3 C.F.R. (1981).
98. USSID 18, *supra* note 5, § 9.2.
99. *Id.* § 9.11.
100. *Id.* § 9.7.
101. NATIONAL SECURITY AGENCY, *supra* note 6, at 2–3.
102. Applebaum et al., *supra* note 63.
103. *Id.*
104. *See supra* Part I.B.2.

3. Legal Protections for Americans Under EO 12333

EO 12333 states that electronic surveillance should consider the rights of US persons.[105] The details of this consideration are further specified in the underlying documentation, particularly USSID 18.[106] In the Washington Post, a former NSA chief analyst claimed that surveillance regulated by EO 12333 affords fewer legal protections to Americans than operations authorized under FISA:

> N.S.A. has platoons of lawyers, and their entire job is figuring out how to stay within the law and maximize collection by exploiting every loophole . . . . It's fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA.[107]

Despite the redactions in USSID 18, the 2011 version makes several new contributions to our collective understanding of how legal protections for US persons are less restrictive under EO 12333.

Intentionally targeting US persons. This Article concentrates on not "intentionally targeting US Persons."[108] But EO 12333 establishes that electronic surveillance operations—ones that fall under its regime *and* do not fall under the FISA regime—may intentionally intercept US persons' communications as long as they meet the requirements summed up in USSID 18. USSID 18 § 4 is titled "Collection" and contains an entire section that is completely redacted.[109] Moreover, § 4.1 spans four full pages of exceptions for situations in which US persons may be intentionally targeted.[110] Furthermore, a central passage of the opening paragraph of §4.1 is redacted. It reads:

> 4.1. Communications which are known to be to, from or about a U.S. PERSON [one complete line redacted] not be intentionally intercepted, or selected through the use of A SELECTION TERM, except in the following instances . . .[111]

In addition, the entire subsection on "international communications" is redacted.[112] These subsections would be some of many candidates for transparency that could be obtained via political oversight or FOIA requests.[113]

---

105. Exec. Order No. 12,333, 3 C.F.R. (1981).
106. *See* USSID 18, *supra* note 5.
107. Gellman & Soltani, *supra* note 13.
108. 50 U.S.C. § 1801(f) (2012).
109. USSID 18, *supra* note 5, § 4.2.
110. *See* USSID 18, *supra* note 5, § 4.1.
111. *Id.*
112. *Id.* § 4.1(b)(1)(b).
113. FOIA requests have been made, but unfortunately, as of February 2015, we have not seen anything useful about the redactions in USSID 18 that we mention here. *See generally* American Civil Liberties Union, *Executive Order 12,333 - FOIA Lawsuit*, ACLU (Feb. 3,

There are other specific exceptions where "communications which are known to be to, from, or about US persons" may be "intentionally intercepted."[114] Even with the many redactions, it is possible to see that the exceptions provide more diminished protections on critical points than the already permissive "minimization procedures" under FISA.

Often, instead of FISA Court approval, some operations merely require the Attorney General or the NSA Director's approval.[115] Out of dozens of scenarios mentioned, one especially interesting instance is the *consent* exception.[116] It states that when US persons (including US corporations) consent to a surveillance operation, the approval of the Director of the NSA suffices to go ahead with a program as long as the surveillance does not fall within the FISA regime. Indeed, May 2014 saw revelations on NSA's "strategic partnerships" with several leading corporations, which may point to a "consent"-based relationship.[117]

To clarify the impact of the *consent* exception, consider the following hypothetical example of how it could be interpreted and applied: the NSA might ask for and obtain consent from AT&T—a "US person" because the AT&T headquarters are located in Texas—to tap and collect all traffic flowing through an AT&T switch located abroad. Traffic (both "content" and "metadata") at this switch could then be collected, regardless of whether it contains communication records of Americans or foreigners. Perhaps the underlying rationale for operation MUSCULAR[118] was a situation in which Google and Yahoo! did not provide such consent, spurring the intelligence community to seek other ways to access to the data. However, several sentences in USSID 18 remain redacted,[119] thus prohibiting us from establishing scenarios with complete certainty and leaving our hypotheticals a thought exercise. To enable further understanding of the scope of surveillance abroad on Americans, authorized by unilateral approval by the Director of the NSA combined with the "consent" of US corporations, it would be useful to target political pressure or FOIA requests at USSID 18 § 4.

WIDE EXEMPTIONS TO PROCESS US PERSON DATA ALREADY COLLECTED. Under USSID 18, further processing of communications of foreigners after

---

2015), https://www.aclu.org/national-security-technology-and-liberty/executive-order-12333-foia-lawsuit.

114. USSID 18, *supra* note 5 §§ 4.1(a)–(d).

115. *Id.* § 4.1(b) (requiring Attorney General's approval); *Id.* § 4.1(c) (requiring the Director of NSA's approval).

116. *See id.* § 4.1(c)(1).

117. *See* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE US SURVEILLANCE STATE (Metropolitan Books, 2014), *available at* https://usnewsghost.wordpress.com/2014/05/14/latest-nsa-edward-snowden-documents-slides-leaks-no-place-to-hide-documents-pdf-glenn-greenwald.

118. *See supra* Part II.A.1.

119. USSID 18, *supra* note 5, § 4.1.

collection is unrestrained.[120] In addition, there are several generous exemptions that allow for further processing of communication between US persons intercepted during the collection of foreign communications, including when communications are encrypted; when they are significant for foreign intelligence purposes; when they are useful as evidence in criminal proceedings and when they are helpful to reveal communications security vulnerabilities.[121] Under USSID 18, the NSA Director decides whether these scenarios apply, and whether communications between US persons can be retained pursuant to procedures approved by the Attorney General.[122] Under FISA, the Attorney General makes such determinations subsequent to procedures approved by the FISA Court.[123]

4. The Official NSA Response to Our Analysis

As noted in the Introduction to this Article, coverage of an earlier online version of this Article by *CBS News* spurred an official response from the NSA compliance department.[124] The relevant part of the media report reads as follows:[125]

> However, an N.S.A. spokesperson denied that either EO 12333 or USSID 18 authorizes targeting of U.S. persons for electronic surveillance by routing their communications outside of the U.S., in an emailed statement to CBS News.
>
> 'Absent limited exception (for example, in an emergency), the Foreign Intelligence Surveillance Act requires that we get a court order to target any U.S. person anywhere in the world for electronic surveillance. In order to get such an order, we have to establish, to the satisfaction of a federal judge, probable cause to believe that the U.S. person is an agent of a foreign power,' the spokesperson said.

Our response to the NSA statement was published online on July 11, 2014, and the NSA has not yet responded.[126] The NSA statement to *CBS News* cleverly sidetracks our analysis by re-framing the issue to construct a legal situation that evades our main arguments. Specifically, the statement concentrates on the legality of "targeting US persons," an issue we barely

120. *See id.* § 5.3.
121. *Id.* § 5.4(d).
122. *Id.* § 4.1(c).
123. *See supra* note 28.
124. Zack Whittaker, *Legal Loopholes Could Allow Wider NSA Surveillance, Researchers Say*, CBS News (June 30, 2014), http://www.cbsnews.com/news/legal-loopholes-could-let-nsa-surveillance-circumvent-fourth-amendment-researchers-say.
125. *Id.*
126. Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution, the NSA Statement, and Our Response*, Freedom To Tinker, July 11, 2014, *available at* https://freedom-_to-_tinker.com/blog/axel/our-_response-_to-_the-_nsa-_reaction-_to-_our-_new-_internet-_traffic-_shaping-_paper.

analyze. Indeed, the loopholes we identify in this Article exist when 1) surveillance is conducted abroad and 2) operations do *not* intentionally target a US person. The NSA statement, therefore, does not address our concerns.

Moreover, in re-wiring the legal situation to cover the targeting of US persons, the element "absent limited exceptions (for example, an emergency)"[127] of the NSA statement is also misleading. Exceptions for targeting US persons under EO 12333 are outlined in USSID 18 § 4.[128] These exceptions span four redacted pages and include a completely classified paragraph.[129] It is impossible to tell what lies beneath those redactions, and we do not intend to speculate on their contents. Even so, it seems unlikely that one could reasonably characterize four pages of exceptions and an entirely classified paragraph—which could amount to dozens of actual scenarios—as "limited."

5. EO 12333 Reform: The Sole Province of the Executive Branch

Aside from the differences discussed thus far, EO 12333 has a more fundamental difference from FISA: over the next years, all three branches of government could be involved with Patriot Act and FISA reform. For EO 12333, this is hardly the case. International surveillance regulated under EO 12333 is overseen first and foremost by the executive branch.[130] This simple observation has a long tradition in US Constitutional law that gives broad Article II authority to the President when it comes to protecting national security against overseas threats.[131] As Part II will highlight, however, today's technologies challenge the long-standing core concept in US surveillance law that operations conducted abroad will not affect Americans in large numbers. This tension between local law and global technology surfaces in a particularly striking manner with EO 12333, which regulates surveillance operations conducted abroad.

This broad Article II constitutional authority can result in a lack of oversight, or checks and balances, between separate branches of government. Even if the Attorney General-approved procedures must be submitted to the US Senate Intelligence Committee, tasked to oversee US intelligence agencies, legal and practical constraints to oversight remain.[132] These constraints

127. *See* Whittaker, *supra* note 124.

128. *See supra* Part I.B.3.

129. *Id.*

130. Kenneth R. Mayer, *Executive Orders and Presidential Power*, 61 J. POL. 445, 452 (1999) (stating that "executive orders are a unilateral presidential tool").

131. *See* John C. Duncan, *A Critical Examination of Executive Orders: Glimmerings of Autopoiesis in the Executive Role*, 35 VT. L. REV. 333, 346 (2010).

132. *See* Tye, *supra* note 11; PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., *supra* note 12; *See also* Mark Danner, *He Remade Our World*, THE NEW YORK REVIEW OF BOOKS (Apr. 3, 2014), *available at* http://www.nybooks.com/articles/archives/2014/apr/03/dick-cheney-he-remade-our-world/; Ryan Lizza, *State of Deception*, THE NEW YORKER (Dec. 13, 2013), *available at* http://www.newyorker.com/magazine/2013/12/16/state-of-deception.

range from the executive branch constructing permanent emergency national security scenarios that obstruct oversight, to Congress being practically barred from oversight via classification to practical constraints that include being forbidden to take notes or bring assistants to briefings. The Committee Chair, Senator Dianne Feinstein, said that EO 12333 "programs are under the executive branch entirely," and have "few, if any, privacy protections."[133]

The relative lack of authority for EO 12333 policies in the broader policy arena, beyond the executive branch, might explain why there are still so many redactions in place in USSID 18. In any event, considering the legal loopholes in EO 12333 and the technical means by which they can be exploited,[134] EO 12333 reform is urgent to protect Americans' privacy. Although the PCLOB announced in July 2014 that it will investigate EO 12333 policies,[135] the PCLOB reports directly to the President; technically, the investigation cannot be said to be fully independent because the executive branch controls the prospects of EO 12333 reform as investigated by the PCLOB.

Finally, during its annual intelligence community budget negotiations in December, 2014, Congress introduced and approved a new legal provision, all within forty-eight hours. This provision could have deep implications for protections afforded to US persons during surveillance operations conducted abroad. Intelligence Authorization Bill 2014–15 § 309[136] mandates that the Attorney General set a five year retention limit on data collected abroad that involves US persons, thereby codifying similar provisions similar to USSID 18.[137] This provision was introduced shortly before the deadline of the budget negotiations, hardly debated, and approved within forty-eight hours

133. Ali Watkins, *Most Of NSA's Data Collection Authorized By Order Ronald Reagan Issued*, McClatchyDC (Nov. 31, 2013), *available at* http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html; *See also* Privacy & Civil Liberties Oversight Bd.,*supra* note 12.

134. *See infra* Part II.

135. Privacy and Civil Liberties Oversight Bd., *PCLOB Posts Status of Attorney General-Approved U.S. Person Procedures Under Executive Order 12333*, pclob.gov (Feb. 19, 2015), https://www.pclob.gov/newsroom/20150219.html (stating that the PCLOB ". . . plans to prepare one or more public reports on E.O. 12333 activities.").

136. Intelligence Authorization Act for Fiscal Year 2015, Pub. L. 113-293, 128 Stat. 3990.

137. *See supra* Part II.C.3; U.S. House of Representatives Permanent Select Comm. on Intellegence, Fact Sheet on H.R. 4681, The Fiscal Year 2015 Intelligence Authorization Act (Dec. 12, 2014), http://intelligence.house.gov/press-release/fact-sheet-hr-4681-fiscal-year-2015-intelligence-authorization-act (the official record mentioning that "although the executive branch already follows procedures along these lines, Section 309 would enshrine the requirement in law").

by both the Senate and the House.[138] The bill was then sent to the President, who signed the bill into law shortly thereafter.

The wording of § 309 leaves many open questions of interpretation. It has become the subject of considerable controversy and debate amongst lawmakers, the media, and the public. For instance, it is unclear how § 309 relates to FISA §§ 703 and 704, which afford more robust protections to US persons when data is collected abroad.[139] One plausible explanation could be that the new provision legitimizes an already existing surveillance operation that collects huge amounts of US person data on foreign soil, without approval of the FISA Court.[140] This would be an intelligent move from a compliance perspective. By approving § 309, Congress might have created a statutory basis for further uses of data collected abroad, formerly based on USSID 18 minimization procedures merely approved by the Attorney General. With § 309, diminished legal protections to Americans under USSID 18 minimization procedures could have a chance to become statute, making the legitimacy of programs based on EO 12333 and USSID 18, like MUSCULAR,[141] no longer an issue if a court would find these now disclosed programs should have been based on FISA and reviewed by the FISA Court.

The lack of comprehensive legislative debate on § 309 renders it impossible to come to robust conclusions on its implications. At this point, this is merely an issue for further research. But one can criticize the approval both in the House and the Senate of such critical surveillance policy introduced 48 hours before a budgetary deadline, without proper legislative debate to establish the actual meaning of a provision or to express the intent of the legislature.

§ 309 could go down as a historic moment in surveillance policy. It could entail a significant depression of legal protections afforded to US persons when data is collected abroad. It is also apparently the first time that Congress involved itself directly with data collection and retention usually regulated under EO 12333. Paradoxically, the effect of § 309 might be a legal precedent for more transparently deliberated, better informed and perhaps privacy protective approaches going forward.

D. *Summary*

Surveillance programs under EO 12333 might collect startling amounts of sensitive data on both foreigners and Americans. Agents acting under the

138. *See* Facebook Page of Rep. Justin Amash, FACEBOOK (Dec. 10, 2014, 9:10 PM), https://www.facebook.com/repjustinamash/posts/812569822115759.

139. *See supra* Part I.B.

140. *See* Marcy Wheeler, *Section 309: A Band-Aid for a Gaping Wound in Democracy*, EMPTYWHEEL (Dec. 14, 2014), https://www.emptywheel.net/2014/12/14/section-309-a-band-aid-for-a-gaping-wound-in-democracy (discussing public statements made by Bob Litt, General Counsel in the Office of the Director of National Intelligence).

141. *See infra* Part II.A.1 (providing a more detailed discussion of this program).

authority of EO 12333 and USSID 18 may presume communications are non-American, precisely because their operations are conducted abroad. Such operations are regulated by guidelines adopted almost entirely within the executive branch, without any meaningful congressional or judicial involvement. Generous exemptions, more permissive than under FISA, enable use of information "incidentally" collected on US persons, and critical details remain classified. These concerns remain primarily within the purview of the executive branch. So far, the executive branch has not yet sufficiently addressed these concerns. The lack of checks and balances between three branches of government in this respect is likely exacerbating the situation.

Oversight between branches of government and constitutional safeguards can be circumvented by designing surveillance operations in ways that lead to application of the EO 12333 regime, instead of FISA. Consequently, regardless of the outcome of Patriot Act and FISA reform, EO 12333 will continue to provide opportunities for largely unrestrained surveillance on Americans from abroad.

II. Loopholes that Exploit Network Protocols

The collection of a US person's network traffic from abroad presents a loophole that can be exploited to circumvent both legal safeguards protecting Americans' privacy and oversight mechanisms established by other branches of government. The current regulatory framework, therefore, creates incentives for intelligence agencies to conduct surveillance operations on foreign soil, regardless of whether these operations actually affect American communications.

This Part discusses how the Internet's core protocols can cause traffic sent by Americans to be routed abroad, where data can be collected under the most permissive third legal regime for network surveillance. We distinguish two settings: 1) situations where the vagaries of Internet protocols cause Americans' traffic to naturally be routed abroad, and 2) situations where Internet protocols are deliberately manipulated to cause Americans' traffic to be routed abroad.

A. *US Traffic Can Naturally Be Routed Abroad*

The Internet was not designed around geopolitical borders; instead, its design reflects a focus on providing robust and reliable communications while minimizing cost. In this section, we discuss why it is not uncommon for network traffic between two endpoints located on US soil to be routed outside the United States, both in the *intradomain* (within a single organization's network) and the *interdomain* (between different networks run by different organizations) settings. Traffic between two US endpoints that is naturally routed abroad can then be collected abroad under the permissive EO 12333 regime.

1. Interception in the Intradomain

A network owned by a single organization can be physically located in multiple jurisdictions, even if a company or organization is nominally headquartered in the US, like Yahoo! or Google. The revealed MUSCULAR program illustrates how the NSA presumed authority under EO 12333 to acquire traffic between company servers by tapping fiber-optic cables on foreign territory (in the United Kingdom), collecting up to 180 million user records per month, regardless of nationality.[142] Companies like Yahoo! and Google replicate data across multiple servers that periodically send data to each other, for backup and synchronization.[143] These servers are located in different countries to prevent valuable data from being lost in case of outages or errors in one location.[144] The MUSCULAR program collects the traffic sent between these data centers: although this traffic traverses multiple national jurisdictions, it remains within the logical network boundaries of the internal corporate networks of Yahoo! and Google. This is one example where loopholes under the legal regime of EO 12333 were utilized in the *intradomain*, i.e., within the logical boundaries of a network owned by a single organization.

2. Interception in the Interdomain

Another method for utilizing the EO 12333 legal regime is the *interdomain* setting, where digital traffic traverses networks belonging to different organizations. Specifically, interdomain routing with the Border Gateway Protocol (BGP) can naturally cause traffic originating in a US net-

142. *See* Tye, *supra* note 11 (the fact that collection is done on British territory was noted here: "We do not know exactly how the NSA and GCHQ intercept the data, other than it happens on British territory."); Barton Gellman, Ashkan Soltani, and Andrea Peterson, *How We Know The NSA Had Access To Internal Google And Yahoo Cloud Data*, THE WASHINGTON POST, Nov. 4, 2013, *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data.

143. GOOGLE, *Data and Security*, http://www.google.com/about/datacenters/inside/data-security/index.html ("Rather than storing each user's data on a single machine or set of machines, we distribute all data—including our own—across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure.") (last visited May 3, 2015); GOOGLE, *Data Center Locations*, http://www.google.com/about/datacenters/inside/locations/index.html (google datacenter location are distributed worldwide); YINGYING CHEN ET AL., A FIRST LOOK AT INTER-DATA CENTER TRAFFIC CHARACTERISTICS VIA YAHOO! DATASETS, presented at IEEE INFOCOM 2011, *available at* http://www-users.cs.umn.edu/~yingying/papers/infocom11-yingying-paper.pdf (Yahoo datacenter locations).

144. GOOGLE, *Data and Security*, http://www.google.com/about/datacenters/inside/data-security/index.html ("Rather than storing each user's data on a single machine or set of machines, we distribute all data—including our own—across many computers in different locations. We then chunk and replicate the data over multiple systems to avoid a single point of failure.") (last visited May 3, 2015).

work to be routed abroad, even when it is destined for a network that is located on US soil.

BGP is the routing protocol that enables communication between Autonomous Systems (ASes),[145] which are networks owned by different organizations.[146] ASes are interconnected,[147] creating a graph where nodes are ASes and edges are the links between them.[148] ASes use BGP to learn paths through the AS-level graph: an AS discovers a path to a destination AS via BGP messages received from each of its neighboring ASes.[149] An AS then uses its local routing policies to choose a single most-preferred path to the destination AS from the set of paths it learned from its neighbors. The AS then forwards all traffic for the destination AS to the neighboring AS that announced the most-preferred path.[150]

Importantly, the local policies used to determine route selection in BGP are typically agnostic to geopolitical considerations; path selection is often based on the price of forwarding traffic to the neighboring AS that announced the path, as well as on the number of ASes on the path announced by that neighbor.[151] This means that it can sometimes be cheaper to forward traffic through a neighboring AS that is physically located in a different country. This situation is common, for example, in South America, where network paths between two South American endpoint ASes often cross undersea cables to Miami,[152] and Canada, where network paths between two Canadian endpoint ASes regularly traverse American ASes.[153]

3. The NSA's Ability to Intercept Traffic on Foreign Soil

Recent revelations indicate that the NSA has the capability to collect Internet traffic on foreign soil by tapping into transnational fiber-optic cables. A single transnational fiber-optic cable can aggregate huge volumes of both interdomain and intradomain telecommunications (including Internet, telephony, facsimile, and VoIP traffic) generated by hundreds of dif-

145. Yakov Rekhter & Tony Li, *RFC1771: A Border Gateway Protocol 4 (BGP-4)*, The Internet Eng'g Task Force, p. 1, (Mar. 1995), *available at* http://tools.ietf.org/html/rfc1771.

146. E.g., Google's network, China Telecom's network, or Boston University's network.

147. Rekhter, *supra* note 145.

148. *See infra* Fig. 2 at Part II.B.1 for a graphical representation that discusses a deliberate BGP manipulation to route Internet traffic abroad.

149. Rekhter, *supra* note 145.

150. *Id.*

151. Matthew Caesar & Jennifer Rexford, *BGP Routing Policies in ISP Networks*, IEEE Networks Mag., Nov.–Dec. 2005 at 5, 6, *available at* http://web.engr.illinois.edu/~caesar/papers/policies.pdf.

152. Doug Madory, *'Crecimiento' in Latin America*, Dyn Research (May 23, 2013), http://www.renesys.com/2013/05/crecimiento-in-latin-america.

153. *See* IXmaps, http://ixmaps.ca (last visited May 3, 2015) (ongoing work by Sharon Goldberg seeks to measure how often this occurs when both endpoints are located in the US).

ferent ASes.[154] This sub-Part briefly describes cable-tapping activities apparently connected by a division of the NSA known as Special Sources Operation (SSO).[155]

One program, codenamed WINDSTOP, deals with collection from so-called "second party" countries (the United States, the United Kingdom, Canada, New Zealand, Australia). The MUSCULAR program (discussed in Part II.A.1) falls under the umbrella of WINDSTOP, as does the INCENSER program, which likely collects billions of records each month.[156] INCENSER involves tapping into the network linking one trans-Atlantic fiber-optic cable from the United States to the United Kingdom (the "FLAG Atlantic 1" cable) to another transnational cable from the United Kingdom to Japan via the Mediterranean, India, and China (the "FLAG Europe Asia" cable).[157] The cable was tapped on British soil by the British Government Communications Headquarters (GCHQ), and the collected traffic was shared with the NSA.[158]

Moreover, the NSA's RAMPART-A operation is a cable-tapping program undertaken in collaboration with a foreign "third-party" country, i.e., a country other than one of the "five eye" countries.[159] The foreign country taps into international fiber-optic cables located on its own territory, moves

---

154. *See, e.g.*, FLAG TELECOM, http://sdc.flagtelecom.com/network/flag_atlantic_1.html (last visited May 3, 2015) (The FLAG Atlantic 1 cable from the U.K. to the U.S. for instance has a potential capacity of 4.8 terabit per second.).

155. The SSO division "had an official seal that might have been parody: an eagle with all the world's cables in its grasp." Barton Gellman, *Edward Snowden, After Months Of NSA Revelations, Says His Mission's Accomplished*, WASH. POST, Dec. 23, 2013, http://www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html.

156. In the same thirty-day period, the numbers of records collected by the INCENSER program were over two orders of magnitude higher than those collected by MUSCULAR. *See* Gellman, *supra* note 13.

157. *Submarine Cable Map*, TELEGEOGRAPHY SUBMARINE CABLE MAP, http://www.submarinecablemap.com (last visited May 3, 2015); Neal Stephenson, *Mother Earth Mother Board*, WIRED (Dec. 1996), *available at* http://archive.wired.com/wired/archive/4.12/ffglass.html?topic=&topic_set=.

158. Details of the INCENSER program were revealed by Geoff White, *Spy Cable Revealed: How Telecoms Firm Worked With GCHQ*, CHANNEL 4 (Nov. 20, 2014), *available at* http://www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq; Frederik Obermaier et al., *Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts*, SÜDDEUTSCHE ZEITUNG INTERNATIONAL (Nov. 25, 2014), *available at* http://international.sueddeutsche.de/post/103543418200/snowden-leaks-how-vodafone-subsidiary-cable.

159. For a description of the "five eye" countries, *see supra* note 18. Anton Geist et al., *NSA 'Third Party' Partners Tap The Internet Backbone In Global Surveillance Program*, INFORMATION (June 19, 2014), *available at* http://www.information.dk/501280; Ryan Gallagher, *How Secret Partners Expand NSA's Surveillance Dragnet*, THE INTECEPT (June 19, 2014), *available at* https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a.

the raw traffic to a processing center on its territory that contains NSA-provided equipment, and forwards the traffic to a NSA site on US soil.[160] The three largest RAMPART sites—codenamed AZUREPHOENIX, SPINNERET, and MOONLIGHTPATH—tap a total of seventy different international cables; although the locations of various sites remain unknown, media reports suggest that both Germany and Denmark are involved.[161]

B. *How Deliberate Manipulations Can Divert US Traffic Abroad*

In addition to situations where Americans' traffic is naturally routed abroad, the Internet's core protocols—BGP and DNS—can be deliberately manipulated to force traffic originating and terminating in an American network to be routed abroad. Deliberately manipulating Internet protocols for subsequent data collection from abroad, even when the manipulation was performed from within the United States, does not fall under FISA's definition of "electronic surveillance."[162] Instead, these manipulations are regulated under the most permissive third legal regime for network surveillance, EO 12333 (and perhaps further specified in non-public guidelines).[163]

1. Deliberate BGP Manipulations

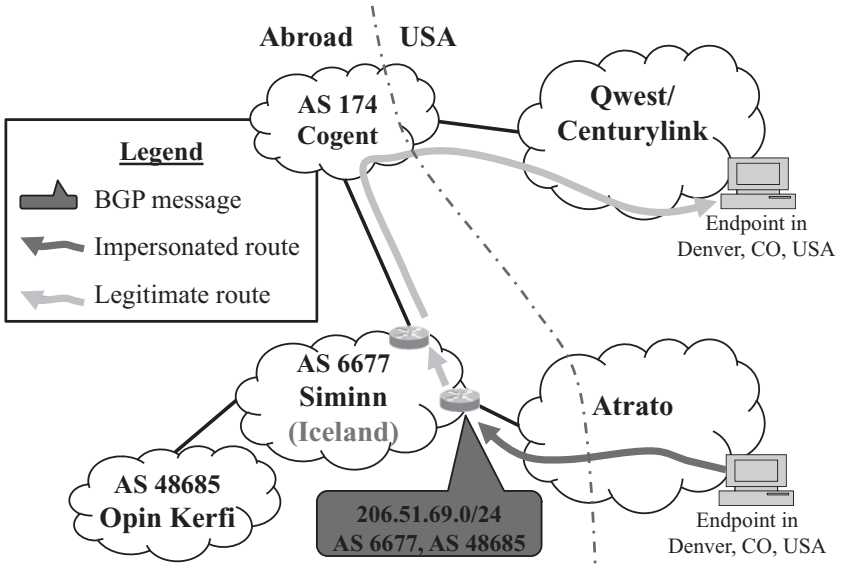
Manipulations of the BGP protocol can cause network traffic to take unusual paths. There have been numerous real-world incidents demonstrating this, including situations where traffic from two American endpoint ASes was rerouted through ASes physically located abroad.[164] Although there is no evidence that these incidents were part of a surveillance operation, or even a clear understanding of why they occurred, it is instructive to consider them as examples of how government agencies could circumvent the legal safeguards protecting US persons by forcing their network traffic to be diverted abroad and intercepting it on foreign soil.

In 2013, global Internet monitoring and research company Renesys observed a number of highly-targeted manipulations of BGP that caused traffic

160. *Id.*
161. *Id.*; Geist et al., *supra* note 159.
162. *See supra* Parts I.B.2 & I.C.2.
163. *See supra* Part I.C.
164. For a scientific survey of these issues, *see* Sharon Goldberg, *Why is it taking so long to secure internet routing?*, ACMQUEUE (Sept. 11, 2014), *available at* http://queue.acm.org/detail.cfm?id=2668966; Kevin Butler et al., *A Survey Of BGP Security Issues And Solutions*, 98 PROC. OF THE IEEE 100 (2010). For some real-life examples, *see* A. Peterson, *Researchers Say U.S. Internet Traffic Was Re-routed Through Belarus. That's a Problem*, WASH. POST, Nov. 20, 2013, http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/20/researchers-say-u-s-internet-traffic-was-re-routed-through-belarus-thats-a-problem/; Declan McCullagh, *How Pakistan knocked Youtube offline (and how to make sure it never happens again*, CNET (Feb. 25, 2008), *available at* http://www.cnet.com/news/how-pakistan-knocked-youtube-offline-and-how-to-make-sure-it-never-happens-again/; Jim Cowie, *China's 18-minute Mystery*, DYN RESEARCH, November 18, 2010, *available at* http://www.renesys.com/blog/2010/11/chinas-18-minute-mystery.shtml.

sent between two American endpoint ASes to be routed through Iceland.[165] On August 2, 2013, manipulator AS Siminn in Iceland used BGP to send an "impersonated route" for an IP address block, allowing Siminn to intercept traffic sent between two endpoints in Denver, Colorado.[166] A summary of that manipulation is shown in Figure 2, below.

FIGURE 2: ON JUNE 31, 2013, MANIPULATOR AS SIMINN IN ICELAND USED BGP TO SEND AN "IMPERSONATED ROUTE" FOR IP ADDRESS BLOCK 206.51.69.0/24, ALLOWING SIMINN TO INTERCEPT TRAFFIC SENT BETWEEN TWO ENDPOINTS IN DENVER, CO, USA.[167]



Traffic, originating at an endpoint physically located in Denver and logically located inside Atrato's AS, travels to an Icelandic AS (Siminn) and then back to its destination (physically located in Denver and logically located in Qwest/Centurylink's AS).[168] Renesys also observed an AS based in Belarus performing similar BGP manipulations.[169]

Similar incidents have occurred periodically across the Internet.[170] In 2010, for example, a routing incident caused traffic sent between multiple

165. *See* Andrea Peterson, *Researchers Say U.S. Internet Traffic Was Re-routed Through Belarus. That's a Problem*, WASH. POST: THE SWITCH, (Nov. 20, 2013), http://www.washingtonpost.com/blogs/the-switch/wp/2013/11/20/researchers-say-u-s-internet-traffic-was-re-routed-through-belarus-thats-a-problem.

166. *See* Cowie, *supra* note 164. *See also* USSID 18, *supra* note 5.

167. *See* Jim Cowie, *The New Threat: Targeted Internet Traffic Misdirection*, RENESYS BLOG (Nov. 19, 2013), http://www.renesys.com/2013/11/mitm-internet-hijacking/.

168. *Id.*

169. *Id.*

170. *See* Butler, *supra* note 164.

American endpoint ASes to be diverted through China Telecom during a single eighteen-minute time period.[171] In 2008, a presentation at DEFCON demonstrated how these manipulations could be performed in a covert manner.[172] This method could be used to confound the network measurement mechanisms[173] that researchers used to detect the 2010 and 2013 incidents mentioned above.

TARGET OF THE BGP MANIPULATION. Understanding the targets of surveillance informs how the legal framework applies to BGP manipulations for the purpose of surveillance. The incidents mentioned above are executed as follows. The manipulating AS depicted in Figure 2 (Icelandic AS Siminn) manages to divert traffic to itself by sending BGP messages that "impersonate" those sent by the legitimate destination AS (Qwest/Centurylink's AS) to carefully selected neighboring ASes.[174] Because BGP lacks authentication mechanisms, these neighbors (Atrato's AS) accept the BGP message for the impersonated route, and select the impersonated route.[175] The neighbors (Atrato) then forward their traffic along the impersonated route to the manipulator's AS (Icelandic AS Siminn).[176] The manipulator receives the traffic and forwards it back to the legitimate destination AS (Qwest/Centurylink) via a legitimate route.[177] The manipulator AS therefore becomes a man-in-the-middle between the targeted source AS (Atrato) and the destination AS (Qwest/Centurylink). Although Figure 2 shows traffic between two individual endpoints within Atrato and Qwest/Centurylink being intercepted by the BGP manipulation, typically all traffic originating inside Atrato and destined to the Qwest/Centurylink AS would be intercepted by the manipulator.[178]

To further understand the targets of this manipulation, we consider what it means to send BGP messages that "impersonate" a legitimate destination AS. A BGP message is used to advertise the path to a specific IP address block hosted by a particular destination AS.[179] Each AS is allocated one or

171. Cowie, *supra* note 164.

172. Anton Kapela and Alex Pilosov, *Stealing The Internet*, DEFCON 16 (Aug. 10, 2008), *available at* https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf.

173. Typically, researchers identify BGP manipulations using diagnostic tools like traceroute, G. Malkin, *Traceroute Using an IP Option*, THE INTERNET ENG'G TASK FORCE, (Jan. 1993), http://tools.ietf.org/html/rfc1393, or BGP looking glasses, David Meyer, University of Oregon Route Views Archive Project, http://www.routeviews.org (last accessed Apr. 28, 2015). However, a clever and dedicated adversary can use various techniques to avoid detection by these diagnostic tools, as demonstrated by Kapela and Pilosov at DEFCON 2008. Kapela, *supra* note 172.

174. Cowie, *supra* note 167.

175. *Id.*

176. *Id.*

177. *Id.*

178. *Id.*

179. An Internet Protocol (IP) address is a numerical address used to identify a particular device connected to the Internet; IP addresses are 32-bit numbers, divided into four 8-bit octets

more IP address blocks, used to identify devices operated by that AS.[180] Multiple devices can use a single IP address;[181] thus, a single IP address can be used by multiple devices or persons. A separate BGP message is used to advertise each IP address block allocated to a particular destination AS.[182]

Sending a BGP message that "impersonates" a legitimate destination AS means that the manipulator AS (Icelandic AS Siminn) sends a BGP message that claims a false route to the IP address block (206.51.69.0/24). As shown in Figure 2, the manipulator AS (Siminn) falsely claims that the IP address block 206.51.69.0/24 is allocated to Siminn's own customer AS, the Icelandic Opin Kerfi AS 48685. In reality, that IP address block is allocated to the legitimate destination AS (Qwest/Centurylink). Because BGP lacks mechanisms that can authenticate allocations of IP address blocks, the manipulator's neighbors will accept this impersonated route, and forward all traffic destined to the IP addresses in the disputed block to the manipulator's AS[183] (Siminn) instead of the legitimate destination (Qwest/Centurylink). This impersonated route will continue to propagate through the network as the ASes that select the impersonated route pass it on to their own neighbors.

The target of this BGP manipulation is 1) all traffic sent by each source AS that selected the impersonated route (e.g., all traffic from Atrato) that 2) is sent to IP addresses in the block that the manipulator falsely claims is allocated to him (e.g., the 256 IP addresses contained in the block 206.51.69.0/24). This has important legal implications: EO 12333's permissive legal regime applies to these surveillance operations, since they do not "intentionally" target a "known, particular US person."[184]

One question here is whether targeting Atrato or Qwest/Centurylink could be seen as "intentionally targeting a US person," which could mean FISA applies.[185] This issue arises because companies may also be recognized as "US persons" under FISA and EO 12333.[186] Although we cannot be fully

---

(written as, e.g., 206.51.69.201). An IP address block is a set of IP addresses that have a common n-bit prefix. For example, the set of IP addresses {206.51.69.0, 206.51.69.1, . . . 206.51.69.255} has a common 24-bit prefix. We write this as address block 206.51.69.0/24, where the notation /24 ("slash twenty four") implies a common 24-bit prefix (here 206.51.69) for all addresses in the block. For more details, *see Number Resources*, INTERNET ASSIGNED NUMBERS AUTHORITY, https://www.iana.org/numbers (last visited Apr. 29. 2015).

180. Rekhter & Li, *supra* note 145.

181. *See* Martin Casado & Michael J. Freedman, *Peering through the shroud: The effect of edge opacity on IP-based client identification*, PROCEEDINGS OF THE 4TH USENIX CONFERENCE ON NETWORKED SYS. DESIGN & IMPLEMENTATION Fig. 6 (2007), *available at* http://dl.acm.org/citation.cfm?id=1973430.1973443.

182. *See* Rekhter & Li, *supra* note 145.

183. *See* Cowie, *supra* note 167. For a comprehensive view of BGP security, *see* Sharon Goldberg, *Why is it taking so long to secure internet routing?*, QUEUE, Oct. 2014, at 56–63.

184. 50 U.S.C. § 1801 (2012); *see supra* Part I.C.

185. *See supra* Part I.C.

186. Corporations have been granted Fourth Amendment rights against unreasonable searches and seizures, *Hale v. Henkel*, 201 U.S. 43, 76 (1906), Fifth Amendment protection

certain how the intelligence community applies FISA and EO 12333 in practice, we can use the revealed MUSCULAR program for some clues. MUSCULAR operations intercepted Google and Yahoo! traffic from abroad under EO 12333.[187] It follows that the authorities are likely not targeting these Internet companies directly, but are instead targeting users of these services that are not yet known. Applying this logic to the Atrato/Qwest/Centurylink example, the permissive legal regime under EO 12333 is likely to apply to such situations. This would be one important point to clarify in any EO 12333 investigation, such as the one announced by the PCLOB.

Location of the BGP manipulation. This BGP manipulation, which involves sending just a single impersonated BGP message from the Icelandic AS Siminn in Figure 2, is executed entirely outside of the targeted endpoint ASes (Atrato and Qwest/Centurylink). In fact, it can be executed entirely abroad. Of course, redactions in USSID 18 and other documents result in uncertainty with regard to whether EO 12333 applies different regulations to manipulations conducted domestically versus on foreign soil. However, the example in Figure 2 indicates that any such legal distinctions would have no effect on an authority's ability to collect network traffic.

2. Deliberate DNS Manipulations

Alternatively, one could divert traffic to servers located abroad by manipulating the Domain Name System (DNS). The DNS is a core Internet protocol that maps human-readable domain names (e.g., *www.facebook.com*) to the IP addresses that identify the servers hosting the domain[188] (e.g., 69.63.176.13). Applications that wish to communicate with the domain *www.facebook.com* first perform a "DNS lookup" to learn the IP address of the server that hosts the domain, and then direct their network traffic to that IP address.[189] DNS lookups for end users and applications within a single AS are typically performed by a device called a "recursive resolver," typically located within the AS.[190] Recursive resolvers usually engage in the DNS protocol with servers located outside their AS, and return responses to DNS lookups to users and applications within their AS.[191]

---

against double jeopardy, *United States v. Martin Linen Supply Co.*, 430 U.S. 564, 569, 572 (1977), Seventh Amendment right to a trial by jury, *Ross v. Bernhard*, 396 U.S. 531, 542 (1970), and First Amendment free speech protections, *Citizens United v. FEC*, 558 U.S. 310, 342 (2010). Expanding "these [constitutional] rights has legitimized corporations as constitutional actors and placed them on a level with humans in terms of Bill of Rights safeguards." Carl J. Mayer, *Personalizing the Impersonal: Corporations and the Bill of Rights*,41 Hastings L.J. 577, 650–51 (1990).

187. *See supra* Part II.A.

188. *See generally* Cricket Liu & Paul Albitz, DNS and BIND 4–8 (Mike Loukides, 5th ed. 2006).

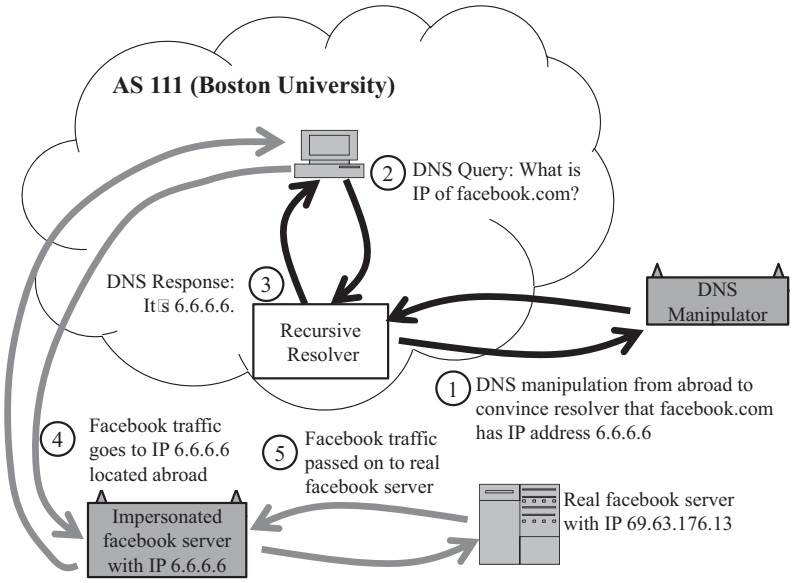
189. *Id.*

190. *See infra* Fig. 3. *See also* Liu & Albitz, *supra* note 188.

191. Liu & Albitz, *supra* note 188.

The DNS is well known to be vulnerable to manipulations that subvert the mapping from a domain name to IP address.[192] These manipulations, which have been observed in the wild as mechanisms for performing network censorship,[193] can also be used to redirect network traffic through servers located abroad. Figure 3, below, presents an example of how DNS manipulations can be used to direct traffic between two US endpoints (Boston University and Facebook) abroad. Figure 4, further below, depicts, in more detail, the DNS manipulation technique labeled (1) in Figure 3.

FIGURE 3: DNS MANIPULATIONS REDIRECTING DOMESTIC TRAFFIC ABROAD



192. Steve Bellovin, *Using The Domain Name System For System Break-Ins*, PROC. OF 5TH USENIX SECURITY SYMPOSIUM (1995), available at http://www.cse.iitd.ernet.in/~sbansal/csl865/readings/bellovin.pdf; Dan Kaminsky, *Black Ops 2008: Its The End Of The Cache As We Know It*, BLACK HAT USA (2008), available at https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf; Amir Herzberg & Haya Shulman, *Fragmentation Considered Poisonous, Or: One-Domain-To-Rule-Them-All.org*, 2013 IEEE CONFERENCE ON COMMUNICATIONS AND NETWORK SECURITY (2013). Indeed, these vulnerabilities have motivated the development of DNSSEC, a security-enhanced version of DNS. However, DNSSEC is far from being fully deployed, so these vulnerabilities remain exploitable today. Moreover the manipulation presented by Hertzberg and Shulman circumvents all known protections of DNS (including source port randomization) apart from full-fledged DNSSEC.

193. Jonathan Zittrain & Benjamin Edelman, *Internet Filtering In China*, IEEE Internet Computing, 7(2), 70–77 (2003), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399920; *see also* THE OPEN NETWORK INITIATIVE, http://opennet.net/.

Suppose that a manipulator wants network traffic destined to *www.facebook.com* from a given source AS (e.g., Boston University) to be routed through a foreign server located abroad. Suppose the foreign server has IP address 6.6.6.6. The manipulator can execute a DNS manipulation that causes the recursive resolver in the source AS (Boston University) to map *www.facebook.com* to IP address 6.6.6.6.[194] All network traffic for *www.facebook.com* from the source AS (Boston University) will then flow to the foreign server at IP address 6.6.6.6. Finally, the foreign server will silently forward the traffic it receives to the real Facebook server at IP address 69.63.176.13.[195] Thus, the foreign server becomes a man-in-the-middle for traffic sent between two US endpoints (Boston University and *www.facebook.com*).

TARGET OF THE DNS MANIPULATION. As with manipulations of the BGP protocol, the surveillance law applied is based on the identity of the target. The DNS manipulation is more targeted than the BGP manipulation we discussed earlier: it targets all traffic to a particular domain that is sent by all users and applications served by the targeted recursive resolver (i.e., within Boston University's AS). Meanwhile, the BGP manipulation, discussed above, collects all the traffic sent between a pair of ASes.

Again, a key question is whether targeting Facebook or Boston University is "intentionally targeting a US person," since organizations[196] can be "US persons" under FISA and EO 12333.[197] The logic from the MUSCULAR operations may apply in this case as well: authorities are not "targeting" Facebook or Boston University in the legal sense, but are instead "targeting" individual users of their Internet services that are not yet known.[198] If the same logic applies as in MUSCULAR, the DNS manipulation is not "intentionally targeting a US person" and is therefore regulated by the permissive legal regime of EO 12333.[199]

LOCATION OF THE DNS MANIPULATION. Like the BGP manipulations discussed earlier, these DNS manipulations can be conducted entirely abroad. Researchers Amir Hertzberg and Haya Shulman describe a technique that allows this manipulation to be executed by a device located en-

194. This is a hypothetical example of a well-known attack on DNS. For more specific examples, *see, e.g.*, Cowie, *supra* note 167; Bellovin, *supra* note 192; Kaminsky, *supra* note 192; Herzberg & Shulman, *supra* note 192.

195. *See* LIU & ALBITZ, *supra* note 188.

196. Any organization can have an AS: it does not have to be a corporation. For example, a non-profit organization or university can have an AS. Even the George W. Bush Foundation appears to have its own AS: http://www.tcpiputils.com/browse/as/393327.

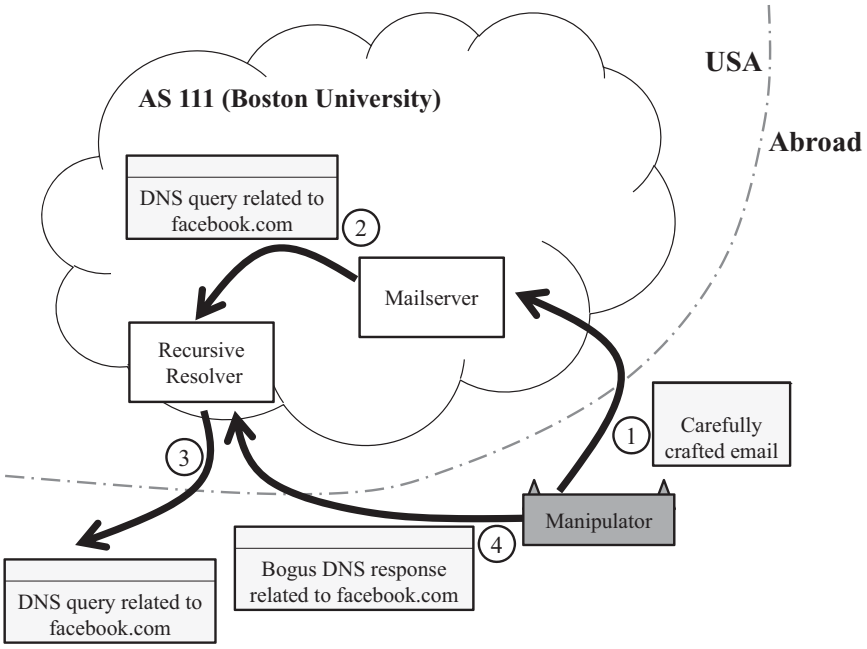
197. *See supra* Part I.

198. *See supra* Part II.A.

199. We reiterate that we cannot establish with full certainty how the intelligence community applies FISA and EO 12333 in specific cases. This point could be clarified as part of any investigation into EO 12333, such as the one announced by the PCLOB.

tirely outside the targeted source AS.[200] The technique is depicted in Figure 4, below.

FIGURE 4. HERTZBERG AND SHULMAN'S TECHNIQUE FOR SUBVERTING THE DNS MAPPING FOR A DOMAIN.



Hertzberg and Shulman's technique subverts the DNS mapping for a particular domain (*www.facebook.com*) by using a recursive resolver that serves a particular target AS (Boston University AS 111).[201] The manipulator can be located entirely outside the target AS, and need only send DNS messages and emails.[202] No devices within the target AS need to be compromised.[203]

It is important to observe that recursive resolvers usually do not accept messages from senders outside their AS,[204] but mailservers do accept such messages.[205] Thus, a manipulator located outside the target AS can use the mailserver to attack the recursive resolver. Specifically, the manipulator

200. *See* Herzberg & Shulman, *supra* note 192.
201. *Id.*
202. *Id.*
203. *Id.*
204. *See* LIU & ALBITZ, *supra* note 188 at 3; OPEN RESOLVER PROJECT, http://openresolverproject.org/ (last visited May 3, 2015).
205. Mailservers are devices that provide email services for an AS. Therefore, they need to accept emails from outside the AS. Since emails can come from any AS on the Internet, the mailservers will accept messages (i.e., emails) from outside their own network. *See* David

sends carefully crafted messages to a mailserver located inside the target AS.[206] These messages act as a trigger for the mailserver to send DNS queries to the DNS resolver inside the AS; the DNS resolver accepts messages from the mailserver, because the mailserver is inside the AS.[207] The recursive resolver then proceeds to resolve the mailserver's DNS queries. To do this, the recursive resolver sends DNS messages to DNS servers outside the target AS.[208] Finally, the manipulator responds to these DNS messages with carefully-crafted bogus DNS messages of its own; this allows the manipulator to subvert the recursive resolver's mapping from a domain name to an IP address.[209] This manipulation only involves sending messages from outside the AS: no internal devices in the AS need to be compromised. And this manipulation can also be executed entirely abroad.

3. Other Manipulations

The BGP and DNS manipulations we describe fall outside of the "intentional acquisition" and the "installation of a . . . device" subsection of the "electronic surveillance" definition under FISA.[210] Therefore, such manipulations are likely regulated by the permissive legal regime of EO 12333. However, protocol manipulations probably do not have to be executed entirely abroad to be regulated under EO 12333.[211]

Although the BGP and DNS manipulations we described here can be executed entirely abroad, and thus regulated by EO 12333, manipulations might be executed on US soil and still regulated by EO 12333. This class of manipulations includes any network exploit executed by an attacker that wishes to become a man-in-the-middle on a communication path.

Any domestic exploit may fall into this category, but one particularly interesting class of manipulations involves hacking into US routers or switches and installing routes that divert traffic abroad. Recent revelations suggest that the NSA has the capability to take control of remote routers.[212]

Crocker, *RFC5598: Internet Mail Architecture*, THE INTERNET ENGINEERING TASK FORCE (July 2009), http://tools.ietf.org/html/rfc5598.

206. Herzberg & Shulman, *supra* note 192.

207. *Id.*

208. *Id.*

209. *Id.*

210. 50 U.S.C. § 1801(f) (2012).

211. To be completely confident that they can also be conducted on US soil under EO 12333, one needs to have complete insight into USSID 18. On the face of it, however, EO 12333 and USSID 18 do not define "targeting" and FISA does not include manipulations within its scope. *See* Exec. Order No. 12,333, 3 C.F.R. (1981); USSID 18, *supra* note 5.

212. The HEADWATER, SCHOOLMONTANA, SIERRAMONTANA, and STUCCOMONTANA programs are examples of this capability at work. *See* Jacob Appelbaum, Judith Horchert & Christian Stöcker, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, DER SPIEGEL, Dec. 29, 2013, http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html; *see also* Darlene Storm, *17 exploits the NSA uses to hack PCs, routers and servers for surveillance*, COMPUTER WORLD (Jan. 3,

The NSA can also physically tamper with US-made routers.[213] Another possibly relevant class of manipulations is the SECONDDATE program, which the NSA calls "an exploitation technique that takes advantage of web-based protocols and man-in-the-middle capabilities."[214] Although we are unable to fully determine the extent to which such capabilities are actually used, based on the recently increased transparency and our subsequent analysis, we do see sufficient basis to conclude that the legal and technical possibilities exist.[215]

III. Possible Remedies

FOIA requests. In order to address the loopholes identified in this Article, the vast amount of still redacted policy documents—in particular in USSID 18—must be addressed. Even though the US government has released several insightful policy documents in recent months,[216] often these documents refer to redacted or completely classified legal documentation that cannot be studied. The lack of transparency on surveillance policies limit policymakers, academics, the general public and even the US Supreme Court[217] from establishing a comprehensive overview of the Fourth Amendment implications of current network surveillance policy.

Technical solutions. Purely technical solutions like encryption, DNS Security Extensions (DNSSEC), and the Resource Public Key Infrastructure (RPKI) can also help combat some of the specific risks of the loopholes we identified. Indeed, the past year has seen a significant increase in efforts to encrypt Internet traffic. In response to revelations about the MUSCULAR program, described in Part II.A.1, Google and Yahoo! have moved to encrypt the intradomain communication links between their data centers, and a

---

2014), http://www.computerworld.com/article/2474275/cybercrime-hacking/17-exploits-the-nsa-uses-to-hack-pcs—routers-and-servers-for-surveillance.html.

213. Glenn Greenwald, *Glenn Greenwald: how the NSA tampers with US-made internet routers*, The Guardian (May 12, 2014), http://www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden.

214. Ryan Gallagher & Glenn Greenwald, *How The NSA Plans To Infect Millions Of Computers With Malware*, The Intercept (Mar. 12, 2014), https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/.

215. Once again, we are not in a position to establish whether the NSA's ability to subvert network protocols and routers is actually used in practice to circumvent the statutory and constitutional protections provided to US persons under the first two legal regimes described. National security secrecy—not so much on the operational level but at the policy level—still limits exhaustive independent analysis and evaluation.

216. *See* USSID 18, *supra* note 5. Note that dozens of EO 12333-related documents released in the FOIA case *ACLU v. NSA* so far do not cover our analysis. Am. Civil Liberties Union v. Nat'l Sec. Agency, No. 13-9198(AT) (S.D.N.Y. 2013).

217. *See, e.g.*, Clapper v. Amnesty, 133 S.Ct. 1138 (2013) (dismissing the case due to lack of standing).

number of other corporations have followed suit.[218] There has also been increased interest in encrypting interdomain traffic between users and websites, through the deployment of the HTTPS protocol for encrypted web traffic.[219] The Internet Architecture Board issued a statement on Internet confidentiality, indicating that "protocol designers, developers, and operators [should] make encryption the norm for Internet traffic."[220] And there are new efforts underway to enable turn-key encryption of websites through the LetsEncrypt project.[221]

However, although encryption can certainly thwart attempts to read the content of collected communications, adoption is still in its infancy. Moreover, even encrypted traffic exposes "metadata" (e.g., who is communicating, the length of the communication, timing information, etc.) that can be used to reconstruct surprisingly detailed information about the contents of the network traffic.[222] In addition, FISA and USSID 18 minimization procedures permit extensive retention and further analysis of encrypted communications even if two communicants are known to be US persons.[223]

The RPKI can limit the scope and impact of BGP manipulations, but cannot completely eliminate them, and it remains far from fully deployed today.[224] DNSSEC can stop the DNS manipulations we described, but it also

218. *See EFF's Encrypt the Web Report*, ELEC. FRONTIER FOUND. (Nov. 4, 2014), https://www.eff.org/encrypt-the-web-report (The Electronic Frontier Foundation maintains an updated scorecard in which leading Internet companies are rated for their adoption of encryption policies, including "Encrypts data center links," "Supports httpS," "httpS Strict (HSTS)," "Forward Secrecy," and "STARTTLS.").

219. *See* Herzberg & Schulman, *supra* note 192.

220. *IAB Statement on Internet Confidentiality*, INTERNET ARCHITECTURE BD., (Nov. 14, 2014), https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality.

221. *See*, *e.g.*, Alex Halderman, *Let's Encrypt: Bringing httpS to Every Web Site*, FREEDOM TO TINKER (Nov. 18, 2014), https://freedom-to-tinker.com/blog/jhalderm/announcing-lets-encrypt.

222. For an extensive body of technical literature on the subject of using "metadata" to reconstruct information about the contents of encrypted network traffic, *see* Brad Miller et. al., *I Know Why You Went To The Clinic: Risks And Realization Of httpS Traffic Analysis*, 8555 LECTURE NOTES IN COMPUTER SCI. 143, 146-64 (2014). The gist of this technical literature is that even encryption cannot hide the fact that a user visited the server hosting a particular site. For example, one might learn the "metadata" that an Internet user visited the server hosting the site www.hivmedicineinfo.com; this "metadata" immediately leaks information about diseases that the user might be likely to have, even if the actual pages the user viewed on website are encrypted.

223. *See* USSID 18, *supra* note 5; *see also* EXHIBIT A, *supra* note 36; EXHIBIT B, *supra* note 36.

224. Danny Cooper et. al., *On The Risk Of Misbehaving RPKI Authorities*, Proc. 12th ACM Workshop on Hot Topics in Networks, 16(1), 2013; M. Lepinski & S. Kent, *RFC 6480: An Infrastructure to Support Secure Internet Routing*, INTERNET ENGINEERING TASK FORCE (Feb. 2012), http://tools.ietf.org/html/rfc6480.

has not reached anything near full deployment.[225] Moreover, new and existing technical loopholes will likely continue to be discovered by security researchers and the intelligence community; thus, reliance on purely technical solutions alone is not sufficient protection against the legal loopholes we have identified here.

EXISTING LEGISLATIVE INITIATIVES. The legislative initiatives that dominate the headlines in the media (including the proposed USA Freedom Act that ultimately failed to pass by a handful of votes)[226] still concentrate on the rights of US persons under the Patriot Act and FISA. Thus, they offer little promise in protecting Americans from the international surveillance loopholes for bulk surveillance on Americans under EO 12333. Presidential Policy Directive 28,[227] issued in January 2014, contains some language concerning the protection of foreigners' rights, along with a set of purposes for which foreign intelligence may be collected. However, the legal status of the Directive relative to the existing framework of US surveillance is unclear, and the Directive explicitly states that "this directive is not intended to alter the rules applicable to US persons in Executive Order 12333, the Foreign Intelligence Surveillance Act, or other applicable law."[228] So far, no substantial changes can be observed since the Directive was released, and the extent to which the Directive will influence actual surveillance policy remains to be seen. In contrast, although its implications remain opaque, § 309 of the 2014–15 Intelligence Authorization Bill—hastily introduced, hardly debated and approved within 48 hours before a budgetary deadline for the new fiscal year passed—seems to lower legal protections for US persons.[229]

More fundamentally, the ability to overcome these loopholes is further constrained by US lawmaking and constitutional traditions. Whereas the Patriot Act and FISA are overseen by all three branches of government, EO 12333 remains solely under the authority of the executive branch (in theory and most certainly in practice). However, as Article II of the US Constitution grants the executive branch wide national security authorities, it is likely that EO 12333 reform will remain an executive affair.

The obstacles impeding long term reform are real. Cross-institutional checks and balances and independent oversight could remain absent from EO 12333 policies in the years to come. The PCLOB investigation, an-

225. Wilson Lian et. al., *Measuring the Practical Impact of DNSSEC Deployment*, USENIX Security Symposium (2013), *available at* https://www.usenix.org/conference/usenixsecurity13/technical-sessions/paper/lian.

226. *See supra* text accompanying note 27.

227. *Presidential Policy Directive: Signals Intelligence Activities*, THE WHITE HOUSE (Jan. 14, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

228. *Id.* at 9.

229. *See supra* Part I.C.5.

nounced on July 23, 2014, is a first step in investigating issues with EO 12333; however, the Board reports directly to the President. So far, the PCLOB has done little besides issue general statements on the modification of policies that have been in place since the Reagan era.[230] It is too early to tell exactly what the PCLOB investigation will focus on, let alone what recommendations will eventually be acted upon by the President. In any event, the legislative and judicial branches of government have limited theoretical and practical ability to change the trajectory of EO 12333 reform unless a court is willing to find the scope of the EO unconstitutional. It is still too early to determine whether § 309 of the 2014–15 Intelligence Authorization Act will set a historical legal precedent for more Congressional involvement or how it will interplay with FISA. But even if the legislative and judicial branches of government address the loopholes in the Patriot Act and FISA, the consolidation of the loopholes in EO 12333 continues to expose Americans to unrestrained bulk surveillance from abroad.

SHORT-TERM REMEDY: REVISE FISA. An actionable short-term remedy would update the definition of "electronic surveillance" in FISA.[231] First, a good modification would ensure that the geographical point of collection does not determine the legal protection offered. Second, the definition of "electronic surveillance" should be formulated in a technology-neutral fashion, to ensure legal protection continues to apply regardless of the technology employed in the surveillance operation. If the legal definition continues to mention explicitly specific technologies, it will quickly be outpaced by new technologies and new surveillance capabilities. Finally, the legal definition of "installing a device" for the purpose of surveillance should be carefully reformulated to avoid introducing new loopholes, such as the ones discussed in Part II.B. Failing to take these issues into account when revising FISA would continue to leave Americans unprotected against advanced forms of network traffic collection from abroad. Historically, Congress has left the critical definition of "electronic surveillance" in FISA untouched for decades, but perhaps increased public scrutiny could instigate change.

LONG-TERM REMEDY: REVISIT CENTRAL CONCEPTS OF US SURVEILLANCE LAW. Over the long term, effectively closing the identified loopholes requires a fundamental reconsideration of central concepts of US surveillance law. Questions that need to be raised include whether the point of collection should continue to determine the applicable legal regime; whether network traffic collection itself (before a user is "intentionally targeted") should constitute a privacy harm; and whether the principle that limits Fourth Amendment protection to US persons, established in *United States v.*

230. A full report on EO1233 will come out later. *See PCLOB Posts Status of Attorney General-Approved U.S. Person Procedures Under Executive Order 12333*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD. (Feb. 19, 2015), https://www.pclob.gov/newsroom/20150219.html.

231. *See supra* Parts I.B.2 & I.C.2.

Verdugo-Urquidez and confirmed in *Clapper v. Amnesty*, effectively protects Americans on a global Internet.[232] As long as these questions remain unaddressed, the interdependent legal and technical loopholes we identify leave the door open for the intelligence community to circumvent the Constitution and to conduct largely unrestrained bulk collection of Americans' Internet traffic from abroad.

Conclusion

International communications intercepted on US soil are regulated by FISA and overseen by Congress and the FISA Court. Revealed surveillance operations regulated by FISA are the subject of a broad public debate and are being constitutionally challenged at courts across the United States. By contrast, however, surveillance of Americans' traffic, when collected abroad, is regulated by EO 12333, solely governed and primarily overseen by the executive branch. An operation can be regulated under EO 12333 if it is designed to adhere to two main criteria: 1) it does not "intentionally target a US person" (e.g., bulk surveillance) and 2) it is conducted abroad. EO 12333 and its underlying guidelines (notably, USSID 18) contain permissive presumptions of foreignness, and as long as users are not intentionally targeted, operations on foreign soil are presumed to affect foreigners exclusively.[233] Since foreigners do not enjoy the legal protections provided by the Fourth Amendment, conducting operations abroad under EO 12333 enables the intelligence community to circumvent constitutional and statutory safeguards in the Patriot Act and FISA, even when Americans' data are intercepted.

Technological developments make these legal loopholes exploitable by intelligence communities. The vagaries of Internet protocols can sometimes cause traffic sent between two US endpoints to be routed abroad. Even when this is not the case, core Internet protocols like BGP and DNS can be deliberately manipulated to ensure that traffic between US endpoints takes an unusual path through a device, under NSA control, located abroad. Recent months have seen a number of revelations on the technical capabilities of the US intelligence community, including tapping fiber optic cables and remotely controlling routers, which could potentially be used to exploit these legal loopholes.

---

232. Justices Brennan and Marshall reject the principle in their Dissenting Opinion to the ruling. As soon as anyone in the world is affected by conduct of the US government, the Justices argue, they become "one of the governed" as mentioned by the US Constitution. They conclude: "when we tell the world that we expect all people, wherever they may be, to abide by our laws, we cannot in the same breath tell the world that our law enforcement officers need not do the same [. . .]. We cannot expect others to respect our laws until we respect our Constitution." United States v. Verdugo-Urquidez, 494 U.S. 284, 297 (1990).

233. *See supra* Part I.C.

If the two main legal criteria for EO 12333 applicability are met, the interdependent legal and technical loopholes enable largely unrestrained surveillance on Americans' Internet communications. For instance, if the aforementioned legal conditions are met, these techniques could be used to collect, in bulk, all communications sent from an autonomous system, like Boston University, to a given IP address block (with a BGP manipulation), or from an autonomous system to a particular domain, like *www.facebook.com* (with a DNS manipulation). Indeed, the MUSCULAR operation demonstrated that collecting network traffic from a US Internet company (like Google or Yahoo!), in bulk, is not considered by the intelligence community to "intentionally target a US person" per the FISA definition. Instead, individual users of these Internet companies' services were considered (in the legal sense) the targets of the operations. Because these users were not specifically targeted at the time the network traffic was collected in bulk, MUSCULAR was regulated under the most permissive legal regime for surveillance in the US legal framework (EO 12333 and its underlying directives, notably USSID 18).[234] From these revelations, we infer that the EO 12333 regime also likely regulates the deliberate network protocol manipulations (of BGP or DNS) described in Part II.B.

We reiterate that we do not intend to speculate on the extent to which the intelligence community is exploiting the described loopholes. Instead, our aim is to broaden the public's understanding of the possibilities and deeper issues at hand. Moreover, this analysis of EO 12333's loopholes is not exhaustive: this Article focused on bulk surveillance on Americans by collecting their network traffic abroad. Other types of surveillance operations not discussed in this Article are also authorized under EO 12333, including the deployment of malware.[235]

This analysis highlights a central problem: the law maintains an old-fashioned focus on physical materiality. The geographic location of interception determines the surveillance laws that apply and the legal protections afforded to Americans. But global communications networks are not organized along the lines of traditional geopolitical boundaries to which current constitutional and statutory protections are tailored. Much of what we have observed concerns, fundamentally, conventional laws challenged by new technical realities. Ultimately, conventional laws will likely continue to be challenged by these new technical realities. If Americans want to bring constitutional protections into the modern age, the US must adapt its legal approaches to deal with these realities.

234. USSID 18, *supra* note 5.
235. Exec. Order No. 12,333, 3 C.F.R. (1981); *NSA Documents*, *supra* note 63.