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

Axel Arnbak and Sharon Goldberg*

TABLE OF CONTENTS

* 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 Assistant 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 pointers 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 updated 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.

I. Introduction

While the general public and the media become overloaded by the string of revelations on surveillance operations conducted by the U.S. intelligence community, we are only beginning the process of precisely describing their legal and technical details. This multi-disciplinary article discusses interdependent legal and technical loopholes that intelligence agencies of the U.S. government could use to circumvent Fourth Amendment protections and statutory safeguards for Americans.

Our central hypothesis is that there are several loopholes in current U.S. surveillance law that allow for largely unrestrained surveillance on Americans by collecting their network traffic abroad while not intentionally targeting a U.S. person. Because the U.S. legal framework regulating intelligence operations has not been updated in accordance with new technical realities, the loopholes we identify may leave the internet traffic of Americans as exposed to network surveillance, and as unprotected by under current U.S. law, as the internet traffic of foreigners.

We aim to broaden our understanding of how U.S. surveillance law is impacted by the technical realities of the current Internet, and reflect remedies that can close the loopholes we identify. We focus on surveillance operations conducted by agencies of the U.S. government. However, we will not speculate on the extent to which the intelligence community is exploiting the loopholes we identify in legal framework. We also will not take a position in the debate on the morality of surveillance based on the (assumed) nationality of internet users.

Our 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 physical borders, or the 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 the new technical reality. Transnational surveillance (i.e., 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 general regulatory conundrum.[1]

While 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 core legal principles underlying U.S. surveillance law. First, the geographical point of collection determines the legal regime applies to a surveillance operation. Second, the collection of network traffic, before its subsequent processing and further analysis, is not firmly protected by the Fourth Amendment of the U.S. Constitution. Third, constitutional protection is limited to "U.S. persons", a term which is not defined uniformly across different regimes of U.S. surveillance laws. These three principles of U.S. surveillance law emerged in different times than ours. If these three principles are maintained, loopholes in antiquated law — particularly Executive Order 12333 — will continue to interact with advanced technical capabilities to enable largely unrestrained surveillance on Americans from abroad.

A. Overview

This article focuses on network traffic surveillance conducted from abroad in the data collection phase, although at times we point at policies for data retention and subsequent analysis as well. Section II describes the three legal regimes that form the core regulatory framework for network traffic collection for intelligence agencies. Section III discusses the technical details of how network protocols can be exploited to conduct surveillance from abroad,

[1] Discussed extensively in Joris van Hoboken, Axel Arnbak and Nico van Eijk, *Obscured By Clouds, or How To Address Governmental Access to Cloud Data From Abroad*, PLSC 2013, June 7, 2013, U.C. Berkeley.

thus circumventing the legal protections in place for Americans when operations are conducted on U.S. soil. In Section IV we briefly reflect on legal and technical remedies.

Legal framework. In Section II we start by describing the current U.S. regulatory framework for intelligence gathering. From public and until-recently secret primary legal sources, we describe the three most relevant regimes:

1. Surveillance of domestic communications records conducted on U.S. soil under s.215 of the "Patriot Act";[2]
2. Surveillance of international communications conducted on U.S. 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 "U.S. Signals Intelligence Directive SP0018" (USSID 18).[5]

Distinguishing factors include where the surveillance is conducted, and who a surveillance operation targets. The first two

[2] USA PATRIOT Improvement and Reauthorization Act of 2005 § 215, 120 Stat. at 196 (codified as amended at 50 U.S.C. § 1861 (2006)). The PATRIOT Sunsets Extension Act of 2011 (H.R. 514) Pub. L. 112-14 (May 26, 2011).

[3] The Foreign Intelligence Surveillance Act of 1978 ("FISA"), 50 U.S.C. ch. 36, 92 Stat. at 1783, Pub.L. 95–511. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (codified as amended at 50 U.S.C. § 1881(a) (2006 & Supp. V 2007-2012)).

[4] Exec. Order 12,333, 46 Fed. Reg. 59941, 3 C.F.R. 200 (1982). Exec. Order 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003); Exec. Order 13,355, 69 Fed. Reg. 53,593 (Aug. 27, 2004); Exec. Order 13, 470, 73 Fed. Reg. 45,325 (July 30, 2008). The discussion will also briefly point at section 309 of the Intelligence Authorization Act for Fiscal Year 2015, H.R.4681, 113th Congress. The Bill was rushed through U.S. Congress within 48 hours, just before the Winter break, with little discussion of sec. 309. The Bill still needed to be signed by the U.S. President when this article submitted on December 25, 2014.

[5] United States Signals Intelligence Directive SP0018 ("USSID 18"), *Legal Compliance And U.S. Persons Minimization*, January 25, 2011, *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

regimes are overseen by all three branches of the U.S. government, and have been discussed at length by the government, media and the 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 or academic arenas. Meanwhile, the N.S.A. states that this third regime, EO 12333, is the "primary legal authority" for its operations.[6]

Executive Order 12333, adopted in 1981 by the Reagan Administration and not substantially updated since, constitutes the cornerstone of our legal analysis. 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 main findings. Coverage on *CBS News*[7] spurred an inadequate official response from the N.S.A. compliance department; we discuss this response further in Section II.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:[8]

> *"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*

[6] National Security Agency, *Memorandum: The National Security Agency: Missions, Authorities, Oversight and Partnerships*, August 9, 2013, at 2-3, *available at* https://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf.

[7] Zack Whittaker, *Legal Loopholes Could Allow Wider NSA Surveillance, Researchers Say*, CBS NEWS, June 30, 2014, *available at* http://www.cbsnews.com/news/legal-_loopholes-_could-_let-_nsa-_surveillance-_circumvent-_fourth-_amendment-_researchers-_say/.

[8] Joseph Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets The NSA Spy On Americans*, THE WASHINGTON POST, July 18, 2014, *available at* 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.

> *the possibility that Section 215 collection does not represent the outer limits of collection on U.S. persons but rather is a mechanism to backfill that portion of U.S. person data that cannot be collected overseas under 12333."*

On 23 July 2014, the Privacy and Civil Liberties Oversight Board ("PCLOB") of the executive branch of government confirmed that it will investigate surveillance policy and operations based on EO 12333.[9] Given the complexity of U.S. surveillance law and especially EO 12333, the investigation is expected to take months. This adds to the necessity of inter-disciplinary research on EO 12333 policy and operations.

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 U.S. 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. As the U.S. Supreme Court has consistently held that foreigners do not enjoy constitutional protection under U.S. law,[10] the legal incentives to conduct surveillance under EO 12333 are substantial.

We emphasize that notion of 'targeting a U.S. person' (in the legal sense) does not rule out bulk collection of Internet traffic, even in situations where the traffic actually contains millions of American's communication records; by collecting the traffic abroad, authorities can presume the traffic belongs to foreigners. Any U.S.

[9] Privacy and Civil Liberties Oversight Board, *Public Meeting 202-220-4158*, July 23, 2014, *transcript available at* http://www.pclob.gov/SiteAssets/meetings-_and-_events/2014meetingsevents/23-_july-_2014-_public-_meeting/Public-_Meeting-_Transcript_July_23_2014.pdf.

[10] *See, e.g.*, *United States v. Verdugo-Urquidez*, 494 U.S. 259, February 28, 1990. *Clapper v. Amnesty International USA a.o.*, 568 U.S. ___, February 26, 2013.

person's traffic that happens to be captured during bulk collection is considered to be 'incidentally collected', and may be stored and retained for further processing. Users are actually 'targeted' in the legal sense once collection is complete, and the surveillance operation moves into the phase of retention and analysis. Indeed, revelations from 25 August 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".[11]

Thus, a main finding of our legal analysis is that there is a legal loophole for surveillance on Americans by collecting their network traffic abroad. Constructing a surveillance operation in a manner that EO 12333 applies allows foreignness to be presumed for data that is intercepted abroad. This circumvents Fourth Amendment protections for Americans that are assumed (in the legal sense) to be U.S. persons under FISA and s.215 of "The Patriot Act" during domestic surveillance operations.

Technical realities. At first blush, one might suppose that a surveillance operation conducted abroad should have no impact on Americans. However, in Section III we discuss why the technical realities of the Internet mean that American's network traffic can easily be routed or stored abroad, where it can then be collected under the permissive legal regime of EO 12333. Indeed, we already know of surveillance programs that have exploited this legal loophole. The revealed MUSCULAR/TURMOIL program, for example, illustrates how the N.S.A. presumed authority under EO 12333 to acquire traffic between Google and Yahoo! servers located

[11] Ryan Gallagher, *Sharing Communications Metadata Across the U.S. Intelligence Community,* at slide 6, THE INTERCEPT, August 25, 2014, *available at* https://firstlook.org/theintercept/document/2014/08/25/sharing-communications-metadata-across-u-s-intelligence-community. Ryan Gallagher, *The Surveillance Engine: How the NSA Built its Own Secret Google,* THE INTERCEPT, August 25, 2014, *available at* https://firstlook.org/theintercept/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/.

on foreign territory; this program allegedly collected up to 180 million user records per month abroad, including those of Americans.[12]

We also discuss other technical means an intelligence agency can exploit the legal loopholes under EO 12333. 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. We explain why interdomain routing with BGP can naturally cause traffic originating in a U.S. network to be routed abroad, even when it is destined for an endpoint located on U.S. soil. We also discuss why core Internet protocols – BGP and DNS – can be deliberately manipulated to force traffic originating in American networks to be routed abroad. We discuss why these deliberate manipulations can fall within the permissive EO 12333 regime, and how they can be 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 U.S. soil (e.g., from Harvard University to Boston University).

Remedies. In Section IV we conclude by discussing possible legal and technical remedies. We explain why Patriot Act and FISA reform will not close the international surveillance loopholes we identify. The focus on the Patriot Act and FISA may be attributed to the legal fact that the Legislative and Judiciary branches of the U.S. Government have little authority over EO 12333 reform, since EO 12333 falls solely under by the Executive branch. Thus, surveillance operations conducted abroad under EO

[12] Barton Gellman and Ashkan Soltani, *N.S.A. Infiltrates Links To Yahoo, Google Data Centers Worldwide, Snowden Documents Say*. THE WASHINGTON POST, October 30, 2013, *available at* 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.

12333, have thus far been overlooked by reform efforts, despite the fact that they can impact the privacy of millions of Americans.

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 new analytical framework to conduct similar research. Our method should be particularly helpful for conducting research into the interdependency of the laws and technologies for network surveillance, as well as surveillance law evaluation in policymaking.

II. Loopholes in the Legal Framework

In the following section, we use recently revealed and declassified primary legal sources to describe and contextualize the U.S. legal framework for network surveillance by intelligence agencies. Our discussion will also highlight the differences in legal protection under the different legal regimes for network traffic collection, and reflect on the outlook on reform under the three legal regimes outlined in Section I.

Before we dive into specific legal regimes, it is critical to briefly discuss one general constitutional principle: non-U.S. persons do not enjoy the protections of the Fourth Amendment of the U.S. Constitution. The U.S. Supreme Court established this principle in *United States v. Verdugo-Urquidez*, and recently confirmed it in *Clapper v. Amnesty International USA a.o.*[13] The legal and technical loopholes we identify can, fundamentally, be traced back to this principle because it profoundly impacts the statutory regimes for network surveillance.

In the U.S. statutory framework, two main criteria determine which of the three legal regimes regulate network traffic collection: *where the communication is taking place* (inside or outside the

[13] *See supra* note 10. *See supra* note 1 at 8.

U.S.), and *who is targeted*. We focus our analysis on the poorly-understood third regime, EO 12333, which primarily regulates intelligence community operations on foreign territory.[14]

Since the third regime covers operations that are not covered by the first two legal regimes (the "Patriot Act" and FISA),[15] we start by analyzing the types of operations that fall under those two legal regimes. We then move on to discussing the EO 12333 and its underlying policies in detail, and find that the Order applies when surveillance does not 'intentionally target a U.S. person' and is conducted abroad, regardless of whether or not the operation actually affects the communications records of Americans.

Our legal analysis is consistent a recently released N.S.A. slide titled 'Sigint Authority decision tree', revealed by the Washington Post on 23 July 2014 (after this article was first posted online) and shown in Fig. 1:[16]

[14] We focus on operations conducted abroad. But as we note in Section II.C.2, EO 12333 also seems to have been interpreted to enable *domestic* operations not covered by the other two legal regimes.

[15] See infra, Section II.B.2 and Section II.C.2.

[16] *See* Barton Gellman and Matt DeLong, *One month, Hundreds of Millions of Records Collected*, THE WASHINGTON POST, October 30, 2013, *available at* http://apps.washingtonpost.com/g/page/world/one-_month-_hundreds-_of-_millions-_of-_records-_collected/554/#document/p1/a129979. 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 U.S., U.K., 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 supra* note 1, at 17-18 and more generally Joris van Hoboken, Axel Arnbak, Nico van Eijk, *Cloud Computing In Higher Education And Research Institutions And The USA Patriot Act*. SURFnet Report, November 27, 2012.

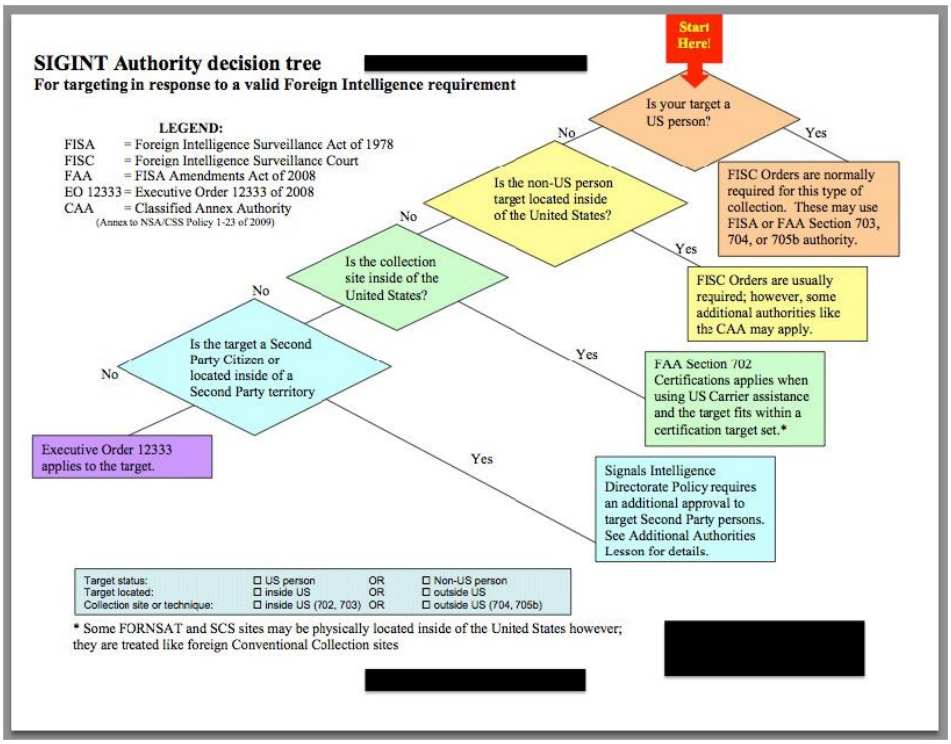

Fig. 1: Internal flowchart showing the N.S.A.'s interpretation of the different legal regimes that regulate surveillance operations.

Indeed, the location of the collection site and the nationality of the target are important elements that determine the applicable legal regime. Two less explicit elements, however, are essential to understand the flowchart.

Targeting. First, surveillance operations that collect network traffic in bulk do not necessarily "intentionally target a U.S. person" in the legal sense. Put differently, 'targeting' a person (as noted in the decision tree depicted in Fig. 1) often occurs after the collection phase i.e., when network traffic has already been intercepted. Upon collection, surveillance operations move into the phase of retention and analysis; phases in which users are actually 'targeted' in the legal sense. Most of our discussion will center around the collection phase. The collection phase is crucially

important, since large volumes of American's communications records can be captured during collection, and subsequently be stored, searched or shared with other government agencies, as revelations of August 2014 suggest.[17]

Presumed foreignness. Second, in surveillance law, conducting network-traffic-collection operations from abroad creates the presumption traffic belongs to foreigners; this presumption holds even though the traffic may, in fact, largely belong to Americans. This leaves Americans less protected under U.S. law, even when operations conducted abroad largely affect their Internet traffic in practice.

We discuss these two observations throughout the rest of this article.

A. First Regulatory Regime: 'Patriot Act Section 215'. Domestic Communications, Surveillance on U.S. Soil.

Some intelligence surveillance operations target domestic communications on U.S. soil. The legal framework of this class of operations is relatively well-known. Under s. 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. The current form of s. 215 was adopted shortly after the 9/11 attacks, broadening the legal authority for domestic surveillance.

A program operating under this legal authority is the production of Americans' telephone records—the so-called 'Verizon Metadata Program'. Immediately after 9/11, U.S. President Bush arranged for the voluntary provisions of communication records by major U.S. telecommunications providers. Upon a 2005 disclosure in the press of the program, one company asked the government to

[17] *See supra* note 11. The revelations of 25 August 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.

obtain a warrant from the FISA Court. Since 2006, the Court has granted the warrants on a rolling basis, including so-called 'gag' orders that prevent the companies from disclosing the requests to customers or the wider public.

With the details of the telephony metadata programs revealed after nearly twelve years, scholars have argued that the program violates both the provisions of the Patriot Act and the Constitution.[18] Proposals to reform this legal regime have also been initiated in the U.S. Congress. Thus far, these proposals have failed.[19] In June 2015, section 215 is expires due to a sunset clause, setting the scene for a new round of legislative debates in U.S. Congress in the near future. Furthermore, court cases are pending in several judiciary circuits with vastly varying outcomes,[20] suggesting that the U.S. Supreme Court will eventually rule on the issue. It is too early to report on the final outcome of these legal and political debates. Regardless of its outcome, all three branches of government (i.e., the Executive, the Legislative and the Judiciary) are involved in establishing the necessary checks and balances and legal protections for Americans under this first regulatory regime. As we will see, both legal protections and reform prospects diminish once we move to the next legal regimes that regulate surveillance operations with international or foreign aspects.

[18] *See* L. K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J. L. & PUB POL'Y, No.3, pp. 757-900 (2014). R. Levinson-Waldman, *What The Government Does With Americans' Data*, Brennan Center for Justice, N.Y.Y. School of Law, October 8, 2013.

[19] 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 U.S. Senate: J. Sensenbrenner, *The USA Freedom Act*, H.R. 3361, s. 1599, October 29, 2013, *available at* http://sensenbrenner.house.gov/uploadedfiles/usafreedomact.pdf. P. Leahy. *The USA Freedom Act*, HEN 14602, August 7, 2014, *available at* https://www.leahy.senate.gov/download/hen14602.

[20] *ACLU v. Clapper*, Civ. No. 13-3994 (S.D.N.Y., 2013). *Klayman v. Obama*, Civ. No. 13-0851 (D. Del. 2013).

B. Second Regulatory Regime: 'FISA'. International Communications, Surveillance On U.S. Soil.

The second regulatory regime covers a class of surveillance operations on international communications conducted on U.S. soil, regulated by the 1978 Foreign Intelligence Surveillance Act ('FISA'). In this section, we overview of this second regime and describe which surveillance operations are covered under FISA. International surveillance operations that do not fall within the FISA regime, including those enabled by the network protocol manipulations we present in Section III, are regulated by the more permissive third legal regime for surveillance under EO 12333 discussed in Section II.C. Finally, we discuss the legal protections afforded to Americans under FISA, as well as the prospect of FISA reform.

1. Overview.

FISA and the FISA Court were introduced in 1978 by U.S. Congress, in response to domestic surveillance overreach and the reform proposals by the Church Committee.[21] In 2008, FISA was amended and broadened by U.S. Congress with the FISA Amendments Act ('FAA').[22] The FAA broadened the definition of 'foreign intelligence information' to include information 'relating to the foreign affairs of the U.S.'[23] With the new definition, economic and political surveillance of foreign governments, corporations, media organizations and citizens was explicitly allowed under its provisions.[24] The FAA also introduced Section 702, enabling warrantless surveillance of foreign communications conducted on U.S. soil, as long as these operations do not 'intentionally target

[21] *See supra* note 1 and 15 for references containing detailed analysis of the legal provisions under FISA and its policy history.

[22] *See supra* note 3.

[23] 50 USC U.S.C. §1801(e)(2) (2006 & Supp. V 2011). Also *see supra* note 1 at 10-12.

[24] *Id.*

U.S. persons'.[25] Ever since, authorities do not require warrants to be issued for a specific case based on a particularized probable cause; instead, the FISA Court issues generalized certifications for surveillance operations aimed at gathering foreign intelligence information. In addition, the FISA Court approves of generalized 'targeting' and 'minimization' procedures to govern the processing of data after it has been collected. These procedures are intended to mediate U.S. person privacy concerns, and have remained classified until recently.

Media reports in December 2005 about bulk wiretapping from the Internet backbone at an AT&T switch have raised public pressure around bulk surveillance operations on Americans.[26] Nonetheless, after the AT&T program was revealed, U.S. Congress first passed the "Protect America Act" in 2007 that already contained many of the provisions adopted in the FAA one year later.[27] On 31 December 2012, the validity of the FAA was extended for another five years. Two months later, the U.S. Supreme Court denied several U.S. organizations legal 'standing' in their claim that the privacy of their international communications was violated by Section 702.[28] In what appeared to be the final ruling on the constitutionality of Section 702, a 5-4 majority argued that the civil society groups filing suit lacked standing before the Court, because they could not prove that their communications had actually been intercepted, since the details of the relevant programs remained classified.

[25] 50 U.S.C. §1881a(b)(1) (2006 & Supp. V 2007-2012).

[26] James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, NEW YORK TIMES, December 16, 2005, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0

[27] 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, No. 1, 2015 (forthcoming).

[28] *Clapper v. Amnesty International USA a.o.*, *see supra* note 10.

The political debate, and the issue of legal standing, have shifted considerably since the first leaks of June 2013. Today, it has become clear that s. 702 serves as the legal basis for surveillance operations like UPSTREAM and PRISM.[29] The N.S.A. has also confirmed that s. 702 is used compel U.S. Internet companies to assist with warrantless surveillance.[30] In addition, several of the classified targeting and minimization procedures under s. 702 have been leaked or declassified,[31] providing unique insights into classified interpretations of the legal provisions in FISA as made by the FISA Court and intelligence community,[32] as well as ongoing court cases filed in 2008 to challenge the constitutionality of the AT&T wiretapping operations under the "Terrorist Surveillance Program".[33]

Before we describe Section 702 in more detail, we mention that FISA also contains Section 703, Section 704 and Section 705b

[29] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content, see supra* note 26.

[30] *See supra* note 6 at 4.

[31] EXHIBIT A: PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES (...), AS AMENDED, July 29, 2009, published by THE GUARDIAN, June 30, 2013, *avalailable at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document. EXHIBIT B: 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, October 31, 2011, Published by THE GUARDIAN, June 30, 2013, *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document.

[32] For the most comprehensive analysis to date, see Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, *supra* note 26.

[33] *Jewel v. NSA*. The Electronic Frontier Foundation, one of the organizations involved in the court proceedings on behalf of a group of AT&T customers, maintains an updated case document repository *at* https://www.eff.org/cases/jewel (viewed August 12, 2014).

that regulate surveillance to intentionally target U.S. persons.[34] These provisions are outside the scope of this article, since our focus is on surveillance operations conducted on foreign territory that do not intentionally target U.S. persons in the collection phase, but affect Americans nonetheless. As an aside, Donohue has observed that the warrant requirements in s. 703 and s. 704 can be circumvented by applying s. 702 criteria to the collection phase, and then seeing whether collected data is of use for further processing after the fact.[35]

2. Scope: The 1978 'Electronic Surveillance' Definition

All communications surveillance operations that constitute 'electronic surveillance' as defined in FISA fall within its scope.[36] The FISA definition has remained largely intact since 1978 and, as we will demonstrate, fails to capture the technical realities of today's global communications networks.

To collect the content or metadata of 'wired communications', surveillance only falls within the FISA definition when authorities 'intentionally target a U.S. person', or when the acquisition is conducted on U.S. territory.[37] When authorities conduct targeted surveillance from abroad, even if they know that both 'sender and all intended recipients are located in the U.S.', then only 'radio' (i.e., wireless) communications fall within the FISA definition of 'electronic surveillance'.[38]

[34] Depicted in the N.S.A. 'Sigint Authority Decision Tree', *supra* fig. 1.

[35] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content, see supra* note 26, at 26.

[36] 50 USC U.S.C. §1801(f) (2006 & Supp. V 2011). Follows from 18 U.S.C. §2511(2)(f) and 50 U.S.C. §1812(a).

[37] 50 USC U.S.C. §1801(f)(1)-(2). The FISA definition only explicitly mentions communications 'content', but also covers 'metadata' (location, time, duration, identity of communicants, etc.).

[38] 50 USC U.S.C. §1801(f)(3).

Intentionally targeting U.S. persons. 'Intentionally targeting a U.S. person' constitutes 'electronic surveillance' under FISA. However, 'intention' and 'targeting' are not defined in FISA, leaving the concepts open to interpretation by authorities in classified 'targeting' and 'minimization' procedures.[39] The recent disclosure of these 'targeting' and 'minimization' procedures illuminates several loopholes. For instance, bulk surveillance is not regarded as 'intentional targeting'; we discuss this further when we look at legal protections afforded to U.S. persons under FISA in Section II.B.3.

Moreover, the 'minimization' and 'targeting' procedures reveal two important new facts related to surveillance operations conducted abroad. Firstly, conducting the surveillance abroad creates the presumption that the surveillance targets a 'non-U.S. person.'[40] Secondly, 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.[41] This implies that unless a communicant is known to be a U.S. person, the procedures consider the communicant to be a non-U.S. person. Thus, authorities have a strong incentive to conduct surveillance abroad: legal protections offered to U.S. persons under FISA can be circumvented, and a more permissive legal regime applies to data collection under EO 12333.

Installing a device. Of particular interest to our analysis is preparing a communications infrastructure for surveillance; for example using network protocol manipulations that modify the flow of network traffic, as described in Section III.

FISA has a clause on 'installing a device for that purpose in the United States', which can be understood as making a

[39] *See supra* note 30.

[40] EXHIBIT B, as amended October 31, 2011, *see supra* note 30, at page 3-4.

[41] EXHIBIT A, as amended July 29, 2009, *see supra* note 30, at page 3-4.

communications infrastructure 'ready' for surveillance. [42] However, this clause only covers 'other than wire or radio communication'; the U.S. Congressional Research Service gives 'a hidden microphone' as an example of such 'other communication'.[43]

Under the current definition, most of today's methods for preparing a networked communications infrastructure for surveillance do not constitute 'electronic surveillance' under FISA, and are as such regulated 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. Today, no installation of devices is necessary; instead, one can exploit vulnerabilities in already-present network devices (routers, web proxies, etc.) and network protocols (BGP, DNS, etc.) in order to alter the flow of network traffic, and divert it towards a specified point of collection; see for example the manipulations described in Section III.B.

It is possible that the intelligence community has secretly expanded the scope of the 'installing a device' definition of 1978 to cover newer technologies. Even if this were true, 'wired communications' fall outside this part of the FISA definition altogether. Therefore, operations for the purpose of 'installing a device' that eavesdrops on internet communications do not constitute 'electronic surveillance' under the 1978 FISA definition, except when U.S. persons are intentionally targeted. Moreover, under the current definition, it is irrelevant whether the 'installation of a device' is conducted U.S. soil or abroad; a relevant factum for our analysis in Section III.B.

Again, without full access to classified surveillance policies underlying FISA and EO 12333, it is impossible to conclusively determine how the intelligence community interprets U.S.

[42] 50 USC U.S.C. §1801(f)(4).

[43] Congressional Research Service, *Reauthorization of the FISA Amendments Act. 7-5700*, R42725, April 8, 2013, at 7.

surveillance statutes. But our textual analysis seems to be supported by recent revelations on untargeted malware operations.[44] These revelations indicate that N.S.A. analysts must 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. Based on these revelations, it seems safe to establish that advanced *active* attacks, that use new technological capabilities to prepare an infrastructure for a subsequent targeted surveillance operation, are regulated under EO 12333. Examples of such active attacks include the advanced network protocol manipulations we describe in Section III, as well as injecting malware and installing backdoors in software or hardware.

3. Legal Protections For U.S. Persons Under FISA.

Applicability of FISA to a surveillance operation is relevant for Americans, because the statute contains some important legal protections for U.S. persons that are 'intentionally targeted'. For instance, the statute states that the Fourth Amendment applies to surveillance operations under FISA and prohibits a narrow set of four surveillance operations.[45] Surveillance under section 702 may not intentionally target a U.S. person; section 703 of FISA regulates those operations instead. Another example is the 'reverse-targeting' prohibition,[46] which holds that authorities may not target a non-U.S. person under section 702 when the actual goal of the operation is to target a U.S. person. By contrast, the third legal regime under

[44] N.S.A. VALIDATOR SLIDE DECK, published by DER SPIEGEL, *NSA-Dokumente: So knackt der Geheimdienst Internetkonten*, December 20, 2013, *avalialable at* http://www.spiegel.de/fotostrecke/nsa-_dokumente-_so-_knackt-_der-_geheimdienst-_internetkonten-_fotostrecke-_105326-_13.html. We further discuss the VALIDATOR revelations in Section II.C.3.

[45] 50 USC U.S.C. §1881(b)(5).

[46] 50 USC U.S.C. §1881(b)(2).

EO 12333 explicitly allows for intentional targeting of U.S. persons, under certain conditions that we discuss in Section II.C.3.

Vast opportunities for surveillance overreach do exist within the bounds of FISA.[47] Donohue has offered a comprehensive analysis of the FISA targeting and minimization procedures, along with a critical assessment of the role of the FISA Court, arguing that these procedures allow for the creation of a 'foreign intelligence' interest in the data sometime after its collection.[48] Even so, three branches of government are involved in FISA reform, granting full legal authority across government to amend current practices when politically feasible or upon court proceedings.

4. FISA Reform: Three Branches Of Government.

FISA and FAA have serious implications for the privacy rights of Americans. In response to the recent disclosures, proposals such as the U.S.A. Freedom Act seek to reform current legal regimes, for instance by introducing a 'civil liberties advocate' that defends privacy interests to make FISA Court hearings adversarial.[49] These proposals, which thus far have failed, pay little attention to loopholes we describe here. However, in the long run, all three branches of Government will be involved in regulating

[47] EXHIBIT B, s*ee supra* note 39. One of the most-discussed loopholes is when U.S. 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 U.S. 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, more recently, Barton Gellman, Julie Tate, and 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.

[48] Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content, see supra* note 26, at Section III and page 187.

[49] *See supra* note 19.

such surveillance. The FISA and FAA statutes have been approved by the U.S. Congress, while the targeting and minimization procedures have been approved by the FISA Court. We will now see that the legal protections afforded to Americans, and the prospects for reform, are significantly lower under EO 12333.

C. Third Regulatory Regime: 'EO 12333'. Surveillance Conducted on Foreign Soil.

Electronic surveillance conducted abroad is by and large regulated by "Executive Order 12333" (EO 12333). Surveillance policies regulated under this regime are designed and adopted solely within the Executive branch. The N.S.A. recently acknowledged that EO 12333 is "the foundational authority by which N.S.A. collects, retains, analyzes, and disseminates foreign signals intelligence information".[50]

Until recently, the public has had limited ability to analyze the full extent of U.S. surveillance policies. Many relevant policies (or updated versions) were completely classified. Secrecy may 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 enable a deeper understanding of EO 12333 surveillance policies. But many relevant sentences, paragraphs, sections and even entire documents containing surveillance policy (rather than actual operations) remain classified. The issue of classified law and policy remains a critical subject for policymakers to address, for example in the PCLOB investigation announced on 23 July 2014.[51]

In this section, we will analyze what is publicly known about the EO 12333, and flag the remaining knowledge gaps relevant to

[50] *See supra* note 6.

[51] *See supra* note 9.

our analysis, focusing on USSID 18. We first discuss the scope of EO 12333, and when it applies to advanced network surveillance methods. We then describe how U.S. intelligence authorities enjoy broad and largely unchecked legal authority when conducting surveillance abroad, and how legal protection offered to Americans under EO 12333 are lower than under the other two regimes. In Section II.C.4, we also discuss the official response of the N.S.A. to an earlier version of our article, that fails to address the main issues we raise. Finally, we point at fundamental institutional issues in the U.S. Constitution that could serve as barriers to the long-term reform of EO 12333 policies. Here, we briefly point at a new legal authority created by U.S. Congress in Mid December 2014, s. 309 of the Intelligence Authorization Bill 2014-15, introduced and voted on within 48 hours. The exact implications of this provision remain opaque, seemingly even to the majority of lawmakers in U.S. Congress, and are subject to speculation by lawmakers, the media and civil society. The bill still needed to be signed into law by the President for definitive adoption when this article was concluded.[52]

Our analysis of loopholes in EO 12333 is not exhaustive; we focus on bulk surveillance on Americans by collecting network traffic abroad. Recent revelations indicate that other types of surveillance operations are also authorized under EO 12333, including the deployment of malware.[53] With regard to actual bulk surveillance operations, the public has learned how the N.S.A. assumed authority under EO 12333 to acquire communications (including those of U.S. persons) within Google and Yahoo! networks because the operation was conducted on foreign territory under the MUSCULAR program;[54] we discuss MUSCULAR in Section III.A.

[52] Section 309, Intelligence Authorization Act for Fiscal Year 2015, H.R.4681, 113th Congress (2013-2014).

[53] *See supra* note 44.

[54] *See supra* note 12.

1. Overview.

EO 12333 itself is a broad overview document, readily available to the public. A complex web of underlying legal documents exists, containing more specific rules for intelligence conduct based on EO 12333.

Two Department of Defense Directives of 1982 and 2007 fall immediately beneath EO 12333 in the legal hierarchy, and contain further general principles on 'DoD activities that may affect U.S. persons'.[55] EO 12333 and the DoD Directives form the basis of U.S. Signals Intelligence Directive 18 ("USSID 18").[56] USSID 18 was drafted by intelligence community executives in the Defense Department, and approved by the Attorney-General in the Justice Department. USSID 18 contains fairly specific surveillance principles, however, many sentences and some complete paragraphs in USSID 18 remain classified. Prior to the MUSCULAR revelations on 30 October 2013, a redacted 1993 version of USSID 18 had been released. Then, on 18 November 2013, a 2011 version of USSID 18 was released to the public. We focus our analysis on this recently declassified, but heavily redacted, 2011 version of USSID 18.

Also, §2 of USSID 18 references several legal documents that further specify intelligence activities governed by the aforementioned Department of Defense Directives, as well as a document establishing oversight procedures titled "NSA/CSS Policy No. 1-23, procedures governing NSA/CSS Activities that affect U.S. persons".[57] Interestingly, the latter document references a classified

[55] U.S. DEP'T OF DEF. DIR. 5240.01, DOD INTELLIGENCE ACTIVITIES, (Aug. 2007); U.S. DEP'T OF DEF. DIR. 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS, (Dec. 1982).

[56] *See supra* note 5.

[57] NSA/CSS POLICY No. 1-23, PROCEDURES GOVERNING NSA/CSS ACTIVITIES THAT AFFECT U.S. PERSONS, (Mar. 2004).

'Annex A' of EO 12333.[58] Some commentators have pointed toward the existence of this Annex, which sits right at the top of the legal hierarchy.[59] It appears that the same Annex is mentioned in a redacted public version of NSA/CSS Policy No. 1-23.[60] While we are not in a position to further reflect on this matter, we do note the potential existence of additional loopholes beyond the ones we identify in this Section.

2. Scope: Surveillance Abroad, Not 'Electronic Surveillance' Under FISA.

As discussed in Section II.B.2, internet surveillance falls within the EO 12333 regime when it is conducted on foreign soil, and when it does not fall within the 1978 FISA definition of "electronic surveillance". Or as the N.S.A. recently put it, when surveillance is "conducted through various means around the globe, largely from outside the United States, which is not otherwise regulated by FISA".[61]

While FISA surveillance is conducted from U.S. soil, EO 12333 surveillance is mostly conducted abroad. EO 12333 presumes that network traffic intercepted on foreign soil belongs to non-U.S. persons.[62] Companies and associations are also considered in the

[58] *Id.*, at §8(f).

[59] *See* Marcy Wheeler, *Snowden: "A Classified Executive Order"*, Emptywheel.net, May 30, 2014, *available at* http://www.emptywheel.net/2014/05/30/snowden-_a-_classified-_executive-_order/

[60] NSA/CSS POLICY No. 1-23, *supra* note 56, at Annex, *available at* http://cryptome.info/nsa-css-1-23.htm#annex.

[61] National Security Agency, *Memorandum: The National Security Agency: Missions, Authorities, Oversight and Partnerships*, see supra note 6, at 2-3. The statement seems to suggest that all surveillance operations, even domestic ones, that do not fall with the 1978 FISA definition are regulated by EO12333. 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.

[62] §9.8 USSID 18, *see supra* note 5, defining 'foreign communications'.

EO 12333 definition of U.S. persons.[63] These entities may be assumed to be non-U.S. persons if they have their headquarters outside the U.S. Even when it is known to the N.S.A. that a company is legally controlled by a U.S. company, it may be assumed a non-U.S. person under USSID 18. Taken together, the barriers for presuming that surveillance does not affect a U.S. person under EO 12333 are low. In contrast, FISA minimization policies direct authorities to presume that surveillance operations conducted on U.S. soil affect U.S. persons.

Installing a device. To understand how EO 12333 regulates the network protocol manipulations we will describe in Section III.B, we now return to the question of 'installing a device'.[64] 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. It is not covered in the definitions of 'collection',[65] 'interception'[66] nor in the definition of 'electronic surveillance'.[67] 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 N.S.A. memorandum does not provide any clarity. To the contrary:[68]

> *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.*

[63] §9.18.e.2, USSID 18, *see supra* note 5, defining 'U.S. person'.

[64] *See* also the discussion in Section II.B.2 of this article.

[65] §9.2 USSID 18, *see supra* note 5.

[66] §9.11 USSID 18, *see supra* note 5.

[67] §9.7 USSID 18, *see supra* note 5.

[68] National Security Agency, *Memorandum: The National Security Agency: Missions, Authorities, Oversight and Partnerships*, see supra note 6, at 2-3.

One sensible observation we can make at this point is that a leaked document seems to suggest that EO 12333 governs untargeted malware. 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 or not "a more sophisticated … implant" may be deployed on infected machine.[69] Importantly, the USSID 18 check is only performed after the untargeted VALIDATOR malware has been deployed. In other words, legal protection only comes into play once the N.S.A. specifically knows who it is targeting, based on the identity of a target or the location of his/her machine. This is consistent with our earlier argument that the 1978 FISA definition of 'installing a device' in itself does not cover the advanced network manipulations we present in Section III.B.[70]

3. Legal Protections For Americans Under EO 12333.

EO 12333 provides that electronic surveillance should consider the rights of U.S. persons.[71] The details are further specified in the underlying documentation, in particular in USSID 18. In the Washington Post, a former N.S.A. chief analyst claims that surveillance regulated by EO 12333 affords less legal protection to Americans than operations authorized under FISA:[72]

[69] N.S.A. VALIDATOR SLIDE DECK, published by DER SPIEGEL*, see supra* note 43.

[70] *See supra* section II.B.2.

[71] §1.1 EO 12333, *see supra* note 4.

[72] Barton Gellman and Ashkan Soltani, *N.S.A. Infiltrates Links To Yahoo, Google Data Centers Worldwide, Snowden Documents Say*. THE WASHINGTON POST, *see supra* note 12.

> *"Look, 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," he said. "It's fair to say the rules are less restrictive under Executive Order 12333 than they are under FISA," the Foreign Intelligence Surveillance Act.*

In spite of the redactions in USSID 18, we can make several new contributions to our collective understanding how legal protection for U.S. persons are less restrictive under EO 12333.

Intentionally targeting U.S. persons. Our analysis concentrates on not 'intentionally targeting U.S. Persons'. But we observe EO 12333 does establish that electronic surveillance operations that fall under its regime *and* do not fall under the FISA regime, may intentionally intercept U.S. persons communications as long as they meet the requirements summed up in USSID 18. Section 4 of USSID 18 is titled 'Collection', and contains a §4.1, spanning four pages of exceptions,[73] as well as a §4.2 which is completely redacted.[74] Before looking at the specific exceptions in §4.1., we mention that a central passage of the opening paragraph of §4.1 is redacted. It reads:[75]

> *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:*

Here we can only call attention to the redaction, but we have no possibility of knowing what it exactly states. In addition, the entire subsection on 'international communications' is redacted.[76] These subsections would be some of many candidates for

[73] §2.4 EO 12333, *see supra* note 4, and §4.1 USSID 18, *see supra* note 5.

[74] §4.2 USSID 18, *see supra* note 5.

[75] *Id.* at §4.1.

[76] *Id.* at §4.1.(b).(a).

transparency that could be obtained via political oversight or FOIA requests.

There are other specific exceptions where 'communications which are known to be to, from, or about U.S. persons' may be 'intentionally intercepted'.[77] Even with the many redactions, we can see that the exceptions provide less protection on critical points than the already permissive 'minimization procedures' under FISA.

Often, instead of FISA Court approval, some operations merely require Attorney-General approval, and others only need the approval of the Director of the N.S.A. Out of over dozens of scenarios mentioned, one especially interesting instance is the *consent* exception.[78] It holds that when U.S. persons (including U.S. corporations) consent to a surveillance operation, the approval of the Director of the N.S.A. suffices to go ahead with a program as long as the surveillance did not fall within the FISA regime. Indeed, May 2014 saw revelations on N.S.A.'s 'strategic partnerships' with several leading corporations, which may point at obtained 'consent'.

To clarify the impact of the *consent* exception, consider a hypothetical example of how it could be interpreted and applied: the N.S.A. could obtain consent from AT&T – a 'U.S. 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 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, we do not intend to speculate on these hypotheticals, especially since several sentences in USSID 18 remain redacted, prohibiting us from establishing scenarios with complete certainty. To enable further

[77] *Id.* at §4.1.(a)-(d).

[78] *Id.* at §4.1.(c).(1).

understanding of the scope of surveillance abroad on Americans, authorized by unilateral approval by the Director of the N.S.A. combined with the 'consent' of U.S. corporations, it would be useful to target political pressure or FOIA requests at section 4 of USSID 18.

Wide exemptions to process U.S. person data already collected. Under USSID 18, further processing of communications of foreigners is unrestrained.[79] In addition, there are several generous exemptions that allow for further processing of communication between U.S. persons intercepted during the collection of foreign communications, including when communications are encrypted; when they are 'significant' for a 'foreign intelligence' purpose; when they are useful as evidence in criminal proceedings and when they are helpful to reveal communications security vulnerabilities.[80] Under USSID 18, the Director of the N.S.A. gets to decide whether these scenarios apply, and whether communications between U.S. persons can be retained pursuant to Advocate-General approved procedures. Under FISA, the Attorney-General makes such determinations subsequent to FISA Court approved procedures.

4. The Official N.S.A. Response To Our Analysis.

As noted in Section I, coverage of an earlier online version of this article by *CBS News* spurred an official response from the N.S.A. compliance department. The relevant part of the media report reads as follows:[81]

> *However, an N.S.A. spokesperson denied that either EO 12333 or USSID 18 authorizes targeting of U.S. persons for electronic*

[79] *Id.* at §5.3.

[80] *Id.* at §5.4.(d).

[81] Zack Whittaker, *Legal Loopholes Could Allow Wider NSA Surveillance, Researchers Say*, CBS NEWS, *see supra* note 7.

> *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 N.S.A. statement was published online on July 11, 2014.[82] We have not received a reaction from the N.S.A. since. We point out that the N.S.A. statement 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 U.S. persons", an issue we barely analyze. Indeed, the loopholes we identify exist when i) surveillance is conducted abroad and ii) when operations do *not* "intentionally target a U.S. person." The N.S.A. statement, therefore, does not address our concerns.

Moreover, in re-wiring the legal situation to cover the targeting of U.S. persons, the element "absent limited exceptions (for example, an emergency)" of the N.S.A. statement also becomes misleading. As mentioned in Section II.B.3., exceptions for targeting U.S. persons under EO 12333 are outlined in USSID 18 Section 4. We have already observed that these span four redacted pages, and include a completely classified paragraph (§4.2). Once again, we emphasize that 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

[82] Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution, the N.S.A. 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/.

paragraph – which could amount to dozens of actual scenarios – as "limited".

5. EO 12333 Reform: Solely The Executive Branch.

A more fundamental difference between EO 12333 and FISA can be signaled at this point: over the next years, three branches of Government are 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 of Government. This simple observation has a long tradition in U.S. Constitutional law, that gives broad Article II authorities to the U.S. President when it comes to protecting national security against overseas threats. As we will point out in Section III, however, today's technologies challenge the long-standing core concept in U.S. 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 the EO 12333 legal regime, which regulates surveillance operations conducted abroad.

The constitutional constrains result in a lack of oversight or checks and balances between separate branches of Government. Even if Advocate-General approved procedures must be submitted to the U.S. Senate Intelligence Committee, tasked to oversee U.S. intelligence agencies, several media have reported on both legal or practical constraints to oversight.[83] These range from the Executive constructing permanent emergency national security scenarios that obstruct oversight, or Congress being practically barred from oversight via classification or practical constraints that include

[83] *See* supra note 11 and note 12. See also Mark Danner, *He Remade Our World*, THE NEW YORK REVIEW OF BOOKS, April 3, 2014, *available at* http://www.nybooks.com/articles/archives/2014/apr/03/dick-cheney-he-remade-our-world/ and Ryan Lizza, *State of Deception*, THE NEW YORKER, December 13, 2013, *available at* http://www.newyorker.com/magazine/2013/12/16/state-of-deception.

being forbidden to take notes or bring assistants to briefings. The Committee Chair, Senator Dianne Feinstein (D-Cal) has said:[84]

> *"Twelve-triple-three [EO 12333] programs are under the executive branch entirely." Feinstein has also said the order has few, if any, privacy protections. "I don't think privacy protections are built into it," she said."*

One could contemplate whether the relative lack of authority for EO 12333 policies in the broader policy arena, beyond the Executive branch, could explain why there are still so many redactions in place in USSID 18. In any event, considering the legal loopholes we identify in EO 12333, and our upcoming discussion on technical means by which they can be exploited, we argue that EO 12333 reform is urgent to protect Americans privacy. Even if the PCLOB announced investigation of EO 12333 policies in July 2014,[85] it reports directly to the U.S. President. 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 concluded in Mid December 2014, U.S. Congress introduced and approved a new legal provision within 48 hours, possibly with deep implications for protections afforded to U.S. persons during surveillance operations conducted abroad. This s. 309 of the Intelligence Authorization Bill 2014-15[86] mandates Attorney-General procedures to set a 5 year retention limit on data collected abroad that involves U.S. persons, in fact codifying similar

[84] Quoted in Ali Watkins, *Most Of NSA's Data Collection Authorized By Order Ronald Reagan Issued*, McCLACTHYDC, November 31, 2013, *available at* http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html. Similar quotes in *supra* note 12.

[85] *See supra* note 9.

[86] Section 309, Intelligence Authorization Act for Fiscal Year 2015, H.R.4681, 113th Congress (2013-2014).

provisions as in USSID 18 into statute.[87] The new provision was introduced shortly before the deadline of the budget negotiations, hardly debated, and approved within 48 hours by both the Senate and the House. The bill has been sent to the President who most probably will sign the entire Intelligence Authorization Bill into law in due course.

Why was the quick introduction of s. 309 needed in the first place? The wording of s. 309 leaves many open questions as to its exact meaning and implications, but has become subject of considerable controversy and debate amongst lawmakers, the media and civil society upon its 'discovery' by Rep. Amash (R-Mich.) on 11 December 2014, hours before the deadline for passing the budget. For instance, it is unclear how s. 309 relates to sections 703 and 704 of FISA, that afford more robust protections to U.S. persons when data is collected abroad. One plausible explanation could be that the new provision legitimizes an already existing surveillance operation that collects huge amounts of U.S. person data on foreign soil, without approval of the FISA Court.[88] This would be an intelligent move from a compliance perspective. By approving s. 309, U.S. Congress may 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 s. 309, lower legal protections to Americans under USSID 18 minimization procedures could have become elevated to statutory law, making compliance of programs such as MUSCULAR – discussed in section III.A.1. – that have been previously based on

[87] See *supra* note 80 and discussion in Section II.C.3. The official record mentions that "although the executive branch already follows procedures along these lines, Section 309 would enshrine the requirement in law." See: http://intelligence.house.gov/press-release/fact-sheet-hr-4681-fiscal-year-2015-intelligence-authorization-act.

[88] See M. Wheeler, *Section 309: A Bandaid for a Gaping Wound in Democracy*, Emptywheel.net, December 14, 2014, available at https://www.emptywheel.net/2014/12/14/section-309-a-band-aid-for-a-gaping-wound-in-democracy/. Wheeler includes public statements made by Bob Litt, General Counsel in the Office of the Director of National Intelligence.

EO 12333 and USSID 18 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 s. 309 renders robust conclusions on its implications impossible. At this point, we can only flag the issue for further research. But one can clearly 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 legislator.

If signed into law by the President, s. 309 may go down as a historic moment in surveillance policy. It could entail a significant lowering of legal protection afforded to U.S. persons when data is collected abroad. It also seems the very first time that U.S. Congress involves itself directly with data collection and retention usually regulated under EO 12333. The paradoxical effect of s. 309 may well be, that a hastily introduced and approved legal provision that lowers privacy protection for Americans may have set a legal precedent for more transparently deliberated, better informed and perhaps privacy protective approaches going forward.

D. Summary.

Surveillance programs under EO 12333 may collect startling amounts of sensitive data on both foreigners and Americans. 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 of judiciary involvement. Generous exemptions, more permissive than under FISA, exist that enable use of information 'incidentally' collected on U.S. persons, and critical details remain classified. Overcoming these concerns remains an issue that will be addressed entirely by the Executive branch. So far, it has not sufficiently been

addressed at all, most probably because the lack of checks and balances between three branches of Government.

Much of the lowered legal protection we have signaled demonstrates how 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, rather than 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.

III. Loopholes that Exploit Network Protocols

We have just argued the that collection of a U.S. 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 agency to conduct surveillance operations on foreign soil, regardless of whether these operations actually affect American communications or not.

We now discuss how the technical details of Internet's core protocols can cause traffic sent by Americans to be routed abroad, where it 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 can be deliberately manipulated to cause Americans' traffic to be routed abroad.

A. Why U.S. 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, at the same time, minimizing cost. It is not uncommon for network traffic between two endpoints located on U.S. soil to be routed outside the U.S.

1. Interception In The Intradomain.

A network owned by a single organization can be physically located in multiple jurisdictions, even if an organization is nominally "based" in the U.S. like Yahoo! or Google. The revealed MUSCULAR program illustrates how the N.S.A. presumed authority under EO 12333 to acquire traffic between Google and Yahoo! servers by tapping fiber-optic cables on foreign territory (in the UK), collecting up to 180 million user records per month, regardless of nationality.[89] Yahoo! and Google replicate data across multiple servers stored that periodically send data to each other, likely for the purpose of backup and synchronization. These servers are located in data centers in geographically diverse locations, likely to prevent valuable data from being lost in case of outages, or errors, in one location. The MUSCULAR program collects the traffic sent between these data centers: while this traffic can traverse multiple national jurisdictions, it remains with the logical network boundaries of the internal networks of Yahoo! and Google. Thus, we already have one example where loopholes under the legal regime of EO 12333 were applied in the *intradomain*, i.e., within the logical boundaries of a network owned by a single organization.

[89] *See supra* note 12. 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, November 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/.

2. Interception In The Interdomain.

Another possibility is the *interdomain* setting, where traffic traverses networks belonging to different organizations. Specifically, interdomain routing with BGP can naturally cause traffic originating in a U.S. network to be routed abroad, even when it is destined for a network that is located on U.S. soil.

BGP (i.e., the Border Gateway Protocol) is the routing protocol that enables communication between networks owned by different organizations (Autonomous Systems or ASes, e.g., Google's network, China Telecom's network, or Boston University's network). ASes are interconnected, creating a graph where nodes are ASes and edges are the links between them.[90] ASes use BGP to learn paths through the AS-level graph; an AS discovers a path to a destination AS via BGP messages that it receives from each of its neighboring ASes. 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, and then forwards all traffic for the destination AS to the neighboring AS that announced the most-preferred path.

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. This means that it can sometimes be cheaper to forward traffic through a neighboring AS that is physically located in a different country, rather than one located in the same country; this situation is common, for example, in South America where network paths between two South American endpoint ASes often cross

[90] *See infra* Fig. 2 at Section III.B.1 for a graphical representation that discusses a deliberate BGP manipulation to route internet traffic abroad.

undersea cables to Miami,[91] as well as Canada where network paths between two Canadian endpoint ASes regularly traverse American ASes.[92]

3. The N.S.A.'s Ability to Intercept Traffic on Foreign Soil.

Recent revelations have indicated that the N.S.A. does have 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 different ASes.[93] We provide a brief and non-exhaustive overview of revelations of cable-tapping activities apparently connected by a division of the N.S.A. known as Special Sources Operation (SSO).[94]

One program, codenamed WINDSTOP, deals with collecation from "second party" countries, i.e., one of the "five eye" countries (the U.S.A., U.K., Canada, New Zealand, Australia). The MUSCULAR program (that we discussed in Section III.A.1) falls under the umbrella of WINDSTOP, as does the INCENSER program that apparently collected two orders of magnitude (14 billion) more user records than MUSCULAR in the same 30 day

[91] Doug Madory, *'Crecimiento' in Latin America*, RENESYS Blog, May 23, 2013, *available at* http://www.renesys.com/2013/05/crecimiento-in-latin-america/.

[92] Andrew Clement et. al., *IXmaps*, UNIV. OF TORONTO, *available at* http://ixmaps.ca/. Ongoing work by Sharon Goldberg seeks to measure how often this occurs when both endpoints are located in the U.S.

[93] The FLAG Atlantic 1 cable from the U.K. to the U.S., for example, is has a potential capacity of 4.8 Terabit/sec., see: http://sdc.flagtelecom.com/network/flag_atlantic_1.html.

[94] 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*, THE WASHINGTON POST, December 23, 2013, *available at* 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.

period.[95] INCENSER involves tapping into the network linking one trans-Atlantic fiber-optic cable from the U.S. to the U.K (the "FLAG Atlantic 1" cable) to another transnational cable from the U.K. to Japan via the Mediterranean, India and China (the "FLAG Europe Asia" cable). The cable was tapped on British soil by the GHCQ, and the collected traffic was shared with the NSA.[96]

Meanwhile, the N.S.A'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. The foreign country taps into international fiber-optic cables located on its own territory, moves the raw traffic to a processing center on its territory that contains N.S.A.-provided equipment, and finally forwards the traffic to a N.S.A. site on U.S. soil. The three largest RAMPART sites – codenamed AZUREPHOENIX, SPINNERET and MOONLIGHTPATH – tap a total of seventy different international cables; while the locations of various sites remain unknown, media reports suggest that both Germany and Denmark are involved.[97]

[95] *See* Barton Gellman and Matt DeLong, *One month, Hundreds of Millions of Records Collected*, THE WASHINGTON POST, *supra* note 16.

[96] Details of the INCENSER program were revealed by Geoff White, *Spy Cable Revealed: How Telecoms Firm Worked With GCHQ*, CHANNEL4, November 20, 2014 *available at* http://www.channel4.com/news/spy-cable-revealed-how-telecoms-firm-worked-with-gchq; Frederik Obermaier, Henrik Moltke, Laura Poitras and Jan Strozyk, *Snowden-Leaks: How Vodafone-Subsidiary Cable & Wireless Aided GCHQ's Spying Efforts*, SÜDDEUTSCHE ZEITUNG INTERNATIONAL, November 25, 2014, *available at* http://international.sueddeutsche.de/post/103543418200/snowden-leaks-how-vodafone-subsidiary-cable.

[97] Anton Geist, Sebastian Gjerding, Henrik Moltke and Laura Poitras, *NSA 'Third Party' Partners Tap The Internet Backbone In Global Surveillance Program*, INFORMATION, June 19, 2014, *available at* http://www.information.dk/501280 and Ryan Gallagher, *How Secret Partners Expand NSA's Surveillance Dragnet,* THE INTERCEPT, June 19, 2014, *available at* https://firstlook.org/theintercept/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a.

B. How Deliberate Manipulations Can Divert U.S. 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. As we discussed earlier,[98] deliberately manipulating Internet protocols for subsequent data collection from abroad, even when the manipulation was performed from within the U.S., does not fall under the legal definition for 'electronic surveillance' in FISA; 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).

1. Deliberate BGP Manipulations.

We know of numerous real-world incidents where manipulations of the BGP protocol have caused network traffic to take unusual paths, including situations where traffic from two American endpoint ASes was rerouted through ASes physically located abroad. While 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 U.S. persons by forcing their network traffic to be diverted abroad and intercepting it on foreign soil.

In 2013, Renesys observed a number of highly-targeted manipulations of BGP that caused traffic sent between two American endpoint ASes to be routed through Iceland.[99] One manipulation that occurred on June 31, 2013, is shown in Fig. 2:

[98] *See supra* at Section II.B.2 and Section II.C.2.

[99] *See* A. Peterson, *Researchers Say U.S. Internet Traffic Was Re-routed Through Belarus. That's a Problem*, THE WASHINGTON POST, November 20, 2013, *available at*

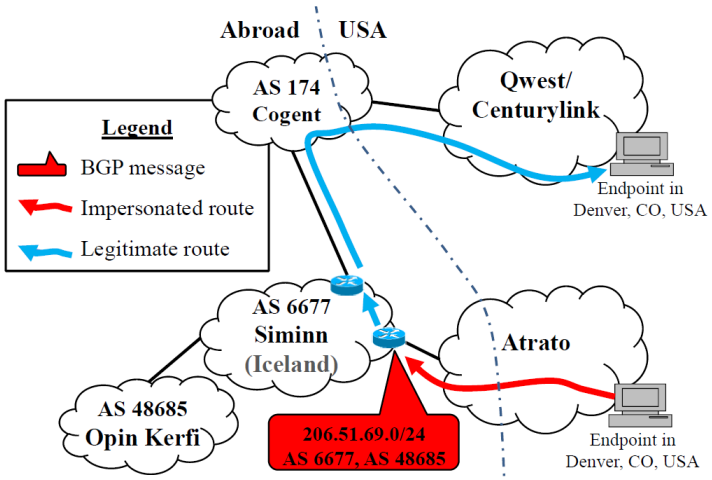

Fig. 2: On June 31, 2013, manipulator AS Siminn in Iceland used BGP to send an "impersonated route" for IP address block 206.51.69.0/24, allowing Siminn to intercept traffic sent between two endpoints in Denver, CO, USA.[100]

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

Similar incidents have been known to occur periodically in the Internet.[101] In 2010, for example, a routing incident caused

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/.

[100] *See* Jim Cowie, *The New Threat: Targeted Internet Traffic Misdirection*, RENESYS Blog, November 19, 2013, *available at* http://www.renesys.com/2013/11/mitm-internet-hijacking/. Also, *see supra* note 99.

[101] *See* Kevin Butler et. al., *A Survey Of BGP Security Issues And Solutions*, Proc. of the IEEE, 98(1), 2010, at 100-122.

traffic sent between multiple American endpoint ASes to be diverted through China Telecom during a single 18-minute time period.[102] In 2008, a presentation at DEFCON demonstrated how these manipulations could be performed in a covert manner.[103] This method could be used to confound the network measurement mechanisms (e.g., traceroute, BGP looking glasses) that researchers used to detect the 2010 and 2013 incidents mentioned above.

Target of the BGP manipulation. To understand how the legal framework applies to manipulations of the BGP protocol for the purpose of surveillance, we need to understand who is targeted.

The incidents mentioned above are executed as follows. Per Fig. 2, the manipulating AS (e.g., Icelandic AS Siminn) manages to divert traffic to itself by sending to some carefully selected neighboring ASes, BGP messages that "impersonate" those sent by the legitimate destination AS (Qwest/Centurylink's AS). Because BGP lacks authentication mechanisms, these neighbors (Atrato's AS) accept the BGP message for the impersonated route, and select the impersonated route. The neighbors (Atrato) then forwards their traffic along the impersonated route to the manipulator's AS (Icelandic AS Siminn). The manipulator receives the traffic, and forwards it back to the legitimate destination AS (Qwest/Centurylink) via a legitimate route. The manipulator AS therefore becomes a man-in-the-middle between targeted source AS (Atrato) and the destination AS (Qwest/Centurylink). While Fig. 2 shows traffic between two individual endpoints within Atrato and Qwest/Centurylink being intercepted by the BGP manipulation,

[102] Jim Cowie, *China's 18-minute Mystery*, RENESYS Blog, November 18, 2010, *available at* http://www.renesys.com/blog/2010/11/chinas-_18-_minute-_mystery.shtml.

[103] Anton Kapela and Alex Pilosov, *Stealing The Internet*, DEFCON 16, August 10, 2008, *available at* https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf.

typically all traffic originating inside Atrato and destined to the Qwest/Centurylink AS would be intercepted by the manipulator.

To further understand the targets of this manipulation, we consider what it means to send BGP messages that "impersonate" a legitimate destination AS. First, we provide more detail on BGP messages. A BGP message is used to advertise the path to a specific IP address block hosted by a particular destination AS.[104] Each AS in the Internet is allocated one of more IP address blocks, used to identify devices operated by that AS. Multiple devices can use a single IP address; thus, referring back to our legal analysis, a single IP address can be used by multiple devices or even 'persons'. A separate BGP message is used to advertise each IP address block allocated to a particular destination AS.

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 Fig. 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 (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.

[104] 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 (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.

Thus, we can see that 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).

That has important legal implications: the permissive legal regime under EO 12333 applies to such surveillance operations, as it does not necessarily 'intentionally' target a 'known, particular U.S. person'. One issue to flag here is whether targeting Atrato or Qwest/Centurylink could be seen as "intentionally targeting a U.S. person", which could mean FISA applies. This issue arises because companies can also be "U.S. persons" under FISA and EO 12333. As we saw in the MUSCULAR operations outlined in Section III.A, Google and Yahoo! traffic had been intercepted from abroad under EO 12333; from the revelations, it follows that the authorities are not "targeting" these internet companies directly in the legal sense, but are instead "targeting" users of these services that are not yet 'known' in the legal sense. Applying this logic to the Atrato/Qwest/Centurylink example, we argue that the permissive legal regime under EO 12333 applies. We reiterate here that we cannot establish with full certainty how the intelligence community applies FISA and EO 12333 in practice, but we can use the revealed MUSCULAR program for some clues. This would be one of the important points to clarify in any EO 12333 investigation, such as the one announced by the PCLOB.

Location of the BGP manipulation. Finally, we note that this BGP manipulation, which involves sending just a single impersonated BGP message from the Icelandic AS Siminn, shown in red in Fig. 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 mean that we do not know if EO 12333 applies different regulations to manipulations conducted domestically vs. on foreign soil; however, the example in Fig. 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 DNS (i.e., Domain Name System). 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 (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. 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.[105] 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.

The DNS is well known to be vulnerable to manipulations that subvert the mapping from a domain name to IP address.[106] These manipulations, which have been observed in the wild as mechanisms for performing network censorship,[107] can also be used

[105] *See infra* Fig. 3.

[106] Steve Bellovin, *Using The Domain Name System For System Break-Ins*, Proc. of 5th USENIX Security Symposium, 149(1), 1995; Dan Kaminsky, *Black Ops 2008: Its The End Of The Cache As We Know It*, Black Hat USA, 2008; Amir Herzberg and Haya Shulman, *Fragmentation Considered Poisonous, Or: One-Domain-To-Rule-Them-All.Org*, Communications and Network Security, IEEE, 2013, p. 224–232. 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.

[107] Jonathan Zittrain and Benjamin Edelman, *Internet Filtering In China*, IEEE Internet Computing, 7(2), p. 70–77, 2003. *See also* The Open Network Initiative at http://opennet.net/.

to redirect network traffic through servers located abroad. Fig. 3 presents an example:

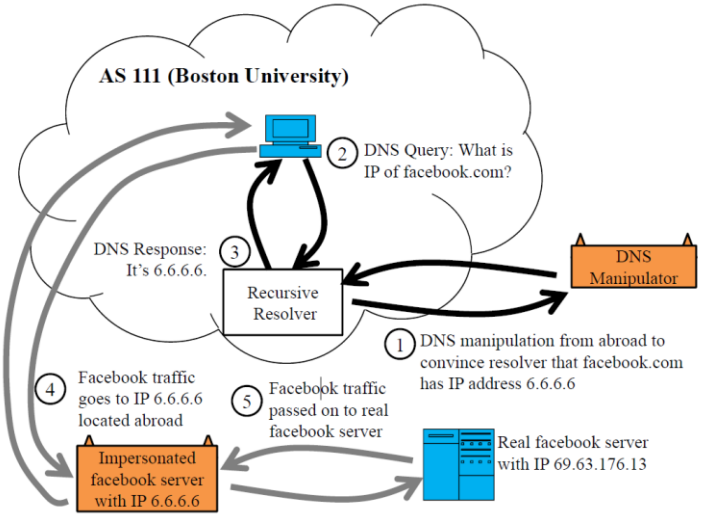

Fig. 3: Schematic showing how DNS manipulations can be used to direct traffic between two American endpoints (Boston University and facebook) to be routed abroad. The DNS manipulation technique labeled (1) is described in more detail in Fig. 4.

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. 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. 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, what surveillance law applies is based on who is targeted. The DNS manipulation is more fined-grained than the BGP manipulation we discussed earlier: it targets all traffic sent to a particular domain that is sent by all users and applications served by the targeted recursive resolver (i.e., within a Boston University's AS).

As we discussed in Section II, we again need to consider whether targeting Facebook or Boston University is "intentionally targeting a U.S. person", since organizations can be "U.S. persons" under FISA and EO 12333. Again, 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' in the legal sense. If the same logic applies as in MUSCULAR, our DNS manipulation is not 'intentionally targeting a U.S. person' and is therefore regulated by the permissive legal regime under EO 12333. We reiterate that we cannot establish with full certainty how the intelligence community applies FISA and EO 12333 in specific cases. Again, this point could be clarified as part of any investigation into EO 12333, such as the one announced by the PCLOB.

Location of the DNS manipulation. Like the BGP manipulations we described earlier, these DNS manipulations can be conducted entirely abroad; Hertzberg and Shulman describe a technique that allows this manipulation to be executed by a device located entirely outside the targeted source AS.[108] The technique can be explained with Fig. 4:

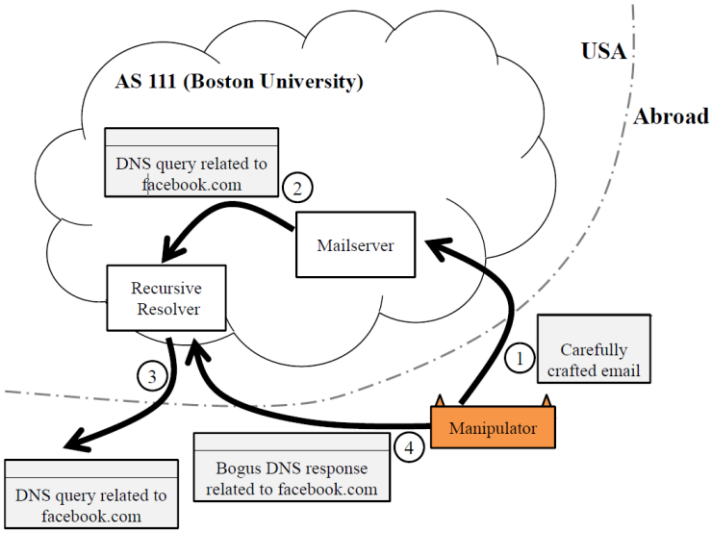

Fig. 4: Hertzberg and Shulman's technique for subverting the DNS mapping for a particular domain (www.facebook.com) in a recursive resolver that serves a particular target AS (Boston University AS 111). The manipulator can be located entirely outside the target AS, and need only send DNS messages and emails. No devices within the target AS need to be compromised.

First, it is important to observe that recursive resolvers usually do not accept messages from senders outside their AS; however, mailservers do.[109] Thus, a manipulator located outside the

[108] Amir Herzberg and Haya Shulman, *Fragmentation Considered Poisonous, Or: One-Domain-To-Rule-Them-All.Org*, *see supra* note 106.

[109] Mailservers are devices that provide email services for an AS. They therefore need to accept emails from outside the AS.

target AS can use the mailserver to attack the recursive resolver. Specifically, the manipulator sends some carefully-crafted messages to a mailserver located inside the target AS. 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. 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. 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. Observe that this manipulation just involves sending messages from outside the AS; no internal devices in the AS need to be compromised. Again, this manipulation can 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. Therefore, we argue that such manipulations are regulated by the permissive legal regime under EO 12333.

From a close look at the definitions in the legal regimes, it follows that protocol manipulations do not have to be executed entirely abroad to be regulated under EO 12333. To be completely confident that they can also be conducted on U.S. soil under EO 12333, one needs to have complete insight into USSID 18. On the face of it, however, EO 12333 and USSID do not define 'targeting' and FISA does not include manipulations within its scope.

While the BGP and DNS manipulations we described here can be executed entirely abroad, and thus regulated by EO 12333 as we have argued, there are whole other classes of manipulations that might be executed on U.S. soil. This class of manipulations include

any network exploit executed by an attacker that wishes to become a man-in-the-middle on a communication path.

Here we just mention a particularly interesting class of manipulations: hacking into U.S. routers or switches and installing routes that divert traffic abroad. Recent revelations suggest that the N.S.A. does have the capability to take control of remote routers (e.g., the HEADWATER, SCHOOLMONTANA, SIERRAMONTANA, and STUCCOMONTANA programs).[110] It was also revealed that the N.S.A. can physically tamper with U.S.-made routers.[111] Another possibly relevant class of manipulations is the SECONDDATE program, which the N.S.A. calls "an exploitation technique that takes advantage of web-based protocols and man-in-the-middle capabilities".[112] Once again, we are not in a position to establish whether the N.S.A.'s ability to subvert network protocols and routers is actually used in practice to circumvent the statutory and constitutional protections provided to U.S. 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. However, based on the recently increased transparency and our subsequent analysis we do see sufficient basis to conclude that the legal and technical possibilities are there.

[110] Jacob Appelbaum, Judith Horchert and Christian Stcker, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, DER SPIEGEL, December 29, 2013, *available at* 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, January 3, 2014, *available at* http://www.computerworld.com/article/2474275/cybercrime-hacking/17-exploits-the-nsa-uses-to-hack-pcs--routers-and-servers-for-surveillance.html.

[111] Glenn Greenwald, *How The NSA Tampers With US-Made Internet Routers*, THE GUARDIAN, May 12, 2014, *available at* http://www.theguardian.com/books/2014/may/12/glenn-_greenwald-_nsa-_tampers-_us-_internet-_routers-_snowden?r.

[112] Ryan Gallagher and Glenn Greenwald, *How The NSA Plans To Infect Millions Of Computers With Malware*, THE INTERCEPT, March 12, 2014, *available at* https://firstlook.org/theintercept/article/2014/03/12/nsa-_plans-_infect-_millions-_computers-_malware/.

IV. Conclusion

International communications intercepted on U.S. soil are regulated by FISA and overseen by Congress and the FISA Court. Revealed surveillance operations regulated by FISA are subject of a broad public debate, and being challenged on constitutional merits at courts across the U.S. By contrast, 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 — to not 'intentionally target a U.S. person' (e.g., bulk surveillance) and to be conducted abroad. EO 12333 and its underlying guidelines (notably USSID 18) contain permissive "foreignness-presumptions", and as long as users are not intentionally targeted, operations on foreign soil are presumed to affect foreigners exclusively. As foreigners do not enjoy 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.

Technological developments make these legal loopholes exploitable. The vagaries of Internet protocols can sometimes cause traffic sent between two U.S. 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 U.S. endpoints takes an unusual path through a device under N.S.A. control located abroad. Recent months have seen a number of revelations on the technical capabilities of the U.S. intelligence community, including tapping fiber optic cables and remotely controlling routers, which could potentially be used to exploit these legal loopholes.

If the two main legal criteria for EO 12333 applicability are met, the interdependent legal and technical loopholes enable largely unrestrained surveillance on the internet communications of

Americans. 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 U.S. Internet company (Google, Yahoo!), in bulk, is not considered to "intentionally target a U.S. person" per the legal definition in FISA by the intelligence community. Instead, individual users of these Internet companies' services were considered (in the legal sense) to be the 'target' of the operation. Because these users were not specifically 'targeted' in the legal sense at the time the network traffic was collected in bulk, MUSCULAR was regulated under the most permissive legal regime for surveillance in the U.S. legal framework, i.e., EO 12333 and its underlying Directives, notably USSID 18. From these revelations, we infer that the EO 12333 regime also regulates the deliberate network protocol manipulations (of BGP or DNS) that we described in Section III.B.

We reiterate that we do not intend to speculate on the extent to which the intelligence community is exploiting the loopholes we describe. Instead, our aim is to broaden our understanding of the possibilities and deeper issues at hand. Moreover, our analysis of loopholes in EO 12333 is not exhaustive; we focus on bulk surveillance on Americans by collecting their network traffic abroad. Recent revelations indicate that other types of surveillance operations are also authorized under EO 12333, including the deployment of malware.

Our analysis has highlighted a central problem in law; namely, that law has an old-fashioned focus on physical materiality. The geographical site of interception determines what surveillance laws apply, and thus the legal protection 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.

A. Possible remedies.

FOIA requests. In terms of addressing the loopholes we identify, the vast amount of still redacted policy documents — in particular in USSID 18 — is a first point to address. Even if the U.S. Government has released several insightful policy documents in recent months, often these refer to redacted or completely classified legal documentation that cannot be studied. The dozens of documents released in the FOIA case ACLU v. N.S.A. so far do not cover our analysis.[113] The lack of transparency on surveillance policies limit policymakers, academics, the general public and even the U.S. Supreme Court in *Clapper v. Amnesty* from establishing a comprehensive overview of the Fourth Amendment implications of current network surveillance policy.

Technical solutions. Purely technical solutions like encryption, DNSSEC, and the RPKI can also help combat some of the specific risks of the loopholes we identified.

Indeed, this year has seen a significant increase in efforts to encrypt Internet traffic. In response to revelations about the MUSCULAR program we described in Section 3.A.1, Google and Yahoo! have moved to encrypt the intradomain communication links between their data centers, and a number of other corporations have followed suit.[114] There has also been increased interested in encrypting interdomain traffic between users and

[113] American Civil Liberties Union et. al. v. National Security Agency et. al., Civil Action No. 13-9198 (AT) U.S. District Court Southern District of New York.

[114] See *EFF's Encrypt the Web Report, available at* https://www.eff.org/encrypt-the-web-report. The Electronic Frontier Foundations 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".

websites, through the deployment of the HTTPS protocol for encrypted web traffic.[115] The Internet Architecture Board (IAB) issued a statement on Internet confidentiality, indicating that "protocol designers, developers, and operators [should] make encryption the norm for Internet traffic."[116] And there are new efforts underway to enable turn-key encryption of websites through the LetsEncrypt project.[117]

However, we note here that while 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.[118] In addition, FISA and the USSID 18 minimization procedures permit extensive retention and further analysis of encrypted communications even if two communicants are known to be U.S. persons.

Meanwhile, the RPKI can limit the scope and impact of BGP manipulations, but cannot not completely eliminate them, and it

[115] *See supra* note 115.

[116] Internet Architecture Board, *IAB Statement on Internet Confidentiality,* November 14, 2014, *available at* https://www.iab.org/2014/11/14/iab-statement-on-internet-confidentiality/.

[117] See https://letsencrypt.org/ and Alex Halderman, *Let's Encrypt: Bringing HTTPS to Every Web Site*, November 18, 2014, *available at* https://freedom-to-tinker.com/blog/jhalderm/announcing-lets-encrypt/.

[118] 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*, Proc. Of the 16th Privacy Enhancing Technologies Symposium, LNCS 8555, 2014, at p. 146-164. 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.

remains far from fully-deployed today.[119] DNSSEC can stop the DNS manipulations we described, and it also has not reached anything near full deployment. Moreover, we can reasonably assume that new and existing technical loopholes will continued 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 U.S.A. Freedom Act that ultimately failed to pass by a handful of votes,[120] still concentrate on the rights of U.S. 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,[121] 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 is unclear, and the Directive explicitly states that "this directive is not intended to alter the rules applicable to U.S. persons in Executive Order 12333, the Foreign Intelligence Surveillance Act, or other applicable law".[122] So far, no substantial changes can be observed since the Directive was released; it remains to be seen to what extent the Directive will influence actual surveillance policy. In contrast, while its implications remain opaque, s. 309 of the 2014-15 Intelligence Authorization Bill – hastily introduced, hardly debated and

[119] Danny Cooper et. al., *On The Risk Of Misbehaving RPKI Authorities*. Proc. 12th ACM Workshop on Hot Topics in Networks, 16(1), 2013.

[120] *See supra* note 18

[121] PRESIDENTIAL POLICY DIRECTIVE 28 – SIGNALS INTELLIGENCE ACTIVITIES, January 14, 2014. *available at* http://www.whitehouse.gov/the-_press-_office/2014/01/17/presidential-_policy-_directive-_signals-_intelligence-_activities.

[122] *Id*. at 9.

approved within 48 hours before a budgetary deadline for the new fiscal year passed – seems to lower legal protections for U.S. persons.

More fundamentally, the ability to overcome these loopholes is further constrained by U.S. lawmaking and constitutional traditions. Whereas the Patriot Act and FISA are overseen by all three branches of Government, EO 12333 remains solely under Executive Branch authority; in theory and most certainly in practice. It is likely that EO 12333 reform will remain an executive affair, as Article II of the U.S. Constitution grants the Executive branch wide national security authorities to protect the nation from threats overseas.

The implications for long term reform are real. Cross-institutional checks and balances and independent oversight may remain absent from EO 12333 policies in the years to come. The Privacy and Civil Liberties Oversight Board (PCLOB) investigation, announced on 23 July 2014, is a first step of investigating issues with EO 12333; note, however, that the Board reports directly to the U.S. President. Save general statements on the modification of policies that have been in place since the Reagan era, 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 U.S. President. In any event, the legislative and judiciary branches of Government have limited theoretical and practical ability to change the trajectory of EO 12333 reform. It is still too early to determine the exact implications of s. 309 of the 2014-15 Intelligence Authorization Bill, its interplay with FISA and whether it sets a historical legal precedent for more Congressional involvement. But our analysis shows that even if the legislative and judiciary 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 be to update the definition of 'electronic

surveillance' in FISA.[123] The first aim would be to ensure that the geographical point of collection does not determine the legal protection on offer. The second aim would be to formulate the definition 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 explicitly mention 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 we discuss in Section III.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. Unfortunately, there is a historical precedent of leaving the critical definition of 'electronic surveillance' in FISA untouched for decades, but perhaps this could change with increased public scrutiny.

Long-term remedy: the need to revisit central concepts of U.S. surveillance law. On the long term, however, effectively closing the identified loopholes requires a fundamental reconsideration of central concepts of U.S. 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 established in *United States v. Verdugo-Urquidez* and confirmed in *Clapper v. Amnesty*, that limits Fourth Amendment protection to U.S. persons, effectively protects Americans on a global internet.[124] As long as these questions remain

[123] See supra, Section II.B.2 and Section II.C.2.

[124] 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 U.S. Government, the Justices argue, they become "one of the governed" as mentioned by the U.S. Constitution. They conclude: "when we tell the world that we expect all people, wherever

unaddressed, the interdependent legal and technical loopholes we identify leave the door open for the intelligence community to circumvent the U.S. Constitution and conduct largely unrestrained bulk collection of Americans' internet traffic from abroad.

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." See *United States v. Verdugo-Urquidez*, 494 U.S. 259.