ARTICLE

No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333

Mark M. Jaycox*

*Mark M. Jaycox, Policy Counsel, Google. Prior to this, the author served as the Civil Liberties Legislative Lead at the Electronic Frontier Foundation, where he specialized on consumer privacy issues, cybersecurity, electronic surveillance, and national security law. B.A., Reed College; J.D., UC Berkeley School of Law. The author would like to thank the Professor who oversaw the initial drafts of this paper at Berkeley, Jim Dempsey. He would also like to thank Lee Tien, Jonathan Mayer, Ashkan Soltani, Neema Singh Guliani, and many more for their critical insights, discussions, and debates on this topic.

Abstract

Executive Order 12,333 ("EO 12333") is a 1980s Executive Order signed by President Ronald Reagan that, among other things, establishes an overarching policy framework for the Executive Branch's spying powers. Although electronic surveillance programs authorized by EO 12333 generally target foreign intelligence from foreign targets, its permissive targeting standards allow for the substantial collection of Americans' communications containing little to no foreign intelligence value. This fact alone necessitates closer inspection.

This Article conducts such an inspection by collecting and coalescing the various declassifications, disclosures, legislative investigations, and news reports concerning EO 12333 electronic surveillance programs in order to provide a better understanding of how the Executive Branch implements the order and the surveillance programs it authorizes. The Article pays particular attention to EO 12333's designation of the National Security Agency as primarily responsible for conducting signals intelligence, which includes the installation of malware, the analysis of internet traffic traversing the telecommunications backbone, the hacking of U.S.-based companies like Yahoo and Google, and the analysis of Americans' communications, contact lists, text messages, geolocation data, and other information.

After exploring the electronic surveillance programs authorized by EO 12333, this Article proposes reforms to the existing policy framework, including narrowing the aperture of authorized surveillance, increasing privacy standards for the retention of data, and requiring greater transparency and accountability.

Table of Contents

I. Introduction

In 2013, investigative journalists disclosed that the U.S. government had used section 215 of the USA PATRIOT Act as authorization for a now-defunct surveillance program that collected the daily call records of Americans from telecommunications companies.[1] Reporting also revealed that section 702 was, and still is, read to authorize the collection of Americans' information from the telecommunications backbone,[2] even though section 702 targets foreigners outside the United States for foreign intelligence information.[3] Since then, national security scholars have applied particular scrutiny to those two key legal authorities used for electronic surveillance, while neglecting the legal authority used for the majority of the National Security Agency's ("NSA") signals intelligence collection: Executive Order 12,333 ("EO 12333").[4]

EO 12333 codifies the President's Article II power as Commander-in-Chief and head of the Executive Branch. It authorizes the intelligence community to conduct intelligence activities "necessary for the conduct of foreign relations and the protection of the national security of the United States," including the "collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the United States, international terrorist…activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and their agents."[5] It also authorizes the collection of information "constituting foreign intelligence or counterintelligence" so long as no foreign intelligence collection by the intelligence community is "undertaken for the purpose of acquiring information concerning the domestic activities of U.S. persons."[6] In another section, it allows surveillance that would

---

[1] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, The GUARDIAN (Jun. 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/FYK7-NN9S]; Barton Gellman & Askhan Soltani, *NSA Collects Millions of E-Mail Address Books Globally*, WASH. POST (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html [https://perma.cc/VR2K-5V2R].

[2] Charlie Savage, Eileen Sullivan, & Nicolas Frandos, *House Extends Surveillance Law, Rejecting New Privacy Safeguards*, N.Y. TIMES (Jan. 11, 2018), https://www.nytimes.com/2018/01/11/us/politics/fisa-surveillance-congress-trump.html [https://perma.cc/CJ8S-6HPG].

[3] *See Signals Intelligence*, NAT'L SEC. AGENCY (May 3, 2016), https://www.nsa.gov/what-we-do/signals-intelligence/ [https://perma.cc/3UFS-L8W2]; 50 U.S.C. §§ 1801–1813; 50 U.S.C § 1881a (2017); Laura Donahue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 139 (2015); PRIV. AND C. L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 6 (2014), https://documents.pclob.gov/prod/Documents/OversightReport/823399ae-92ea-447a-ab60-0da28b555437/702-Report-2.pdf [https://perma.cc/52U9-YQ68].

[4] *See generally* NAT'L SEC. AGENCY, LEGAL FACT SHEET: EXECUTIVE ORDER 12333 (2013), https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf [https://perma.cc/S647-QR9P].

[5] Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (1981).

[6] *Id.*

typically require a warrant, such as surveillance in the United States or against a U.S. person abroad, so long as the Attorney General determines there is probable cause to believe the surveillance is directed at a foreign power or agent of a foreign power.[7]

President Ronald Reagan signed the order in 1981, giving birth to an immense policy regime that oversees a variety of intelligence collection.[8] Disclosures about the legal authority provide some insight into the NSA's EO 12333 signals intelligence—and specifically electronic surveillance—programs.[9] Much of the information is still difficult to decipher despite the disclosures. Even government analysts with full access to classified documents are advised to "adjust [their] vocabulary" before beginning EO 12333 training.[10] One handbook describes EO 12333's implementation as a "maze" due to its complexity.[11]

Documents reveal EO 12333 authorizes the collection and analysis of communications, metadata, individual identifiers like International Mobile Equipment Identity (IMEI) and mobile telephone numbers, credentials to online platforms, and other electronic information.[12] The intelligence community collects

---

[7] *See id.*

[8] *See* Mark M. Jaycox, *A Primer on Executive Order 12333: The Mass Surveillance Starlet*, ELEC. FRONTIER FOUND. (Jun. 2, 2014), https://www.eff.org/deeplinks/2014/06/primer-executive-order-12333-mass-surveillance-starlet [https://perma.cc/25QD-EMES]. *See also* NAT'L SEC. AGENCY, LEGAL COMPLIANCE AND U.S. PERSON MINIMIZATION PROCEDURES (2011); NAT'L SEC. AGENCY, SIGINT AUTHORITY DECISION TREE, https://img.washingtonpost.com/wp-apps/imrs.php?src=https://img.washingtonpost.com/blogs/the-switch/files/2014/07/12333flowchart.jpg&w=1484 [https://perma.cc/7WJ5-3DCT]; NAT'L SEC. AGENCY, OVSC1100, LESSON 2 – CONVENTIONAL COLLECTION 4 (2007), https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf [https://perma.cc/T7DC-3UG4].

[9] While some documents concerning CIA 12,333 surveillance have been released, this paper focuses on EO 12333's electronic surveillance programs operated by the NSA. For the CIA's procedures, see generally CENTRAL INTEL. AGENCY, ANNEX A—GUIDANCE FOR CIA ACTIVITIES OUTSIDE THE UNITED STATES (2013), https://www.cia.gov/library/readingroom/docs/DOC_0006235714.pdf [https://perma.cc/WJ5C-YUV3]; Electronic surveillance by CIA may be increasing in light of recent restructuring, but the CIA's actions are still largely classified. *See*, *e.g.*, Greg Miller, *CIA Looks to Expand Its Cyber Espionage Capabilities*, WASH. POST (Feb. 23, 2015), https://www.washingtonpost.com/world/national-security/cia-looks-to-expand-its-cyber-espionage-capabilities/2015/02/23/a028e80c-b94d-11e4-9423-f3d0a1ec335c_story.html [https://perma.cc/L4ZK-DZ6T]; Procedures also likely exist for electronic surveillance conducted by Air Force drones in furtherance of foreign intelligence missions. Memorandum from the Dep't of the Air Force, Air Force Guidance Memorandum to Air Force Instruction 14-104, Oversight of Intelligence Activities (Oct. 4 2018), https://fas.org/irp/doddir/usaf/afi14-104.pdf [https://perma.cc/59YG-WKNK].

[10] DEF. INTEL. AGENCY, INTELLIGENCE LAW HANDBOOK: DEFENSE HUMINT SERVICE § 3-7(a) (2004), https://www.aclu.org/files/assets/eo12333/DIA/Intelligence%20Law%20Handbook%20Defense%20HUMINT%20Service.pdf [https://perma.cc/KH5W-5A2S].

[11] *Id.*

[12] *See* Barton Gellman, Julie Tate, & Askhan Soltani, *In NSA-intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-

this information by installing malware, obtaining access to internet traffic traversing the telecommunications backbone, and hacking U.S.-based companies like Yahoo and Google.[13] One program authorized by EO 12333 is estimated to collect more than 1.8 billion emails a month.[14] Information collected under EO 12333 is even used to map Americans' social networks.[15]

This Article draws together various declassifications, disclosures, legislative investigations, and news reports to paint a clearer picture of the electronic surveillance programs implemented by the Executive Branch under EO 12333.[16] Particular attention is paid to EO 12333's designation of the NSA as the agency primarily responsible for conducting signals intelligence.[17] This Article's discussion of authorized surveillance is particularly important because EO 12333 collects Americans' information despite the order's focus on targeting foreign individuals for foreign intelligence.[18] This Article provides an introduction to EO 12333's electronic surveillance programs, and aims to serve as a foundation for further research into critical legal and policy issues. Such research could investigate separation of powers concerns, including whether Congress can regulate certain Executive Branch powers or whether a foreign intelligence exception to the Fourth Amendment of the U.S. Constitution exists.

Part I provides a general introduction to signals intelligence by broadly walking through the U.S. electronic surveillance system, including key definitions.[19] Part II provides a foundation for understanding EO 12333's legal-

---

targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [https://perma.cc/63HU-SB66]; Dominic Rushe, Spencer Ackerman, & James Ball, *Reports That NSA Taps Into Google and Yahoo Data Hubs Infuriate Tech Giants*, WASH. POST (Oct. 31, 2013), https://www.theguardian.com/technology/2013/oct/30/google-reports-nsa-secretly-intercepts-data-links [https://perma.cc/4ZZY-336G].

[13] *See* Rushe et al., *supra* note 12.

[14] Ryan Gallagher & Henrik Moltke, *The Wiretap Rooms: The NSA's Hidden Spy Hubs in Eight U.S. Cities*, THE INTERCEPT (Jun. 25, 2018), https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/ [https://perma.cc/NKH3-FL2J].

[15] *See* U.S. DEP'T OF DEF., SUPPLEMENTAL PROCEDURES GOVERNING COMMUNICATIONS METADATA ANALYSIS 278 (2008), https://www.dni.gov/files/documents/0909/DoD%20Supplemental%20Procedures%2020080314.pdf [https://perma.cc/6Z35-MBSG].

[16] This paper focuses on the large-scale acquisitions occurring under EO 12333 and not *individualized* and *particularized* surveillance. By *individualized* and *particularized*, this paper means acquisitions that target a discrete individual selector on a discrete personal device, such as a mobile telephone number used by an adversarial world leader.

[17] *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

[18] The Article does not delve into the potential definitional inconsistencies of certain Executive Branch documents. For instance, a valiant attempt at deciphering inconsistent terms such as collection, acquisition, and interception has already been attempted. *See generally* Diana Lee, Paulina Perlin, & Joseph Schottenfeld, *Gathering Intelligence: Drifting Meaning and the Modern Surveillance Apparatus*, 10 J. NAT'L SEC. L. & POL'Y 77 (2019).

[19] While this part focuses on the practical process of surveillance, for an in-depth look at the culture of the intelligence community through an ethnography, *see generally* Bridget Rose Nolan, Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center (2013) (Ph.D. dissertation, University

policy framework by summarizing existing congressional oversight of Executive Branch surveillance activities and the associated laws. This broader, cross-policy approach is necessary because the core surveillance authorities—Title I of the Foreign Intelligence Surveillance Act ("FISA") of 1978, Title VII's section 702 of FISA, and EO 12333—do not operate in silos. Part III outlines the origins of EO 12333. It discusses the executive order's antecedents and describes the various iterations of the executive order leading up to its present form. Part III then describes EO 12333 and its implementing procedures. Part IV explores the known electronic surveillance programs associated with EO 12333 and argues that the order's permissive targeting standards allow for large-scale acquisitions of enormous amounts of U.S. person information. Such collection is exacerbated by permissive processing methods prescribed in EO 12333's implementing procedures, originally intended to protect U.S. person privacy.[20] This Article argues that these processing procedures fail to adequately preserve U.S. person privacy in the event that U.S. person information is mistakenly collected.[21] The activities described in Part IV combine to form a complex surveillance regime that collects significant amounts of information to, from, and about U.S. persons, despite its original focus on foreign intelligence information.[22] The Article concludes by offering potential reforms for EO 12333. These include proposals to narrow the aperture of surveillance, increase privacy standards for storing information, and exert more stringent transparency and accountability requirements over EO 12333. Potential non-U.S. person reforms are beyond the scope of this paper.[23]

In short, the presidential spying occurring under EO 12333 faces little oversight by Congress and collects a tremendous amount of U.S. person information, which ends up in the NSA's—and other agencies'—databases despite EO 12333 primarily directing its surveillance outside the United States and against non-U.S. persons for foreign and counter intelligence information. This Article

---

of Pennsylvania) (ProQuest), https://repository.upenn.edu/dissertations/AAI3565195/ [https://perma.cc/SX66-M62L].

[20] *See* NAT'L SEC. AGENCY, USSID 18 LEGAL COMPLIANCE AND U.S. PERSON MINIMIZATION PROCEDURES § 6 (2011) [hereinafter USSID 18] http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf [https://perma.cc/3MSU-EAWS].

[21] The intelligence community argues USSID 18 preserves privacy because the procedures only allow analysts to intentionally target a U.S. person selector with Attorney General (AG) approval and mandate the use of generic labels to *minimize* U.S. person information, like substituting a person's name with "U.S. Person One." *See* Press Release, Office of the Director of Nat'l Intel., NSA's Activities: Valid Foreign Intelligence Targets Are the Focus (Oct. 3, 2013), https://icontherecord.tumblr.com/post/65656690222/nsas-activities-valid-foreign-intelligence [https://perma.cc/HAD7-SKRC].

[22] This Article doesn't argue that EO 12333 intentionally targets U.S. persons indiscriminately. It is well settled that EO 12333 generally targets non-U.S. persons outside the United States, and allows for certain specific targeting of U.S. persons. *See, e.g.*, DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 7:17 (2d ed. 2012).

[23] Such a topic deserves its own dedicated paper. This is especially so in light of the recent *Schrems II* decision. *See* Case C-311/18, Data Prot. Comm'r v. Facebook Ir. Ltd. and Maximillian Schrems, ECLI:EU:C:2020:559 (July 16, 2020) (striking down the EU-U.S. Privacy Shield Framework for insufficient protections of EU citizen data in personal data transfers).

explores the large-scale data acquisitions authorized by EO 12333, the explicit authorization of collecting U.S. person information, and the use of broad EO 12333 foreign intelligence selectors that inevitably collect U.S. person information. The analysis and collection of U.S. person information at such a scale and scope demands closer inspection and robust public debate.

II. Through the Looking Glass

While different legal authorities authorize different electronic surveillance programs, many of the programs share the same nomenclature and methods. This Part discusses the process of electronic surveillance in order to define key terms used throughout the paper.[24]

The first term is *electronic surveillance*. FISA, the main statute governing foreign intelligence collection, defines electronic surveillance with strict specificity to include four narrow categories.[25] This Part colloquially defines electronic surveillance as any acquisition of electronic information.[26] Often, electronic surveillance is an acquisition of information that occurs over the telecommunications infrastructure, which includes fiberoptic cables transferring internet and other communications traffic, or on or from a given device.[27]

A second term is *collection*. Documents across the intelligence community define it in different ways. The most updated documents drafted by the Department of Defense, which applies to subordinate agencies like the NSA, notes: "[i]nformation is collected when it is received . . . Collected information includes information obtained or acquired by any means."[28] The NSA's own documents mark collection as occurring when "[information] is intentionally tasked ('selected') for subsequent processing."[29] Some commenters have noted the inherent confusion in the terms; however, it is likely that the NSA's use of collection is a subset of the collection mentioned in DoD documents.[30] That is, and as described below, NSA collects data by tasking selectors that trigger the prioritization, sessionization, analysis, and eventual storage of information into NSA databases. This paper defines *collecting* colloquially, i.e., the act of bringing

---

[24] This Part is influenced by the Privacy and Civil Liberties Oversight Board's ("PCLOB") Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act. *See generally* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3. The PCLOB is an independent agency within the Executive Branch tasked "to ensure that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties." *See generally* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov [https://perma.cc/3JLG-QCNF] (last visited Oct. 23, 2020).

[25] *See* discussion *infra* Part II.A.

[26] *See* 50 U.S.C. § 1801(f) (2018).

[27] A device can be as discrete as a personal mobile phone to data centers. *Cf. id.*

[28] *See* U.S. DEP'T OF DEF., MANUAL 5240.01: PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES § G.2 (2016).

[29] *See* USSID 18, *supra* note 20, § 9.2.

[30] For a thorough parsing of the different terms, *see generally* Lee et al., *supra* note 18.

together into one body or place.[31] Collecting electronic information most often occurs when it is gathered in a searchable NSA database, but it may also occur in order when data is sessionized into information that is then prioritized and analyzed.

A. *Selectors, Tasking, and Querying*

Although EO 12333 surveillance can target U.S. persons in some circumstances, generally speaking, EO 12333 electronic surveillance programs target non-U.S. persons, governments, groups, or agents.[32] In electronic surveillance parlance, people and entities are "targeted" and "selectors" are "tasked."[33] When an NSA analyst wants to surveil a target, the analyst will "task" a surveillance system with a "selector" associated with a target.[34] Selectors include any identifier related to a target,[35] and may include phone numbers, mobile identifiers like IMEIs, unique advertising identifiers, email addresses, personal IP addresses, server IP addresses or other electronic information.[36] Selectors can also be used to search for patterns of behavior.[37]

After tasking selectors, data may be prioritized, sessionized, and eventually stored in NSA databases through a variety of authorized electronic surveillance techniques.[38] Most techniques capture a "single communication transaction," which is the collection of a discrete—single—communication to, from, or about a selector.[39] Information "about" the selector includes communication containing the selector of a targeted person, even though the information is not "to" or "from" the

---

[31] *Collecting*, *Merriam-Webster Dictionary*, https://www.merriam-webster.com/dictionary/collecting [https://perma.cc/YUZ7-WQSU] (last visited on Oct. 23, 2020).

[32] 50 U.S.C. § 1801(a)–(b) (2018). Foreign intelligence "means information relating to the capabilities, intentions and activities of foreign powers, organizations or persons, but not including counterintelligence except for information on international terrorist activities." Counterintelligence "means information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not including personnel, physical, document or communications security programs." Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

[33] Judgment of Justice Costello, *Schrems II* [2016] No. 4809 P. (Hi. Ct.) (Ir.), ¶ 182. NSA documents also define "target" to include entities. *See* NAT'L SEC. AGENCY, INSPECTOR GENERAL REPORT, UNCLASSIFIED SUMMARY: SPECIAL STUDY OF NSA CONTROLS TO COMPLY WITH SIGNALS INTELLIGENCE RETENTION REQUIREMENTS 4 (2019).

[34] *See* Judgment of Justice Costello, *supra* note 33.

[35] Web browser tags can also be used as selectors. *See* Leaked Five Eyes Document Describing *Selector Types*, THE INTERCEPT, https://theintercept.com/document/2014/03/12/selector-types/ [https://perma.cc/BLP8-2H8F] (last visited Jan. 30, 2021).

[36] *See id.*

[37] Boolean operation errors occur in various memos and intelligence oversight reviews. *See* NAT'L SEC. AGENCY, NSAW SID INTELLIGENCE OVERSIGHT (IO) QUARTERLY REPORT—FIRST QUARTER CALENDAR YEAR 2012 (1 JANUARY–31 MARCH 2012)—EXECUTIVE SUMMARY § II.b (2012), https://www.eff.org/files/2013/11/15/20130816-wapo-sid_oversight.pdf [https://perma.cc/KUL7-TTC6].

[38] *See* discussion *infra* Part I.B.

[39] *See* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 39.

target.[40] Information can also be captured as a "multiple communication transaction," or "MCT."[41] MCTs occur when the government targets a given communications traffic stream, but the communications traffic stream contains multiple communications.[42] NSA is unable to untangle the MCT into separate discrete communications and instead collects all the communications in the traffic stream.[43] Thus, NSA collects email traffic containing multiple emails in one acquisition, even though the traffic being surveilled may contain only one selector. The government acknowledges MCTs "inevitabl[y]…collect[s]" wholly domestic communications.[44]

Once in NSA databases, analysts can query collected information with a selector. *Query* is generally understood to mean the searching of information within a database by a human analyst with the intent to view the information associated with a selector.[45] Analysts routinely intercept, review, and share U.S. person information after querying NSA databases.[46]

B. *Bulk Acquisitions and Bulk Collections*

Privacy advocates, lawyers, government practitioners, and others have different names for the numerous surveillance programs exposed by Edward

---

[40] *See id.* at 7; For example, an email from a U.S. person to a person living abroad that included an email address associated with a target might be included as an "about" communication. In 2017, the NSA announced it would stop "about" collection under section 702. Charlie Savage, *NSA Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html [https://perma.cc/7MPL-JX44].

[41] *See* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 7.

[42] *See id.*

[43] *See id*.

[44] *FISA Amendments Act Reauthorization: Hearing Before the H. Select Comm. on Intel.*, 112th Cong. 7 (2011) (joint statement of Lisa O. Monaco, Assistant Att'y Gen. of the United States for Nat. Sec., John C. (Chris) Inglis, Deputy Dir. of NSA, Robert S. Litt, Gen. Counsel of ODNI); As the PCLOB noted, "If a single discrete communication within an MCT is to, from, or about a section 702 tasked selector, and at least one end of the transaction is foreign, the NSA will acquire the entire MCT." *See* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 39.

[45] *See* FISA defines "query" as "the use of one or more terms to retrieve the unminimized contents or non-contents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized" by section 702. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, §101 132 Stat. 3 (2018); The legislative history of section 702 defines "query" to refer "only to retrievals 'of or concerning United States persons,' and, therefore, the new querying procedures requirement does not apply to queries that are not specifically intended to return communications 'of or concerning United States persons.'" H.R. REP. NO. 115-475, at 18 (2017).

[46] *See* Robyn Greene, *A History of FISA Section 702 Compliance Violations*, OPEN TECHNOLOGY INSTITUTE (Sept. 28, 2017), https://www.newamerica.org/oti/blog/history-fisa-section-702-compliance-violations/ [https://perma.cc/BA6P-FZD6]; Some analysts even proactively queried and reviewed communications of their current or former spouses and lovers up until internal reforms were made by NSA. Alina Selyukh, *NSA Staff Used Spy Tools on Spouses, Ex-lovers: Watchdog*, REUTERS (Sept. 27, 2013), https://www.reuters.com/article/us-usa-surveillance-watchdog/nsa-staff-used-spy-tools-on-spouses-ex-lovers-watchdog-idUSBRE98Q14G20130927 [https://perma.cc/Z4Z3-M9NL].

Snowden. Some have labelled the entire subset of surveillance as "mass surveillance" or "bulk collection" because the information is gathered in "bulk" and then eventually collected and stored for potential review in NSA databases.[47] Others call some, but not all, of the programs "bulky collection" on the basis that some sort of discriminant was used to surveil and analyze information close to, but not entirely, in "bulk."[48] The government, under the Obama administration, defined "bulk collection" as any surveillance that does not use a discriminant, labelling all other surveillance as "targeted surveillance."[49] In contrast, the National Academy of Sciences defined "bulk collection" as a collection that results "in a database in which a significant portion of the information pertains to identifiers not relevant to current targets."[50]

Whatever the term used, "bulk collection" is only an apt name for programs similar to the now-defunct section 215 Call Detail Records Program.[51] That surveillance required telephone service providers to send the call detail records of its customers on an ongoing daily basis in 90-day intervals.[52] No discriminants, *selectors*, were used or sent to the phone companies.[53] Phone companies received an order for all daily call records for a certain period of time and then those records were sent to NSA databases.[54] After NSA stored the information in databases, NSA analysts would then "query" the phone records database with a selector reasonably suspected of being associated with a specific terrorist organization.[55]

This Article prefers the term bulk acquisition as a general term because it better describes the electronic surveillance performed by NSA. A bulk acquisition occurs when data is temporarily sessionized and analyzed at a large scale, discriminants are applied to the data stream for analysis, but the entire data stream

---

[47] *See US: End Bulk Data Collection Program*, HUMAN RIGHTS WATCH (Mar. 5, 2020), https://www.hrw.org/news/2020/03/05/us-end-bulk-data-collection-program [https://perma.cc/3NCL-LQKX]].

[48] *See* Julian Sanchez, *All the Pieces Matter: Bulk(y) Collection Under Section 702*, JUST SECURITY (July 25, 2014), https://www.justsecurity.org/13227/pieces-matter-bulky-collection-§702/ [https://perma.cc/J35Y-5EM8].

[49] *See* Press Release, Office of the Press Sec'y, The White House, Presidential Policy Directive—Signals Intelligence Activities at n.5 (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/AR3K-HMZW]; The reliance on a discriminant should not be the litmus test for whether or not a given collection is "bulk collection." A zip code can be considered a discriminant; however, New York City's 10021 has over 100,000 people in it. *See Quick Facts*, U.S. CENSUS BUREAU, https://www.census.gov/quickfacts/fact/table/US/PST045219 [https://perma.cc/38QT-W93T] (last visited on Oct. 23, 2020).

[50] According to NAS, "not relevant" includes information referring "to parties that have not been, are not now, and will not become subjects of interest." *See* NAT'L ACAD. OF SCIENCES, BULK COLLECTION OF SIGNALS INTELLIGENCE 33 (2015).

[51] *See* Greenwald, *supra* note 1.

[52] PRIV. AND C. L. OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 23 (2014).

[53] *See id.* at 22.

[54] *See id.*

[55] *See id.* at 26.

that is initially analyzed is not necessarily stored, i.e., *collected*, in databases. This is similar to the surveillance occurring under section 702 techniques like UPSTREAM, now simply called "upstream collection,"[56] or EO 12333 surveillance programs similar to UPSTREAM, in which the government compels providers controlling the telecommunications backbone to send communications and information to, from, and potentially about selectors to the NSA.[57]

C. *Incidental and Inadvertent Collection*

Bulk acquisition techniques are not exact. In addition to MCTs, overcollection occurs in a variety of ways. The most traditional way is when NSA collects a communication between a non-targeted U.S. person and a targeted non-U.S. person.[58] In such instances the non-targeted U.S. person's communication would be collected "incidental" to the intended target of the surveillance.[59] The government uses information obtained from incidental collection in intelligence analysis and criminal investigations.[60]

Incidental collection is not *inadvertent* collection, or *mistaken* collection. It occurs when an analyst reasonably believes she is targeting a non-U.S. person located abroad or when an analyst may not have enough information to confirm the selector is definitively a U.S. person.[61] In such instances, the analyst may end up targeting a U.S. person and only learns the selector belongs to a U.S. person after reviewing the collected information.

D. *Conclusion*

Understanding key terms is fundamental to understanding the electronic surveillance regime. Selectors associated with targets are tasked and surveillance systems act in different ways to collect information to, from, or about the selector.

---

[56] UPSTREAM is referred to as a "technique" and not a program or authority because it is still unclear how exactly the intelligence community refers to UPSTREAM. As of April 2017, the intelligence community, now refers to UPSTREAM as "upstream collection." *See* Press Release, Nat'l Sec. Agency, NSA Stops Certain Section 702 "Upstream" Activities, (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/#:~:text=After%20considerable%20evaluation%20of%20the,about%22%20a%20foreign%20intelligence%20target [https://perma.cc/L3VR-SDQ3].

[57] The surveillance occurring under upstream collection involves acquisitions of data transiting the telecommunications backbone without selectors, parsing the data for specific selectors, and then eventually storing a narrower—yet still large—amount of data created by the selector and (up until April 2017) "about" the selector in NSA databases. PRIV. AND C. L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2014) 35.

[58] *See* Robert Litt, Gen. Counsel of ODNI, Remarks on U.S. Intelligence Community Surveillance One Year After President Obama's Address at the Brookings Institution 17 (Feb. 4, 2015), https://www.brookings.edu/events/u-s-intelligence-community-surveillance-one-year-after-president-obamas-address/ [https://perma.cc/Q4BA-BLEF].

[59] *See id.*

[60] *See id.* at 19. NSA also forwards such information to other relevant agencies. *See id.*

[61] *See id.* at 17.

The collection occurs via bulk acquisitions and bulk collections; however, this Article refers to *bulk acquisition* instead of *bulk collection* or *bulky* collection because the latter terms are misnomers describing surveillance techniques authorized by EO 12333. Inevitably, surveillance both incidentally and inadvertently collects information that may not even be to, from, or about a selector.

III. Situating EO 12333 in the National Security Legal Framework

Executive Order 12333 organizes the intelligence community and, among other things, authorizes the Executive Branch's intelligence collection. This Part provides a foundation for understanding EO 12333's policy and legal framework by summarizing relevant statutes and other legal authorities related to EO 12333's electronic surveillance programs. It does so through an overview of the origins of U.S. national security surveillance, the history of American Executive Branch actions, and EO 12333's subsequent regulation—in part—by Congress.

Congress formally assigned intelligence collection to the Central Intelligence Agency (CIA) in 1947 after the passage of the National Security Act,[62] which unified the military establishment and created the CIA, National Security Council, and Joint Chiefs of Staff.[63] Less than ten years later, President Harry Truman created the National Security Agency via classified order, in large part because Truman recognized the need for a single entity to be responsible for the signals intelligence mission of the United States.[64] From President Truman until the 1970s, national security surveillance was largely kept secret from Congress and the public.[65]

However, the 1970s offered a decade of increased oversight of the Executive Branch's intelligence collation. An early instance of this occurred in *United States v. United States District Court for the Eastern District of Michigan*, when the Attorney General approved the surveillance of individuals in the United States that President Nixon believed were domestic national security threats.[66] The Supreme Court concluded that the government must obtain a warrant whenever it surveils individuals in the United States for any purpose, including for domestic national security purposes.[67]

Furthermore, the 1970s saw the formation of committees, in both the House and Senate, that reviewed CIA and NSA operations dating back to their inception

---

[62] *See* National Security Act of 1947, 50 U.S.C.A. § 3001 (West 1947).
[63] *See id.*
[64] *See* Memorandum from President Harry S. Truman to the Sec'y of State and the Sec'y of Def. (Oct 24, 1952) (on file with the Nat'l Sec. Agency) https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/truman/truman-memo.pdf [https://perma.cc/8G54-Y49X].
[65] Secrecy even stretched to budgets, preventing any sense of type, scale, or scope of surveillance activities. *See* S. REP. NO. 94-755 at 367 (1976).
[66] *See generally* United States v. U.S. District Court (*Keith)*, 407 U.S. 297 (1972).
[67] *Id.* at 321.

in the late 1940s and early 1950s.[68] In particular, the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known informally as the "Church Committee" after its leader Senator Frank Church, conducted one of the most thorough investigations ever into the intelligence community.[69] It produced fourteen volumes of reports detailing troubling actions from assassination attempts to the collection by the NSA of every single telegram entering and exiting the United States.[70] These congressional investigations, combined with the impact of the Keith case, culminated in passage of the Foreign Intelligence Surveillance Act of 1978.[71]

A. *The Foreign Intelligence Surveillance Act*

The Foreign Intelligence Surveillance Act of 1978 represented one of the first Congressional regulations of the President's Article II powers related to foreign intelligence collection and electronic surveillance.[72] Generally speaking, the Act provided a legal regime to surveil "agents of a foreign power" to obtain "foreign intelligence information," or information about broad national security issues depending on the location and status of the target.[73] Agents of a foreign power can be United States persons or non-United States persons acting on behalf of a foreign power or individuals threatening harm to the United States through international terrorism, espionage, or the international proliferation of weapons.[74]

Title I of FISA authorizes electronic surveillance in four scenarios: collection against radio or wire communications sent or received by a targeted U.S. person located inside the United States,[75] collection from a wire inside the United States with one end terminating in the United States,[76] collection of private

---

[68] The House of Representatives created the United States House Permanent Select Committee on Intelligence led by Otis G. Pike of New York and the Senate created the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities led by Frank Church of Idaho. *See* Thomas Young, *40 years ago, Church Committee investigated Americans spying on Americans*, BROOKINGS BLOG (May 6, 2015), https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans/ [https://perma.cc/6XH7-HLLA].

[69] *See* S. Res. 21, 94th Cong. (1975).

[70] *See* S. REP. NO. 94-755 (1976).

[71] *See* Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2014).

[72] *See* 50 U.S.C. § 1801(e). Congressional regulation of domestic electronic surveillance for national security purposes was acknowledged by the Supreme Court and the Attorney General at the time. *See* United States v. U.S. District Court (*Keith)*, 407 U.S. 297, 324 (1972).

[73] 50 U.S.C. § 1801(e).

[74] 50 U.S.C. § 1801(b).

[75] "[T]he acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(1).

[76] "[T]he acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those

domestic radio communications,[77] and the use of a device to collect information other than from a wire or radio communication in the United States for which a warrant would be otherwise required.[78] Title I of FISA also includes an "exclusive means provision" specifying that the criminal wiretap laws and FISA are the only means through which "electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted."[79]

FISA requires the Executive Branch to apply for a search warrant based on probable cause to a judge on the Foreign Intelligence Surveillance Court in order to obtain communications or conduct a physical search of an agent of a foreign power.[80] The application includes statements and affidavits by officials that there are facts and circumstances justifying the belief the target is a foreign power or an agent of a foreign power and that a significant purpose of the surveillance is to obtain foreign intelligence information.[81] The court proceedings are classified and ex parte, and the court approves, denies, or modifies the application.[82] Congress has increasingly regulated Executive Branch national security surveillance through various amendments to FISA.[83] These amendments added two key sections for purposes of this Article in the aftermath of the September 11th attacks: section 215 of the PATRIOT Act, which was incorporated into FISA in section 501, and the FISA Amendments Act, which was incorporated as Title VII of FISA; the most notorious of which is section 702.[84]

---

communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18." 50 U.S.C. § 1801(f)(2).

[77] "[T]he intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States." 50 U.S.C. § 1801(f)(3).

[78] "[T]he installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f)(4).

[79] 50 U.S.C. § 1812 (2018).

[80] *See* 50 U.S.C. § 1804 (2018).

[81] The application must include a statement of facts justifying the officer's belief the target is an agent of a foreign power, a statement that the facilities targeted is used or about to be used by the target, a statement of the proposed minimization procedures, a description of the information sought, a certification the information is foreign intelligence information, that a significant purpose is to obtain foreign intelligence, a statement that the information can't be obtained through normal investigative techniques, and a statement describing when the surveillance will occur. 50 U.S.C. § 1804.

[82] *See* 50 U.S.C. §§ 1803–1805.

[83] *See* FISA Reauthorization Act of 2012, Pub. L. No. 112-238 (2012); FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118 (2018); Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261 (2008); USA FREEDOM Act of 2015, Pub. L. No. 114-23 (2015). The physical search provisions of FISA were added as Title III of that Act by the Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359 (1994).

[84] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261; FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118; USA FREEDOM Act, Pub. L. No. 114-23; The former is codified in FISA as 50 U.S.C. § 1861, while the latter is codified in FISA as 50 U.S.C. § 1881(a); *see* BRENNAN CTR. FOR JUST., ARE THEY ALLOWED TO DO THAT? A

Section 215 added a subpoena-esque power to the Executive Branch by authorizing it to collect records or any other "tangible things" if they are relevant to international terrorism, counterespionage, or a foreign intelligence investigation.[85] As noted above, this section was also used for the now-defunct program collecting Americans' calling records.[86]

Under section 702 of FISA, the Attorney General and the Director of National Intelligence are permitted to file annual certifications with the FISA court to target "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[87] The certifications attest that a significant purpose of the acquisition is to obtain foreign intelligence information and are accompanied by targeting procedures, minimization procedures, and query procedures submitted for approval to the FISA court.[88] Along with specific procedures, the FISA court reviews the certifications no later than 30 days after the procedures and guidelines are submitted.[89] The court approves the procedures so long as they comport with the statute and do not violate the Fourth Amendment.[90] After a certification and its associated procedures are approved by the FISA court, intelligence analysts are free to initiate the section 702 surveillance process.[91]

There are two types of collection. The first is called "downstream" collection, as used in PRISM, in which NSA receives communications *to* or *from* a section 702 selector after sending an order to a telecommunications or information

---

BREAKDOWN OF SELECTED GOVERNMENT SURVEILLANCE PROGRAMS 1 n.1, https://www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf [https://perma.cc/3VTJ-48HG].

[85] *See* 50 U.S.C. § 1861 (2018).

[86] *See* supra Part I.

[87] 50 U.S.C. § 1881(a) (2018).

[88] *See* 50 U.S.C. § 1881a(h).

[89] *See* 50 U.S.C. § 1881a(j)(1).

[90] *See* 50 U.S.C. § 1881a(j)(2)–(3); Procedures include targeting procedures, minimization procedures, and query procedures. The targeting procedures describe how the government ensures the targets are non-U.S. persons outside the United States who will collect communications containing foreign intelligence and also describe to the court how the government intends to prevent the collection of purely domestic communications. 50 U.S.C. § 1881a(d); The minimization procedures describe how the government intends to minimize acquisition and interception and prohibit dissemination of unnecessary or irrelevant information (non-foreign intelligence information) and U.S. person information. The minimization procedures still allow for the retention of unanalyzed data. U.S. DEP'T OF JUSTICE, 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 3–4 (2007) [hereinafter NSA Minimization Procedures]; The query procedures detail how U.S. person information collected under section 702 is searched in NSA or other intelligence community databases. 50 U.S.C. § 1881a(f)(1).

[91] *See* 50 U.S.C. § 1881a(a). For more details, see also NAT'L SEC. AGENCY, CRSK1304, LESSON 3: HOW DO I CREATE A FOREIGNNESS EXPLANATION, https://www.aclu.org/sites/default/files/field_document/FAA702PracticalApplications000917-001000.pdf [https://perma.cc/42VU-8GMK].

services provider, like Google.[92] As discussed above, the second is called "upstream" collection, also known as UPSTREAM.[93]

Understanding section 702 is critical to understanding the surveillance occurring under EO 12333 because they authorize similar surveillance techniques.

B. *Congressional Regulation Through Appropriation*

Congress has also regulated Executive Branch activities through appropriations. Section 309 of the Intelligence Authorization Act for Fiscal Year 2015 imposes minimization procedures similar to the ones used for section 702 of FISA on all EO 12333-acquired information.[94] The section requires any incidentally collected communications be deleted after five years unless they meet a number of exceptions.[95] Exceptions relating to encryption are quite broad, allowing for any encrypted communications to be retained forever until the communication is decrypted.[96] Other exceptions include whether the communication contains any evidence of a crime, whether it contains foreign intelligence, or whether the communication is necessary for "technical assurance or compliance purposes."[97] Section 309 also mandates that the heads of each intelligence community agency develop procedures, in compliance with the new data retention requirements established by section 309.[98]

Section 309 is significant in that Congress signaled it can and will regulate EO 12333 programs, albeit narrowly. Some critics voted against the provision on the basis that it represented Congress affirmatively authorizing U.S. person collection and sharing under EO 12333.[99] A spokesperson for Senator Ron Wyden, who supported the bill, noted the provision fell short of placing any "meaningful new restrictions" on the NSA.[100] However, others, like the former chairman of the

---

[92] *See* Robert O'Harrow Jr., Ellen Nakashima, & Barton Gellman, *U.S., Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data*, WASH. POST. (Jun. 8, 2013), https://www.washingtonpost.com/world/national-security/us-company-officials-internet-surveillance-does-not-indiscriminately-mine-data/2013/06/08/5b3bb234-d07d-11e2-9f1a-1a7cdee20287_story.html [https://perma.cc/JP4J-EG8T]. *See generally* NAT'L SEC. AGENCY, PRISM TASKING PROCESS, https://www.eff.org/files/2013/11/15/20130629-wapo-prism.pdf [https://perma.cc/5Y7L-N2LU].

[93] Press Release, Nat'l Sec. Agency, NSA Stops Certain Section 702 "Upstream" Activities, (Apr. 28, 2017), https://perma.cc/5R9C-BD5B. *See supra* Part I.B.

[94] *See* Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293 (2014).

[95] *See id.* § 309(b)(3)(B).

[96] *See id.* § 309(b)(3)(B)(iii).

[97] *See id.* § 309(b)(3)(B).

[98] *See id.*

[99] *See* Julian Hattem, *GOP Rep Attempted Late Bid to Kill Spy Bill*, THE HILL (Dec. 11, 2014), https://thehill.com/policy/technology/226752-gop-rep-attempted-late-bid-to-kill-spy-bill [https://perma.cc/K4GA-Z9SD].

[100] *See* Ellen Nakashima, *Congress Sets Limits on Overseas Data Collection*, WASH. POST (Dec. 17, 2014), https://www.washingtonpost.com/world/national-security/congress-sets-limits-on-overseas-data-collection/2014/12/17/82972c6e-8558-11e4-a702-fa31ff4ae98e_story.html [https://perma.cc/3JPU-UPWR].

Privacy and Civil Liberties Oversight Board, noted that section 309 was "an important statement by Congress that it has the authority and is willing to step in and legislate in a realm that has largely been governed by the Executive Branch."[101]

C. *Conclusion*

Congress has made incremental steps towards authorizing and regulating Executive Branch foreign intelligence activities. Often, these steps have been narrow, but they are undoubtedly a signal that Congress does have the authority to regulate some aspects of Executive Branch spying. Amendments to FISA have displaced some aspects of section 2.5 of EO 12333 and unilateral spying programs by the president, like President Bush's post-September 11, 2001 STELLARWIND program, and placed these elements within the ambit of a statutory regime.[102] At the same time, that statutory regime has given tremendous discretion to the Executive Branch.[103] Similarly, the mandate of minimization procedures in the Intelligence Authorization Act of 2015 can be read in two different ways. In one sense, Congress did exert authority to regulate EO 12333 activities, but it did so narrowly.

IV. Executive Order 12333

President Ronald Reagan issued EO 12333 in 1981, but the order traces its history to previous executive orders by Presidents Gerald Ford and Jimmy Carter.[104] EO 12333 is the primary authority for the majority of the NSA's signals intelligence collection.[105] It primarily focuses on providing surveillance authority for collecting information on non-U.S. persons outside the United States. [106] However, it also provides authority for other types of surveillance so long as the surveillance does not fall under FISA.[107] This is significant because FISA only covers a specific subset of electronic surveillance.[108] This Part discusses the

---

[101] *See id.*

[102] *See* INSPECTORS GEN. REPORT, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 30–31 (2009); The publicly disclosed program called the Terrorist Surveillance Program intercepted the content of certain international communications. The NSA assigned the cover term STELLARWIND to its activities as part of this program. *See also* James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html [https://perma.cc/5DR2-NEQH].

[103] *See* INSPECTORS GEN. REPORT, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 31 (2009).

[104] *See* NAT'L SEC. AGENCY, *supra* note 4.

[105] *See id.*

[106] *See* Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM. & TECH. L. REV. 317, 321 (2015)

[107] *See id.* at 321. *See generally* Amos Toh, Faiza Patel, & Elizabeth Goitein, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD (2016), https://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf [https://perma.cc/QJM8-TU5W].

[108] *See supra* Part II.A.

executive order's antecedents and describes the various iterations of the executive order until its final form in 2008. It then describes EO 12333 as it exists today, including its broad guidelines and principles, before introducing the procedures implementing EO 12333's electronic surveillance drafted by the Department of Defense and the NSA.

A. *The Origins of EO 12333*

In 1976, President Ford issued Executive Order 11,905 ("EO 11905"), titled "United States Foreign Intelligence Activities."[109] Written in the wake of the Church and Pike Committees' revelations about intelligence abuses, the order placed restrictions on intelligence activities, including formally barring the U.S. government from engaging in political assassinations.[110] EO 11905 also established Executive Branch oversight of the intelligence community by describing the roles and responsibilities of intelligence community agencies, providing guidelines for foreign intelligence collection, creating the Intelligence Oversight Board, and directing semi-annual reviews of the intelligence community.[111]

Two years later, President Jimmy Carter replaced EO 11905 with his own order, Executive Order 12,036 ("EO 12036").[112] EO 12036 further delineated the responsibilities of the intelligence community agencies and provided new oversight of the intelligence community.[113] It established additional Executive Branch coordinating and oversight committees, introduced restrictions on intelligence community contracting and covert diplomatic activity, specifically mandated compliance with congressional oversight, and incorporated the FBI's counterintelligence activities under the purview of the executive order.[114]

Ford and Carter's executive orders provided the foundation for President Ronald Reagan's Executive Order 12,333 ("EO 12333"). Using EO 12036 as a framework, President Reagan elaborated on the roles and responsibilities of the intelligence community, clarified what information could be collected, and detailed the scope of the Foreign Intelligence Surveillance Act.[115] EO 12333 also rolled back some of the more restrictive oversight language regarding reporting requirements laid out in EO 12036.[116]

---

[109] *See* Exec. Order No. 11,905, 3 C.F.R. 90 (1977).
[110] *See id.* § 3. The Executive Order accomplished this through the National Security Council, Committee on Foreign Intelligence, and "Operations Advisory Group." It also placed the CIA Director in charge of all intelligence components and created a Presidential Intelligence Oversight Board.
[111] *See id.*
[112] *See* Exec. Order 12,036, 50 Fed. Reg. 3,073 (Jan. 23, 1978).
[113] *See id.*
[114] *See id.* §§ 2–3. For example, it listed members of a Special Coordination Committee at the National Security Council who would approve special covert activities.
[115] *See* Exec. Order No. 12,333, 45 Fed. Reg. 59,941 (1981).
[116] *See id.*

EO 12333, as issued by President Reagan, remains largely intact today. President George W. Bush made minor changes to the order as result of the Intelligence Reform and Terrorism Prevention Act of 2004 ("IRTPA").[117] IRTPA established an Office of the Director of National Intelligence to be led by a Director of National Intelligence (DNI).[118] Under IRTPA, the DNI serves as the head of the intelligence community and the principal adviser to the President, National Security Council, and Homeland Security Council on national security matters.[119] The updated order acknowledged these changes by replacing the CIA Director with the Director of National Intelligence as the head of the intelligence community.[120] President Bush's revisions also clarified the role of the FBI—and other domestic law enforcement—to emphasize the close relationship and necessary information sharing between law enforcement and the intelligence community.[121]

Executive Order 12333 continues to be the core document governing Executive Branch surveillance by the intelligence community. While amended by President Bush, the document has continued to generally describe the roles and responsibilities of Executive Branch intelligence components, authorized some of these components to collect foreign intelligence, and exerted Executive Branch oversight over the intelligence community.

B. *EO 12333 Section-by-Section*

In broad strokes, EO 12333 provides both authorizations for and restrictions on intelligence collection. EO 12333 specifies certain signals intelligence activities may be conducted only pursuant to procedures approved by the Attorney General or a designated executive agency.[122] Attorney General approval is required for: the clandestine collection of foreign intelligence inside the United States;[123] intelligence collection, retention, and dissemination concerning U.S. persons;[124] intelligence collection within the U.S. or directed against U.S. persons abroad;[125] determinations on how information is provided to or accessed by the intelligence community;[126] and, decisions regarding how signals intelligence is disseminated.[127] Attorney General approval is not required for procedures or policies regulating signals intelligence targeting non-U.S. persons or non-U.S. targets outside the United States.[128] Attorney General approval is also not required for collection outside the bounds of FISA, such as when a collection site is not in the United

---

[117] *See* 50 U.S.C. § 3002 (2018).
[118] *See id.*
[119] *See* 50 U.S.C. § 3021 (2018).
[120] *See* Exec. Order No. 12,333, 45 Fed. Reg. 59,941 (1981), *reprinted as amended in* 73 Fed. Reg. 45,325 (2008).
[121] *See id.* at § 1.1(f).
[122] *See id.* § 1.9(d) and 2.3.
[123] *See id.*
[124] *See id.* § 2.3.
[125] *Id.* § 2.4.
[126] *Id.* § 3.2.
[127] *Cf.* § 2.5 (identifying when Attorney General Approval is needed).
[128] *See id.*

States.[129] This Section will primarily focus on the role EO 12333 assigns to the NSA as the agency with the sole authority to engage in signals intelligence.[130]

EO 12333 section 1 covers the roles of the individual components of the intelligence community.[131] Section 1.7(c) tasks the NSA with its primary signals intelligence mission.[132] Under this section, the Director of NSA shall: "Collect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign intelligence and counterintelligence purposes to support national and departmental missions."[133] The Director is also ordered to "control signals intelligence collection and processing activities, including assignment of resources to an appropriate agent for such periods and tasks as required for the direct support of military commanders."[134]

EO 12333 section 2 regulates the conduct of intelligence activities, outlines the scope of intelligence, and provides certain restrictions on intelligence components.[135] It broadly establishes what information intelligence agencies can collect, retain, and share.[136] EO 12333 section 2.3 authorizes only the collection, retention, and dissemination of certain information concerning U.S. persons pursuant to Attorney General-approved procedures.[137] This information includes any information that is available to the public;[138] about employees;[139] used to determine the credibility of potential intelligence sources;[140] necessary for administrative purposes;[141] concerns security investigations of personnel;[142] acquired by overhead reconnaissance not directed at specific United States

---

[129] *See id.* By policy, the U.S. person rules are followed when the target is not a "second party citizen" or located inside of a "second party" territory, like Australia, Canada, New Zealand, and Great Britain. *SIGINT Authority Decision Tree*, *supra* note 8; NAT'L SEC. AGENCY, OVSC1100, LESSON 3—ADDITIONAL AUTHORITIES 11 (2007), https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf [https://perma.cc/2KSD-5S3M].

[130] As such, this document does not discuss Section 2.5 of EO 12333 at length because it is likely used by the FBI in national security investigations. Section 2.5 authorizes the Attorney General to approve intelligence collection within the United States or against a United States person abroad. *See* Exec. Order No. 12,333 §1, 46 Fed. Reg. 59,941 (1981); DAVID S. KRIS & J. DOUGLAS WILSON, *supra* note 22, § 17:18 (2d ed. 2012); FBI, FBI DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE, https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20%28DIOG%29 [https://perma.cc/KX8V-698S].

[131] Exec. Order No. 12,333 §1, 46 Fed. Reg. 59,941 (1981).

[132] *Id.* § 1.7(c).

[133] *Id.* § 1.7(c)(1).

[134] *Id.* § 1.7(c)(3).

[135] *Id.* § 2.3.

[136] *Id.*

[137] *Id.*

[138] *Id.* § 2.3(a).

[139] *Id.* § 2.3(e).

[140] *Id.* § 2.3(f).

[141] *Id.* § 2.3(j).

[142] *Id.* § 2.3(g).

persons;[143] incidentally collected about a criminal violation;[144] or that constitutes foreign intelligence information obtained in the course of a lawful foreign intelligence, counterintelligence, or international drug or terrorism investigation.[145]

Section 2.4, "Collection Techniques," requires agencies to use the least intrusive means possible for collection within the U.S. or directed against U.S. persons abroad.[146] Electronic surveillance, physical surveillance, physical searches, and mail surveillance are authorized inside the U.S. or directed against U.S. persons abroad only in accordance with Attorney General-approved guidelines.[147]

Section 2.5 separately authorizes the Attorney General to approve surveillance within the United States or against a U.S. person abroad using any technique for which a warrant would be required if it was undertaken by law enforcement.[148] Since electronic surveillance must be conducted in accordance with FISA and EO 12333, FISA amendments have substantially limited the Attorney General's power under Section 2.5 by demanding a court order for most collection in the U.S. targeting a U.S. person.[149] Thus, generally, in order to approve surveillance without a warrant, the Attorney General must determine there is probable cause to believe the surveillance is directed against a foreign power or an agent of a foreign power and the purpose is to acquire significant foreign intelligence information.[150] However, the amendments have not completely undone section 2.5. EO 12333 and its implementing procedures govern all surveillance outside the contours of FISA.[151] A still classified legal memo describes such collection; however, the public can only guess as to what that surveillance is, by identifying the gaps in current surveillance law.[152]

Section 2.6 directs the Attorney General to approve procedures governing when intelligence components can assist law enforcement.[153] The section

---

[143] *Id.* § 2.3(h).
[144] *Id.* § 2.3(i).
[145] *Id.* § 2.3(c).
[146] *Id.* § 2.4.
[147] *Id.*
[148] *Id.* § 2.5.
[149] *See* USSID 18, *supra* note 20, § 4.1(a).
[150] *See id.* § 4.1(b)(1)-(3) (2011). As noted below, "significant foreign intelligence information" is defined in a circular manner; *Infra* Part IV.B.
[151] Exec. Order No. 12,333 §2.5, 46 Fed. Reg. 59,941 (1981).
[152] *See* Memorandum for the Attorney General from Theodore B. Olson, Assistant Attorney General, Office of Legal Counsel, *Re: Constitutionality of Certain National Security Agency Electronic Surveillance Activities Not Covered Under the Foreign Intelligence Surveillance Act of 1978* at 59 (May 24, 1984), *quoted in* Memorandum for the Attorney General from Kenneth L. Wainstein, Assistant Attorney General, National Security Division, Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States, 4 n.4 (Nov. 20, 2007), https://www.aclu.org/other/nsa-memo-dod-proposed-amendment-conduct-analysis-metadata [https://perma.cc/AP8Z-US28]; Jonathan Mayer, *Executive Order 12333 on American Soil, and Other Tales from the FISA Frontier*, WEB POLICY (Dec. 3, 2014), http://webpolicy.org/2014/12/03/eo-12333-on-american-soil/ [https://perma.cc/9BL8-BB4C].
[153] *See* Exec. Order No. 12,333 §2.6, 46 Fed. Reg. 59,941 (1981).

authorizes intelligence components to "[p]rovide specialized equipment, technical knowledge, or assistance" to support law enforcement.[154]

Section 3.5 of EO 12333 defines key terms. EO 12333 uses a definition of "[a]gent of a foreign power" similar to the one used in FISA, but broadens the definition of "foreign intelligence,"[155] to "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."[156] The EO 12333 definition for "electronic surveillance" is also broader than the one used in FISA.[157] For all purposes other than electronic surveillance conducted under FISA,[158] "electronic surveillance" is defined in EO 12333 as the "acquisition of a nonpublic communication by electronic means without the consent of a person who is a party" to the communications.[159]

EO 12333 tasks the NSA with overseeing signals intelligence collection and sections 2.3, 2.4, and 2.5 make up the bulk of EO 12333's signals intelligence provisions. These provisions make broad grants of authority to the intelligence community to conduct foreign intelligence collection, but also mandate the intelligence community flesh out the authorization in EO 12333, by creating Attorney General-approved guidelines in section 2.3, section 2.4, and section 2.5.[160] This includes directing the cabinet-level department, the Department of Defense, and its units, the NSA, to draft relevant policies and procedures implementing EO 12333.[161] EO 12333 also directs agencies responsible for signals intelligence to draft Attorney General-approved guidelines in certain instances of signals intelligence.[162] These two sections are implemented in the policies and procedures described below.

C. *EO 12333's Implementation*

NSA's electronic surveillance under EO 12333 is implemented by four key documents. The first is "Department of Defense Manual 5240.01: Procedures Governing the Conduct of DoD Intelligence Activities" ("DoD 5240.01").[163] DoD 5240.01 contains ten procedures and a classified annex authorizing the collection

---

[154] *Id.* § 2.6(c).
[155] *Id.* § 3.5(e).
[156] *Id.*
[157] *Id.* § 3.5(c).
[158] In FISA, surveillance of communications occurs in four specific categories. *See* 50 U.S.C § 1801(f)(1)–(4); *supra* Part II.A.
[159] *See* Exec. Order No. 12,333 §3.5(c), 46 Fed. Reg. 59,941 (1981).
[160] *See id.* §§ 2.3, 2.4, 2.5.
[161] *See id.*
[162] *See id.* § 2.3.
[163] U.S. DEP'T OF DEF., MANUAL 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES (2016). Previous to 2016, the document was titled DoD Regulation 5240.1-R: Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons. *See* U.S. DEP'T OF DEF, DIR. 5240.1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (1982).

of information, defining the categories of collection, and specifying how DoD components must handle U.S. person information.[164] DoD 5240.01 authorizes electronic surveillance, unconsented physical searches, mail surveillance, physical surveillance, or monitoring devices not barred by the section.[165] DoD 5240.01 also directs subordinate units, including the NSA, to create further procedures.[166]

NSA has drafted three additional documents to implement DoD 5240.01. The first is National Security Agency/Central Security Service Policy 1-23 ("NSA/CSS Policy 1-23"), which assigns duties and responsibilities within NSA and its related signals intelligence departments.[167] The second is the Classified Annex Authority to DoD 5240.01.[168] The Classified Annex to DoD 5240.01 first appeared publicly in an annex to DoD Regulation 5240.01-R (the predecessor to DoD 5240.01); however, more recent declassifications released the document as an annex to NSA/CSS Policy 1-23.[169] The Classified Annex Authority implements Executive Order Section 2.3, Section 2.4, Section 2.6(c), and Procedure 5 of DoD 5240.01.[170] The Classified Annex Authority, in part, authorizes signals intelligence involving communications for "receipt" in the United States and activities intentionally directed against the communications of a U.S. person outside the U.S.[171] The third, which incorporates and expands on the Classified Annex Authority, is titled "USSID 18: Legal Compliance and U.S. Persons Minimization Procedures" ("USSID 18") and serves as the NSA's overarching legal and minimization procedures for signals intelligence directed at or concerning U.S. persons.[172] It incorporates all regulations and procedures for the collection,

---

[164] *See* U.S. DEP'T OF DEF. MANUAL 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES.

[165] *See id.*

[166] *See id.*

[167] *See* NAT'L SEC. AGENCY, NSA/CSS POLICY 1-23: PROCEDURES GOVERNING NSA/CSS ACTIVITIES THAT AFFECT U.S. PERSONS (Mar. 11, 2014).

[168] U.S. DEP'T OF DEF., DIR. 5240.1-R, CLASSIFIED ANNEX TO PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (1988), https://www.dni.gov/files/documents/0909/DoD%20Procedures%20Classified%20Annex.pdf [https://perma.cc/3JUA-WWGL]. For the more recent declassification, *see* OFFICE OF THE DIRECTOR OF NAT'L INTEL., CLASSIFIED ANNEX TO DEPARTMENT OF DEFENSE PROCEDURES UNDER EXECUTIVE ORDER 12333 at 118 (2017), https://www.dni.gov/files/documents/1118/CLEANED022.%20NSA%20Core%20Intelligence%20Oversight%20Training.pdf [https://perma.cc/344A-JXSN].

[169] *See* U.S. DEP'T OF DEF. *supra* note 168. For the more recent declassification, OFFICE OF THE DIRECTOR OF NAT'L INTEL. *supra* note 168, at 118.

[170] *See* U.S. DEP'T OF DEF. *supra* note 168, §1. Prohibitions include the CIA's inability to engage in electronic surveillance within the United States except for the purpose of training, testing, or conducting countermeasures to hostile electronic surveillance, unconsented physical searches in the United States by elements of the intelligence community other than the FBI with certain exceptions, and physical surveillance of a United States person in the United States by elements of the intelligence community other than the FBI with certain exceptions. *See also* Exec. Order No. 12,333 §2.4, 46 Fed. Reg. 59,941 (1981); U.S. DEP'T OF DEF. MANUAL 5240.01, PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES § 3.5.

[171] *See* U.S. DEP'T OF DEF. *supra* note 168, §1.

[172] *See generally* USSID 18, *supra* note 20; NAT'L SEC. AGENCY, OVSC1100, LESSON 2—CONVENTIONAL COLLECTION, *supra* note 8, at 5.

retention, processing, and dissemination of U.S. person information. [173] It also includes non-U.S. person information procedures[174]. NSA views the document as a core protection against collection of U.S. persons' communications.[175]

More recently the Obama Administration drafted additional requirements in a directive titled Presidential Policy Directive 28 ("PPD-28") that applies on top of all of the above documents.[176] It "articulates principles to guide why, whether, when, and how the United States conducts signals intelligence activities for authorized foreign intelligence and counterintelligence purposes," but does not amend the text of EO 12333.[177] PPD-28 lays out specific requirements for collection and grants privacy rights to non-U.S. persons.[178] Much of the document reiterates and codifies current signals intelligence policy and procedures.[179]

D. *Conclusion*

Conceptually the policy guidelines implementing EO 12333 are voluminous and sometimes overlapping. DoD 5240.01, a 2016 update on the 1988 DoD 5240.01-R, is the main cabinet-level EO 12333 policy for the Department of Defense. NSA/CSS Policy 1-23 assigns roles and responsibilities to the NSA departments and leaders engaged in signals intelligence. The Classified Annex Authority is the primary document authorizing the collection of U.S. person

---

[173] *See* USSID 18, *supra* note 20, §§4–7.
[174] *See id.* app. 1, §§ 6–7.
[175] NAT'L SEC. AGENCY, *supra* note 4. The same fact sheet notes: "[The Department of Justice] concluded that the incidental collection and processing of United States person communications, when controlled by the minimization procedures…satisfy the constitutional standard of reasonableness." *Id.* at 4.
[176] Office of the Press Sec'y, *Presidential Policy Directive—Signals Intelligence Activities*, Policy Direction/PPD-28, WHITE HOUSE (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/L8HH-AS4W].
[177] *Id*; Conceptually, PPD-28's policies are applied to all signals intelligence, including EO 12333's signals intelligence collection, in tandem with all relevant EO 12333 procedures. Much of the document reiterated and codified current signals intelligence policy and procedures. For instance, it prohibits collecting signals intelligence for the purpose of suppressing dissent. *See* PPD-28 at § 1(b); It also limits all signals intelligence collection to a foreign intelligence or counter intelligence purposes. *Id*.; Both requirements were already imposed on the intelligence community. Benjamin Wittes, *The President's Speech and PPD-28: A Guide for the Perplexed*, LAWFARE (Jan. 20, 2014), https://www.lawfareblog.com/presidents-speech-and-ppd-28-guide-perplexed [https://perma.cc/R8XM-TMMY]; It acknowledges relevant statutes, codifies the U.S. prohibition on economic espionage, and reiterates signals intelligence should be as "tailored as feasible." Office of the Press Sec'y *supra* note 176; The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the United States or its partners and allies. It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially. PPD-28 narrows the definition of foreign intelligence information. The definition theoretically supersedes all other definition in use by NSA. Foreign intelligence information is limited to "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists." *Id.* at n.2.
[178] *See* Wittes, *supra* note 177.
[179] *See id.*

communications outside the U.S. and any communication received in the United States that is not covered by FISA. USSID 18 incorporates and expands, and in some instances duplicates, the authorizations in the Classified Annex Authority, while also providing protections to U.S. person information.

V. Permissive Targeting Standards, Bulk Acquisition Programs, and Permissive Processing Procedures

This Part synthesizes the various declassifications, disclosures, legislative investigations, and news reports about EO 12333 to show how permissive targeting standards allow for bulk acquisitions that analyze and collect U.S. person information. This electronic surveillance includes the installation of malware; the analysis of internet traffic traversing the telecommunications backbone; the hacking of U.S.-based companies like Yahoo and Google; and, the analysis of Americans' communications, contact lists, text messages, geolocation, and other information. The collection of U.S. person information is exacerbated by permissive processing procedures that facilitate further analysis, human review, and sharing of U.S. person information despite EO 12333 being primarily intended to collect foreign information outside the United States from foreign targets.

Generally, analysts must have only a reasonable belief that the selector is related to a non-U.S. person outside the United States and that the collection will obtain foreign intelligence information to legally initiate an acquisition or search.[180] However, it is unclear how the reasonable belief analysis is conducted in practice. Documents show analysts can use selectors that may collect foreign intelligence information.[181] In other contexts—like at the FBI—a similar requirement was routinely violated.[182] The end result is that a legal authority solely overseen by the Executive Branch and intended to primarily collect foreign intelligence information from non-U.S. persons in reality collects significant amounts of U.S. person information.[183]

After discussing the permissive targeting standards, this Part describes how the targeting standards facilitate the collection of U.S. person information. One program of EO 12333 surveillance analyzes all phone calls and metadata exiting a country.[184] A second program includes surveillance similar to section 702's

---

[180] *See* NAT'L SEC. AGENCY, *supra* note 4.

[181] *Id.* Other requirements also exist, but it is also unclear how they are effectively performed or implemented. *See infra* Part V.D.

[182] *See* Memorandum Opinion, [Caption Redacted], [Docket No. Redacted], at 65–66 (FISA Ct. Dec. 6, 2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf [https://perma.cc/WH3J-J6QM].

[183] *See* ACLU, ACLU COMMENTS TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD ON ITS REVIEW OF EXECUTIVE ORDER 12333 at 11, 16 (Jan. 13, 2016), https://www.aclu.org/sites/default/files/field_document/aclu_comments_to_pclob_on_eo_12333_0.pdf [https://perma.cc/XLR7-NK64].

[184] *See* Ryan Devereaux, Glenn Greenwald, & Laura Poitras, *The NSA is Recording Every Cell Phone Call in The Bahamas*, THE INTERCEPT (May 19, 2014),

upstream collection.[185] A third program, called XKEYSCORE, collects information from multiple sources and is a "front end search engine" for intelligence analysts.[186] However, unlike a traditional search engine, XKEYSCORE can also send commands to servers connected to the global telecommunications backbone to prioritize, analyze, and store information into NSA databases as certain data transits the backbone.[187]

The problems associated with broad collection of information authorized by the permissive targeting standards are exacerbated by permissive processing procedures of the collected data. The permissive processing procedures, detailed in a document called United States Signals Intelligence Directive 18 ("USSID 18"), are intended to minimize the privacy intrusion on already-collected U.S. person information.[188] However, they perform the exact opposite goal by allowing for extensive retention and sharing of U.S. person information.[189] Although some safeguards exist, like a prohibition on intentionally using known U.S. person selectors unless approved by specific procedures.[190] If there is any doubt as to whether a selector is foreign or related to a U.S. person, it is assumed to be foreign.[191] Further, processing procedures also allow for exceptions to retrieve, store, and share known U.S. person information and unevaluated U.S. person information.[192] Broad exceptions also bypass procedures that require destroying communications when all known individuals are U.S. persons.[193] Combined, the permissive targeting standards, bulk acquisitions, and permissive processing procedures provide for the analysis, collection, and storage of an extraordinary amount of U.S. person information.

---

https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/ [https://perma.cc/GC92-E5DG].

[185] *See supra* Part I.A.

[186] *See* Interview with Edward Snowden, NORDDEUTSCHER RUNDFUNK (Jan. 28, 2014), https://web.archive.org/web/20180327212811/https://www.ndr.de/nachrichten/netzwelt/snowden277_page-3.html [https://perma.cc/6P9K-QWMJ]; *see also* Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, THE GUARDIAN (Jul. 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [https://perma.cc/4GM6-UQ68].

[187] *See* Interview with Edward Snowden, NORDDEUTSCHER RUNDFUNK (Jan. 28, 2014), https://web.archive.org/web/20160426181503/https://www.ndr.de/nachrichten/netzwelt/snowden277_page-3.html [https://perma.cc/9X42-CQ6V]; *see also* Greenwald, *supra* note 186.

[188] *See* USSID 18, *supra* note 20. USSID 18 was issued in 1993 and a 2011 version of USSID 18 was declassified in 2017.

[189] *Id.*

[190] *Id.* § 9.18(e). While most of the EO 12333 U.S. person targeting is now covered by FISA, there are still EO 12333 authorizations to collect U.S. person information. *See* OFFICE OF THE DIRECTOR OF NAT'L INTEL., *supra* note 168.

[191] *Id.*

[192] USSID 18, *supra* note 20, § 5.

[193] *Id.* § 5.4(d).

A. *Permissive Targeting Standards*

The NSA obtains the majority of its signals intelligence through EO 12333 surveillance, in part due to permissive targeting standards.[194] Few restrictions are placed on EO 12333 acquisitions: analysts must only conclude a selector is reasonably likely to be outside the United States and will likely possess foreign intelligence information.[195] If any doubt exists as to their nationality, selectors are presumed to be foreign.[196] In addition, U.S. persons may be intentionally targeted under specific provisions of USSID 18, which incorporates section 2.5 of EO 12333.[197]

The first requirement of the permissive targeting standards is a "foreignness determination," in which an analyst must reasonably believe the selector is related to a non-U.S. person outside the United States.[198] A "reasonable belief" is undefined in USSID 18, but a selector is presumed foreign so long as an analyst does not definitively know the selector is related to a U.S. person.[199] Although the factors underpinning a foreignness assessment are classified, leaked documents on foreignness factors include when the person has stated she is located outside the United States or if a human intelligence source knows the person is outside the United States.[200] However, other disclosed foreignness factors are far broader and lead to permissive targeting that collects an enormous amount of U.S. person information.[201] These include factors that do not

---

[194] NAT'L SEC. AGENCY, *supra* note 4.

[195] Guidelines on collecting communications of non-U.S. persons outside the United States are relatively recent additions and are provided in a document detailing supplemental procedures. *See* NAT'L SEC. AGENCY, USSID 18 SUPPLEMENTAL PROCEDURES FOR THE COLLECTION, PROCESSING, RETENTION, AND DISSEMINATION OF SIGNALS INTELLIGENCE INFORMATION AND DATA CONTAINING PERSONAL INFORMATION OF NON-UNITED STATES PERSONS § 4.1 (2015), https://www.nsa.gov/Portals/70/documents/news-features/declassified-documents/nsa-css-policies/PPD-28.pdf [https://perma.cc/P8TY-K5RF] [hereinafter USSID 18 Non-U.S. Persons Supplemental]. Collection is authorized for any signals intelligence activities taken in response to foreign intelligence requirements. *Id.* Collection must occur with selectors and are used in conjunction with USSID 18 for EO 12333-collected information. *Id.* § 4.2.

[196] USSID 18, *supra* note 20, § 9.18(e).

[197] *Id*., § 4.1.

[198] The exact EO 12333 standards are classified; however, under section 702, analysts consider a foreign factor, a foreign source ID, and a foreignness explanation to make a foreignness determination. *See generally* NAT'L SEC. AGENCY, *supra* note 91.

[199] *See* USSID 18, *supra* note 20, § 9.18(e). DOD 5240.01 defines "reasonable belief" as: "When the facts and circumstances are such that a reasonable person would hold the belief. A reasonable belief must rest on facts and circumstances that can be articulated; hunches or intuitions are not sufficient. A reasonable belief can be based on experience, training, and knowledge of foreign intelligence or CI activities as applied to particular facts and circumstances, and a trained and experienced person might hold a reasonable belief that is sufficient to satisfy these criteria when someone unfamiliar with foreign intelligence or CI activities might not." U.S. DEP'T OF DEF., *supra* note 163.

[200] *See XKEYSCORE Presentation From 2008*, THE GUARDIAN (July 31, 2013), https://www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation [https://perma.cc/WJF7-RQU9].

[201] USSID 18, *supra* note 20, § 9.18(e).

necessarily indicate whether a person is foreign. For instance, a selector is presumed foreign if it is in contact with a selector overseas, but no information indicates the potential domestic selector is in the United States.[202] This particular foreignness factor is problematic because VPNs and other anonymity services used by U.S. persons can cause a U.S. person to appear as a foreign selector.[203] The foreignness factors also ignore the fact that everyday technical mistakes may cause a U.S. person to appear as foreign. For example, in November 2018, there was a brief period in which substantial Google traffic was misdirected through Russia and China.[204] Based on the standards above, the broad surveillance programs collecting ostensibly non-U.S. person information almost definitely analyzed and saved U.S. person information during this occurrence.

While little public evidence exists, it is likely that foreignness factors are inadequate protections for U.S. persons.[205] Other large-scale acquisitions by NSA have been conducted with greater oversight and heightened requirements, yet still collected substantial U.S. person information.[206] For example, section 702's upstream collection collected "tens of thousands of wholly domestic communications."[207]

The second requirement for conducting surveillance under EO 12333 is that it must be likely that foreign intelligence information will be collected.[208] Foreign intelligence information is defined in EO 12333 as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists" and also includes counterintelligence.[209] Concrete examples of foreign intelligence

---

[202] *See* Greenwald, *supra* note 186; OVSC1100, LESSON 2—CONVENTIONAL COLLECTION, *supra* note 8, at 4.

[203] *See* A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RESEARCH CENTER (June 4, 2018), https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/ [https://perma.cc/D42D-SYCX].

[204] Drew FitzGerald & Robert McMillan, *Google Internet Traffic is Briefly Misdirected Through Russia, China*, WALL ST. J. (Nov. 12, 2018), https://www.wsj.com/articles/google-internet-traffic-is-briefly-misdirected-through-russia-china-1542068392 [https://perma.cc/TJ7K-2PNZ].

[205] Professors Arnbak and Goldberg provide useful commentary explaining the potential lack of foreignness factors, as well as legal and technical loopholes to surveil U.S. person communications traffic abroad. *See generally* Arnbak & Goldberg, *supra* note 106.

[206] *See* Memorandum Opinion [Caption Redacted], [Docket No. Redacted], 2011 WL 10945618, 43 (FISA Ct. 2011).

[207] *Id.*

[208] *See* REBECCA J. RICHARDS, NSA CIVIL LIBERTIES AND PRIVACY OFFICE, NSA'S CIVIL LIBERTIES AND PRIVACY PROTECTIONS FOR TARGETED SIGINT ACTIVITIES UNDER EXECUTIVE ORDER 12333 (Oct. 7, 2014), https://www.nsa.gov/Portals/70/documents/about/civil-liberties/reports/nsa_clpo_report_targeted_EO12333.pdf [https://perma.cc/GH4X-XRHH].

[209] *See* DEP'T OF DEF., DEF. PRIV., C.L., AND TRANSPARENCY DIV., EXEC. ORDER 12333: UNITED STATES INTEL. ACTIVITIES, § 3.5(e) (2008), https://dpcld.defense.gov/Portals/49/Documents/Civil/eo-12333-2008.pdf [https://perma.cc/RT6K-QJ5T]. Counterintelligence is defined as "information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or

information requirements can be found in the classified National Intelligence Priorities Framework, some of which are reflected in the unclassified Office of the Director of National Intelligence's Worldwide Threats Assessment.[210]

Surveillance systems may be tasked with a selector if both requirements are met. If a selector will result, or may reasonably result, in the interception of U.S. person communications, it must be designed—to the extent practical under the circumstances—to not collect the U.S. person communication.[211] Once information is collected, NSA procedures authorize retaining any incidentally collected information to, from, or about U.S. persons so long as the interception or review was targeted against an "appropriate foreign intelligence target."[212] Further, unevaluated U.S. person information remains in NSA databases until actively reviewed by a human analyst.[213] Once reviewed, broad exceptions apply to retain the information even if the analyst believes the information belongs to a U.S. person and, thus, should be deleted.[214]

B. *U.S. Person Surveillance*

USSID 18 implements EO 12333's authorization for certain U.S. person surveillance by issuing detailed procedures to target, collect, retain, and share U.S. person information.[215] USSID 18 procedures allow for communications that are known to be to, from, or about a U.S. person to be intentionally intercepted or selected: (1) when the person is subject to a FISA court order; (2) with the approval of the Attorney General in certain situations; (3) when the Director of the NSA approves surveillance in situations not requiring Attorney General or FISA court approval; or (4) in emergency situations.[216] While U.S. person surveillance is limited to these four scenarios, the procedures' intersection with FISA remains classified. Therefore, it is unclear whether these limitations actually prohibit a wide breadth of collection on U.S. persons.

First, USSID 18 allows acquisition of communications to, from, or about a U.S. person if they are already under traditional FISA surveillance.[217] It is likely that in every instance a person is surveilled with a FISA court order, they are also

---

assassinations conducted for or on behalf of foreign powers, organizations, or persons, or their agents, or international terrorist organizations or activities." *Id.* § 3.5(a).

[210] Robert Litt, General Counsel, Office of the Dir. of Nat'l Intel., Remarks at the Brookings Institution (Feb. 4, 2015), http://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on [https://perma.cc/7N6Y-LJL7].

[211] OFF. OF THE DIR. OF NAT'L INTEL., FACT SHEET ON EO 12333 RAW SIGINT AVAILABILITY PROC. (2017), http://icontherecord.tumblr.com/post/155766682978/fact-sheet-on-eo-12333-raw-sigint-availability [https://perma.cc/86PU-CZYS]. It is unclear how this requirement is implemented and further details about the circumstances remain classified.

[212] USSID 18, *supra* note 20, § 4.3.

[213] *See id.*

[214] *See id.*

[215] *See id.*

[216] *See id.* § 4.

[217] *See id.* § 4.1(a); Annex A is a template for the minimization procedures filed with the FISA Court and used for section 702 surveillance. 50 U.S.C. §§ 1801(h), 1881a(e).

surveilled with EO 12333. Indeed, one EO 12333 program, UNITEDRAKE, is a computer network attack that implements this surveillance.[218] The user interface of UNITEDRAKE includes a set of buttons allowing an NSA analyst to insert a FISA court order number and the date the order expires.[219] Moreover, the program allows the agency to impersonate the owner of a target's computer.[220] It also permits the NSA to prioritize certain collection from the computer, control the information exfiltrated, and edit and delete the implant on the targeted computer.[221]

Second, the Attorney General can also approve EO 12333 surveillance of U.S. person information if the collection is directed at: (1) communications to or from U.S. persons outside the United States that are already approved for targeting under FISA sections 703, 704, or 705(b); [222] (2) certain international communications;[223] or (3) communications which are not to or from, but merely "about" U.S. persons "wherever located."[224] The Attorney General must conclude that the person is an agent of a foreign power and the purpose of the surveillance is to acquire significant foreign intelligence information.[225] These requirements loosely mirror the findings required under FISA to conduct electronic surveillance; however, USSID 18 does not define "significant foreign intelligence."[226] The Classified Annex Authority notes: "'significant foreign intelligence' shall mean not only those items of information that are in themselves significant, but also items that are reasonably believed, based on the experience of the United States Signals Intelligence System, when analyzed together with other items, to make a contribution to the discovery of 'significant foreign intelligence.'" [227] This circular definition provides little insight into what information would qualify as *significant foreign intelligence* and further supports the idea that permissive targeting standards are rife throughout the EO 12333 electronic surveillance landscape.

Third, the Director of the NSA can acquire U.S. person communications so long as approval is not required from the Attorney General or from the FISA

---

[218] NAT'L SEC. AGENCY, ACCELERATED DEVELOPMENT TEAM, UNITEDRAKE MANUAL, https://assets.documentcloud.org/documents/3987443/The-Shaow-Brokers-UNITEDRAKE-Manual.pdf [https://perma.cc/D63E-ESZU].
[219] *See id.* § 4.10.
[220] *See id*. § 5.1.
[221] *See id.* § 4.
[222] USSID 18, *supra* note 20, § 4.1(b)(1)(a).
[223] Parts of the section are still classified. *See id*.
[224] *See id.* § 4.1(b)(1)(c).
[225] *See id.* §§ 4.1(b)(1)–(3); U.S. DEP'T OF DEF., *supra* note 168, § 4.1(c); Little is known about the implementation of this authority and whether or not this authority implements section 2.5 of EO 12333; however, a 2003 memo confirms the Attorney General has used section 2.5 of EO 12333 and Classified Annex Authority to spy on communications of U.S. persons. NAT'L SEC. AGENCY, REPORT FOR THE CHAIRMAN, INTEL. OVERSIGHT BOARD 2 (Sept. 18, 2003), https://www.aclu.org/foia-document/report-president-36 [https://perma.cc/365Q-5URR].
[226] *See* USSID 18, *supra* note 20, §§ 4.1(b)(1)–(3); *see also* U.S. DEP'T OF DEF., *supra* note 168, § 4.1(c); NAT'L SEC. AGENCY, MEMORANDUM FOR THE CHAIRMAN, INTEL. OVERSIGHT BOARD 2 (Sept. 18, 2003), https://www.aclu.org/foia-document/report-president-36 [https://perma.cc/365Q-5URR].
[227] U.S. DEP'T OF DEF., *supra* note 168, § 4.1(c).

court.[228] Acquisition can occur when a person consents,[229] if the person is reasonably believed to be held hostage or captive,[230] when the target is a foreign entity outside the United States communicating with a U.S. person in the United States,[231] or when technical devices are employed in certain circumstances.[232]

A declassified memo confirms the Director of NSA approved, at minimum, consensual collection of U.S. person information in the early 2000s.[233] However, current use of the approval is classified and redacted from relevant documents. This authority is significant because any surveillance targeting U.S. persons that both falls outside FISA's definition of electronic surveillance, and, according to the Attorney General, is unprotected by the Fourth Amendment, would be permitted so long as one of the several conditions listed in § 4.1(c) are met.[234]

The ability to insert U.S. person selectors into EO 12333 surveillance programs is problematic because of the large-scale acquisitions occurring under these programs. While programs like UNITEDRAKE likely exist to target individual devices, selectors in many EO 12333 programs are not targeting one mobile device or computer, but an entire communications stream travelling through the United States, or within or between foreign countries.[235] Eventual collection of selectors, persons in contact with the selectors, and the telecommunications traffic nearby to the selector when acquisition occurs are all implicated.

EO 12333's surveillance and permissive targeting standards result in so much information that the NSA is unable to fully analyze it.[236] The Obama Administration approved agencies obtaining raw signals intelligence from the NSA so long as there were EO 12333, Attorney General-approved procedures in place for each agency.[237] Each agency requesting access to the information must sign an agreement with the NSA and draft their own Attorney General-approved procedures describing how the information will be handled.[238] These procedures

---

[228] USSID 18, *supra* note 20, § 4.1(c).
[229] *See id.* § 4.1(c)(1).
[230] *See id.* § 4.1(c)(2).
[231] *See id.* § 4.1(c)(4).
[232] *See id.* § 4.1(c)(5). Educated guesses can be made as to the exact type of collection allowed and range from installation of malware or devices on a target's personal laptop to any type of bulk acquisition.
[233] NAT'L SEC. AGENCY, REPORT FOR THE CHAIRMAN, INTEL. OVERSIGHT BOARD, *supra* note 225, at 2.
[234] One recent example may be SpaceX's novel Starlink satellite internet, which is a satellite constellation offering satellite Internet access and likely falls outside the traditional FISA definitions.
[235] *See supra* Part IV.C.
[236] *See, e.g.*, NAT'L SEC. AGENCY, CONTENT ACQUISITION OPTIMIZATION, *passim*, https://bit.ly/37sxRMj [https://perma.cc/N3Y7-AHYA] (last visited Jan. 29, 2021).
[237] Charlie Savage, *NSA Gets More Latitude to Share Intercepted Communications*, N.Y. TIMES, (Jan. 12, 2017), https://www.nytimes.com/2017/01/12/us/politics/nsa-gets-more-latitude-to-share-intercepted-communications.html [https://perma.cc/HWS7-FZVV].
[238] *See, e.g.*, CENTRAL INTEL. AGENCY, CENTRAL INTELLIGENCE AGENCY INTELLIGENCE ACTIVITIES: PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE

are similar to NSA procedures, including the same broad exceptions, but with subtle distinctions tailored to the agencies' needs.[239]

C. *EO 12333's Bulk Acquisition Techniques*

While some EO 12333 programs are used for individualized surveillance, this Article focuses on EO 12333's large-scale electronic surveillance programs. Permissive targeting standards, intended to collect information from foreign targets, result in the collection of substantial amounts of U.S.-person information from mobile phones, laptops, instant messaging apps, business servers, online platforms, and the larger telecommunications backbone.[240] This Section introduces the three different categories of EO 12333's electronic surveillance: (1) pure bulk collection programs, (2) bulk acquisition programs, and (3) a mixture of the two where a graphical user interface serves both as an acquisition, retrieval, and search platform.

1. Bulk Collection Programs

The first EO 12333 electronic surveillance category is similar to the Section 215 Call Detail Records program, which used section 215 of the USA PATRIOT Act to require telephone service providers to submit customer call records on a daily basis during 90-day intervals.[241] The Executive Branch did not possess a particular target, person, or device it was interested in, but received an entire dataset of daily calling records from the telecommunications companies.[242] After receipt into NSA databases, NSA analysts would then search the phone records database with a selector reasonably suspected of being associated with a specific terrorist organization.[243] The disclosure of the program marked the first public glimpse into some of the novel acquisition programs used by the NSA involving bulk collection.

EO 12333 authorizes similar programs. One such program, MYSTIC, includes the collection of foreign content and metadata from entire countries.[244] For example, subprograms of MYSTIC collect the entire telephony metadata created in

---

ORDER 12333 § 6.2.3(c) (2017), https://www.cia.gov/about-cia/privacy-and-civil-liberties/CIA-AG-Guidelines-Signed.pdf [https://perma.cc/5GXF-DYJB].

[239] *See, e.g.*, NAT'L SEC. AGENCY, PROCEDURES FOR THE AVAILABILITY OR DISSEMINATION OF RAW SIGNALS INTELLIGENCE INFORMATION BY THE NATIONAL SECURITY AGENCY UNDER SECTION 2.3 OF EXECUTIVE ORDER 12333 (RAW SIGINT AVAILABILITY PROCEDURES) 7–8 (Jan. 3, 2014), https://www.documentcloud.org/documents/3283349-Raw-12333-surveillance-sharing-guidelines.html [https://perma.cc/JNQ3-C9QC]; The Obama Administration procedures allow communications between U.S. persons to be reviewed, "When the communication contains significant foreign intelligence or counterintelligence." *Id.* at 11.

[240] *See supra* Part I.B.

[241] PRIV. AND C. L. OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 42 (2014).

[242] *See id.* at 8.

[243] *See id.* at 28.

[244] *See* Devereaux, Greenwald, & Poitras, *supra* note 184.

the Bahamas, Kenya, Mexico, the Philippines, and one other unnamed country suspected to be associated with Afghanistan.[245]

It is not just metadata collection. Actual bulk collection of foreign content is also occurring. SOMALGET, a subprogram of MYSTIC, actively records all phone traffic in the Bahamas and the aforementioned unnamed country, archiving its contents for 30 days.[246] SOMALGET's information database managed "roughly 5 billion call events,"[247] "over 100 million calls per day."[248] Prior to applying selectors, SOMALGET was a bulk collection program because the NSA collected a dataset without using an initial selector or target to determine what would be stored in its databases. After applying selectors, SOMALGET shifted to a bulk acquisition program. In total, the SOMALGET's analysis and collection of non-foreign intelligence information is staggering: such analysis and collection sweeps up any U.S. persons communicating in those countries and any person communicating with individuals residing in those countries.

2. Transit Authority and Upstream Collection

The second category of EO 12333 electronic surveillance contains two different techniques. The first is similar to section 702's upstream collection.[249] It relies on an interpretation of FISA and EO 12333 that allows the Executive Branch to collect information travelling through or "transiting" the American telecommunications backbone that is not to or from a U.S. person.[250] With the second technique, the NSA acquires information at foreign access points through which foreign communications transit within and/or between foreign countries.[251] Examples include telecommunications traffic exiting a foreign military installation or telecommunications traffic exiting servers associated with a foreign legislature.

The complete details of Transit Authority are unknown. Transit Authority draws its legal authority from EO 12333 under an interpretation that FISA, in part, regulates communications to or from a person in the United States, but not necessarily foreign-to-foreign communications travelling through the United States.[252] The Reagan administration relied on this legal interpretation in concluding that EO 12333 authorized the collection of foreign-to-foreign

---

[245] *See id.*
[246] *See id.*
[247] *See* NAT'L SEC. AGENCY, INT'L CRIME & NARCOTICS DIVISION, SOMALGET 2 (2012), www.documentcloud.org/documents/1164088-somalget.html [https://perma.cc/RRV3-CK3P].
[248] *See* Devereaux, Greenwald, & Poitras, *supra* note 184.
[249] *See supra* Part II.A.
[250] *See* Charlie Savage, *Power Wars: The Relentless Rise of Presidential Authority and Secrecy*, POWER WARS BLOG (2011) [https://perma.cc/S735-25SX].
[251] *See SIGINT Authority Decision Tree*, *supra* note 8; NAT'L SEC. AGENCY, *supra* note 129, at 11; OVSC1100, LESSON 2—CONVENTIONAL COLLECTION, *supra* note 8, at 4.
[252] *See* Savage, *supra* note 250.

communications travelling through the United States.[253] Transit Authority authorizes surveillance programs similar to section 702's upstream collection in that digital packets are prioritized, sessionized, and analyzed as they traverse through the telecommunications backbone prior to storage in NSA databases.[254] The programs authorized by Transit Authority are particularly efficient because the United States has emerged as a major fiberoptic telecommunications hub.

Authorized by Transit Authority, OAKSTAR is a surveillance program, with sub-programs that provide "access" to different types of data collection.[255] Some sub-programs of OAKSTAR are authorized by section 702 to collect certain information, while others are authorized by EO 12333.[256] One EO 12333-authorized sub-program of OAKSTAR is MONKEYROCKET, which collects entire data sessions from a foreign access point, collecting metadata and content of billing information and IP addresses.[257] The program generates 2,000 events, or activity logs about a selector, per day.[258]

Transit Authority is also used in the STORMBREW, FAIRVIEW, WINDSTOP, RAMPART-T, RAMPART-M, and RAMPART-A programs.[259] The programs collect metadata and content over the telecommunications backbone from

---

[253] *See* Charlie Savage, *Power Wars Document: Transit Authority and the 1990 Lawton Surveillance Memo*, POWER WARS BLOG (Nov. 18, 2015), https://charliesavage.com/?p=557 [https://perma.cc/3JCN-NW4P].

[254] *See supra* Part II.A.

[255] *See* NAT'L SEC. AGENCY, SSO CORPORATE PORTFOLIO OVERVIEW (Aug. 8, 2015), https://www.nytimes.com/interactive/2015/08/15/us/documents.html [https://perma.cc/9KAK-4ZEY].

[256] *Id.*

[257] See NAT'L SEC. AGENCY, MONKEYROCKET, https://theintercept.com/document/2018/03/20/entry-from-ssodictionary-v1-0/ [https://perma.cc/P356-F447] (last visited Jan. 29, 2021).

[258] *See* NAT'L SEC. AGENCY, MONKEYROCKET ACHIEVES INITIAL OPERATIONAL CAPABILITY (2012), https://theintercept.com/document/2018/03/20/entry-from-sso-news/ [https://perma.cc/K8VP-8F44].

[259] *Newly Disclosed NSA Files Detail Partnerships With AT&T and Verizon*, N.Y. TIMES 64 (Aug. 15, 2015), https://www.nytimes.com/interactive/2015/08/15/us/documents.html [https://perma.cc/6ZQF-QNNB] (stressing the collection "must be foreign-to-foreign"); Unilateral NSA access is obtained in RAMPART-I/X and RAMPART-T, which means NSA is operating as the sole entity collecting information from the access point. NAT'L SEC. AGENCY, *Today's Cable Program*, https://robert.sesek.com/static/files/nsa-turbulence/sso-cable-program.jpg [https://perma.cc/4Q7R-U3ZQ]; According to German parliament investigations into NSA's signals intelligence program, Germany's signals intelligence division was able to limit the use of certain selectors when directed to perform surveillance on behalf of NSA as a second-party partner for EO 12333 collection. Hearing of the witness Mr. R. U. (BND, head of the site in Bad Aibling): 14th Meeting, September 25, 2014, https://dipbt.bundestag.de/dip21/btd/18/CD12850/D_I_Stenografische_Protokolle/Protokoll%2014%20I.pdf [https://perma.cc/XL2J-NB57]; s*ee also* Andre Meister, *Live-Blog aus dem Geheimdienst-Untersuchungsausschuss: Was machen NSA und BND zusammen in Bad Aibling?*, NETZPOLITIK (Sept. 25, 2015), https://netzpolitik.org/2014/live-blog-5-anhoerung-geheimdienst-untersuchungsausschuss-was-machen-nsa-und-bnd-in-bad-aibling/ [https://perma.cc/88HZ-PKVF].

different providers or parties.[260] RAMPART-A, which relies on help from allies like Germany, connects to telecommunications cables transferring over three terabits per second and is described as "collection against long-haul international leased communications through special access initiatives with world-wide SIGINT partnerships."[261]

A sub-program that does not rely on foreign allies is MUSCULAR.[262] MUSCULAR allowed NSA to infiltrate the main communication links between Yahoo's and Google's data centers.[263] In a 30-day period from December 2012 to January 2013, MUSCULAR was responsible for collecting 181 million records.[264]

The sheer volume of collection occurring under Transit Authority is significant, second only to techniques authorized by section 702 of FISA.[265] In 2003, FAIRVIEW collected more than one million e-mails per day.[266] Less than ten years later, that number was five million per day, which means FAIRVIEW collected more than 1.8 billion communications annually.[267] These numbers only concern communications—not metadata—and are almost a decade old. In the same one-month period between December 10, 2012 and January 8, 2013, exactly 6,142,932,557 metadata records were collected under Transit Authority.[268] This

---

[260] *See supra* note 259; Kevin Collier, *How the NSA Ranks Its International Spying Partners*, THE DAILY DOT (Mar. 20, 2020), https://www.dailydot.com/debug/nsa-five-nine-14-41-eyes-alliances-spying/ [https://perma.cc/BUB2-NFCE]; *Fairview Defined*, https://static.propublica.org/projects/nsa-att/assets/img/generated/fairview-defined-900*676-96308b.jpg [https://perma.cc/3R6Z-2PM7].

[261] Kristian Jensen, *Black Budget*, INFORMATÍON 61 (Jun. 19, 2014), https://s3.amazonaws.com/s3.documentcloud.org/documents/1200866/foreignpartneraccessbudgetfy2013-redacted.pdf [https://perma.cc/GJ7P-JUP7].

[262] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Datacenters Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2013), https://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 [https://perma.cc/UAT7-7C9Z].

[263] *See* Arnbak & Goldberg, *supra* note 106, at 344; AMOS TOH, FAIZA PATEL, & ELIZABETH GOITEIN, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 5-6 (2016), https://www.brennancenter.org/our-work/research-reports/overseas-surveillance-interconnected-world [https://perma.cc/46TY-93Y9]; The program is likely not used under the FISA authority since the slide says it is less effective than FISA retrospective surveillance.

[264] Gellman & Soltani, *supra* note 262.

[265] One SIGAD under Transit Authority is second in terms of total data ingestion only to a SIGAD used by section 702 authorized surveillance. *See* NAT'L SEC. AGENCY, SSO CORPORATE PORTFOLIO OVERVIEW (Aug. 8, 2015), https://www.nytimes.com/interactive/2015/08/15/us/documents.html [https://perma.cc/9KAK-4ZEY].

[266] NAT'L SEC. AGENCY, FAIRVIEW AND STORMBREW: 'LIVE'—ON THE NET 1 (Nov. 11, 2003), https://www.documentcloud.org/documents/2274320-sidtoday-fairview-and-stormbrew-live-on-the-net.html [https://perma.cc/4G3P-MT8S].

[267] Nat'l Sec. Agency, SSO Corporate Portfolio Overview (Mar. 20, 2012), https://www.documentcloud.org/documents/2274321-sso-corpteambrief20mar2012-s2d.html [https://perma.cc/E974-TYL4].

[268] The FAIRVIEW program is denoted by the SIGAD US-990. *See* NAT'L SEC. AGENCY, *FAIRVIEW—Last 30 Days*, http://4.bp.blogspot.com/-

amount is so large that NSA continues to build data centers to store the information.[269] For example, the NSA data center in Utah is estimated to hold anywhere from 4.5 exabytes to a yottabyte of data.[270] In practical terms, it was once estimated that the total of all human knowledge created from the dawn of man to 2003 totaled 5 exabytes.[271] One yottabyte is about 500 quintillion (500,000,000,000,000,000,000) 8.5 x 11-inch pages of text.[272]

Transit Authority, however, is not the only authority used for bulk acquisitions. The second technique authorized by EO 12333 includes surveillance on information travelling within or between foreign countries collected at single telecommunications access points located in foreign countries. For example, HEADRESS targeted Juniper Networks, a U.S.-based company providing core routers and servers to foreign countries like Pakistan, Yemen, and China.[273] HEADRESS infiltrated a high-value Pakistani government/military secure network in order to exfiltrate data passing through its servers.[274] NSA accomplished the task by exploiting Juniper firewalls, servers, routers, and other computer equipment used by these countries.[275]

3. XKEYSCORE and Soft Selectors

The third category of EO 12333 electronic surveillance is exemplified by XKEYSCORE, which has been described in many ways, including as a search platform for analysts.[276] XKEYSCORE possesses a dual purpose: as a storage database allowing NSA analysts to search for already collected information and as a tool to task servers connected to the telecommunications infrastructure to

---

pmg0VfnBKrA/VdLmWPm9ctI/AAAAAAAACkY/He1Q1Tgg1Og/s1600/boundless-fairview.jpg [https://perma.cc/K5W3-SYG8].

[269] *See* Ingrid Burrington, *A Visit to the NSA's Data Center in Utah*, THE ATLANTIC, Nov. 19 2015, https://www.theatlantic.com/technology/archive/2015/11/a-visit-to-the-nsas-data-center-in-utah/416691/ [https://perma.cc/N6JT-N7RP].

[270] One yottabyte is one septillion bytes. *Yottabyte*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/yottabyte [https://perma.cc/Q8D2-QBQY] (last visited Oct. 22, 2020).

[271] James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 3, 2012), https://www.wired.com/2012/03/ff-nsadatacenter/ [https://perma.cc/Q86D-GKW8].

[272] *Id.*

[273] *See* Nat'l Sec. Agency, Assessment of Intelligence Opportunity—Juniper (Feb. 3, 2011), https://www.documentcloud.org/documents/2653542-Juniper-Opportunity-Assessment-03FEB11-Redacted.html [https://perma.cc/KM54-LHY].

[274] *See id.* (noting that Juniper firewalls are "central to the very high priority HEADRESS NY project targeting a Pakistan government/military secure network").

[275] *See id.* Once public or private servers are infiltrated, other programs can be engaged. QUANTUM tries to surreptitiously interfere when a user tries to connect to a website. *See* Nat'l Sec. Agency, There is More Than One Way to Quantum, https://www.aclu.org/files/natsec/nsa/there-is-more-than-one-way-to-quantum.pdf [https://perma.cc/5NAA-XUPZ].

[276] *See* Morgan Marquis-Boire, Glenn Greenwald, & Micah Lee, *XKEYSCORE: NSA's Google for the World's Private Communications*, THE INTERCEPT (Jul. 1, 2015), https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/ [https://perma.cc/CC67-DKHP].

prioritize and analyze communications traffic in bulk.[277] The full extent to which Transit Authority or other EO 12333 programs feed into XKEYSCORE is unknown.[278] While the program's exact systems architecture is also unknown, XKEYSCORE's function as a unique GUI for analysts that distinguishes it from other EO 12333 surveillance programs noted above, in part because XKEYSCORE consists of a collection methodology that collects information that "may" be of foreign intelligence value and retains that information.[279]

XKEYSCORE provides analysts with metadata and content information including social media platform messages, text messages, VOIP traffic, and login date/time stamps.[280] Generally speaking and as of the early 2010s, most content remains in XKEYSCORE for three to five days, while metadata is stored for 30-45 days.[281]

In 2008, XKEYSCORE included over 700 servers at approximately 150 field sites around the world.[282] These field sites receive raw traffic from "full take feeds."[283] Analysts can program rules representing certain online behaviors to test against the intercepted traffic.[284] These rules not only target information that is of foreign intelligence value from "strong selectors," but also from "soft selectors" that may contain foreign intelligence value.[285] Much like when a selector's location is assumed to be foreign if unknown, analysts appear to use soft selectors that may not actually collect information with foreign intelligence value or which contain a fantastically broad definition of "foreign intelligence information."[286]

Known XKEYSCORE rules are composed of fingerprints, which detect a specific type of content, like emails using a specific language; appIDs, which identify a protocol of traffic being intercepted, like a mail attachment in Gmail; and microplugins, which are a combination of appIDs and fingerprints, like all users

---

[277] *See id.*; Micah Lee, Glenn Greenwald, & Morgan Marquis-Boire, *A Look at the Inner Workings of NSA's XKEYSCORE*, THE INTERCEPT (Jul. 2, 2015), https://theintercept.com/2015/07/02/look-under-hood-xkeyscore/ [https://perma.cc/5GQ5-F2RG]; Greenwald, *supra* note 186; *XKEYSCORE Presentation From 2008*, *supra* note 200.

[278] *See* Devereaux, Greenwald, & Poitras, *supra* note 189.

[279] *See* NAT'L SEC. AGENCY, *supra* note 247.

[280] The 2013 document, "VoIP Configuration and Forwarding Read Me," details how to forward VoIP data from XKEYSCORE into NUCLEON, NSA's database for voice intercepts, facsimile, video, and "pre-released transcription." At the time, it supported more than 8,000 users globally and was made up of 75 servers absorbing 700,000 voice, fax, video, and tag files per day. Lee et al., *supra* note 277.

[281] *XKEYSCORE Presentation From 2008*, *supra* note 200.

[282] *See id.*

[283] *See* Greenwald, *supra* note 186.

[284] *See* Lee, Greenwald & Marquis-Boire, *supra* note 277.

[285] A key NSA document describes a collection methodology where NSA possesses "access to buffered audio files that MAY be associated with selectors not tasked to the collection asset in question" and "buffer[s] certain calls that MAY be of foreign intelligence value." *See* NAT'L SEC. AGENCY, *supra* note 247.

[286] *See* NAT'L SEC. AGENCY, *supra* note 247.

from Germany using a Kurdish language setting while sending encrypted emails.[287] If the rules match, then the information is stored in XKEYSCORE, but it can also be saved in other databases.[288] Some fingerprints have been released and include collecting incoming traffic at XKEYSCORE field sites for particular kinds of criteria and online behavior like individuals using encrypted communications, certain VPNs, or TOR.[289]

Strong selectors, like known unique device identifiers of an adversary, can also be searched in XKEYSCORE and tasked for acquisition by servers feeding into XKEYSCORE databases.[290] If an analyst is aware of an IP address, she can also obtain: other email addresses and phone numbers seen on the same network, files or attachments associated with the IP address or network, logins and passwords associated with the IP address, and websites visited by the IP address.[291] Pattern-of-life analysis can be conducted by tracing where and when selectors connect to mobile networks, websites, and online servers.[292]

XKEYSCORE allows for overly broad surveillance of selectors with an attenuated connection to actual targets possessing foreign intelligence information. The software is continuously fed data from surveillance programs and field sites or servers across the globe, where rules are continuously tested against information traffic streams in order to store the information in XKEYSCORE and other databases.[293] While the surveillance is not true bulk collection, like in the section 215 context, there is still collection of strong selectors that may over-collect and soft selectors that are not even determined to have verifiable foreign intelligence until after the collected information is reviewed. The notion of soft selectors is significant in the context of how much information is being collected. According to a 2009 document, some field sites receive over twenty terabytes of data per day.[294]

4. Inevitable Collection of American Communications

The scale of known surveillance authorized by Executive Order 12333 is breathtaking. The scope of information analyzed and collected includes wholly

---

[287] *See* Lee, Greenwald & Marquis-Boire, *supra* note 277.
[288] *See id.*
[289] *See* J. Appelbaum, A. Gibson, J. Goetz, V. Kabisch, L. Kampf, & L. Ryge, *NSA Targets the Privacy-conscious*, PANORAMA (Jul. 3, 2014), https://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html [https://perma.cc/6E6F-MV66]; *XKEYSCORE Presentation From 2008, supra* note 200.
[290] *See supra* note 289.
[291] Booz Allen Hamilton, *The Unofficial XKEYSCORE User Guide*, THE INTERCEPT 25 (Jan. 8, 2007), https://www.documentcloud.org/documents/2116191-unofficial-xks-user-guide.html#document/p1 [https://perma.cc/4GMY-N8WR].
[292] *See XKEYSCORE Presentation From 2008*, *supra* note 200.
[293] *See PTC Glossary*, SÜDDEUTSCHE ZEITUNG (Nov. 25, 2014), https://netzpolitik.org/wp-upload/2014-11-Snowden-Gerontic/PTC_Glossary_redacted.pdf [https://perma.cc/8GRM-DQ7W].
[294] *See* Lee, Greenwald & Marquis-Boire, *supra* note 277.

domestic communications, communications with at least one U.S person, and information concerning U.S. persons. The collection is further exacerbated by about collections, MCTs, and other incidental and inadvertent collection occurring due to permissive targeting standards and bulk acquisitions.

The public is often told EO 12333 is intended to collect foreign and counterintelligence information from foreign targets outside the United States. However, bulk acquisition programs collecting the entire telephony metadata of countries like the Bahamas, Kenya, Mexico, Philippines, and Afghanistan implicate any U.S. person visiting or living in the monitored country. In 2007, 87% of the 5 million tourists visiting the Bahamas were Americans and the island had approximately 30,000 American residents.[295] Approximately 32.39 million U.S. citizens traveled to Mexico in 2019.[296] It is clear that the surveillance EO 12333 authorizes encourages collections that will inevitably contain U.S. person information.

Aside from bulk collection programs, Transit Authority and XKEYSCORE's ability to perform about and MCT collections poses further problems. Given the staggering volume of information collected under Transit authority and XKEYSCORE,[297] incidental collection occurring under these programs is likely prolific.

In the section 702 context, the FISA court uncovered that upstream collection techniques similar to those authorized by Transit Authority that collected "tens of thousands of wholly domestic communications."[298] Since known bulk collection programs under Transit Authority mirror those programs operating under section 702, it is possible to reasonably conclude that the amount of incidental U.S. person collection is as high, if not higher than for the section 702 analog. This assumption mirrors a Washington Post report that reviewed intercepted communications from unknown legal authorities and concluded: "Nine of 10 account holders found in a large cache of intercepted conversations . . . were not the intended surveillance targets but were caught in a net the agency had cast for somebody else."[299] Nowhere is over-collection and the threat of incidental collection better implicated than by the use of "soft selectors" that may have intelligence value.[300] Surveillance occurring under XKEYSCORE, combined with

---

[295] *The Bahamas*, U.S. DEP'T OF STATE (Jun. 2007), https://2009-2017.state.gov/outofdate/bgn/bahamas/98434.htm [https://perma.cc/J8AK-63BK].

[296] *Number of United States Citizens Traveling to Mexico from 2002 to 2019*, STATISTA (Feb. 24, 2020), https://www.statista.com/statistics/214780/number-of-us-tourists-visting-mexico/ [https://perma.cc/8B7H-QYA7].

[297] *See supra* Part IV.C.ii.

[298] Memorandum Opinion [Redacted], No. [Redacted], 2011 WL 10945618, at *13 (FISA Ct. Oct. 3, 2011).

[299] Barton Gellman, *How 160,000 Intercepted Communications Led to Our Latest NSA Story*, WASH. POST (Jul. 11, 2014), https://www.washingtonpost.com/world/national-security/your-questions-answered-about-the-posts-recent-investigation-of-nsa-surveillance/2014/07/11/43d743e6-0908-11e4-8a6a-19355c7e870a_story.html [https://perma.cc/SWZ3-SU6W].

[300] *See* NAT'L SEC. AGENCY, *supra* note 247.

Transit Authority and other EO 12333 electronic surveillance, poses unique concerns about U.S. person information collected under the auspices of EO 12333.

Incidental collection is merely one piece of the inevitable collection of U.S. person information. As noted above, inadvertent collection occurs when an analyst is mistaken about the identify of a target.[301] Although USSID 18 procedures do require the deletion of communications where all parties are U.S. persons; however, many other communications and information may be retained.[302] Inadvertent collection is particularly egregious under Transit Authority since U.S. person information is analyzed whenever it is routed outside the United States or accessed from outside the U.S., like when a person uses elementary geo-location masking tools like VPNs or TOR.[303] Indeed, in both incidental and inadvertent collection the entire expat American community, which is estimated to be up to nine million U.S. citizens, is likely to be at risk of surveillance from such programs.[304]

The NSA reassures the public that these collections are not problematic because such information is almost never read by an NSA analyst, but remains in databases, and the information is protected under rigorous processing procedures.[305] Unfortunately, as detailed below, the processing procedures are rife with loopholes allowing for significant retention of U.S. person communications.

D. *Permissive Processing Procedures*

Once known U.S. person communications and unevaluated U.S. person information are stored in NSA databases for retrieval by analysts, permissive processing procedures allow for their further analysis and sharing. U.S. person information can be retained so long as the communications contain foreign intelligence information and the reference to the known U.S. person is masked.[306] The foreign intelligence information restriction is effectively useless because foreign intelligence information includes almost anything related to a country or

---

[301] *See supra* Part I.C.

[302] *See infra* Part IV.D.

[303] The number of U.S. internet users using VPNs is unclear, but estimates include 5% of U.S. internet users, while 18% of users in North America have used a VPN in the past month as of the first quarter of 2018. *See VPN Use and Data Privacy Stats for 2020*, VPNMENTOR (Feb. 20, 2020), https://www.vpnmentor.com/blog/vpn-use-data-privacy-stats/ [https://perma.cc/DW7N-9GEB]; *Share of Internet Users Worldwide Who Have Used a VPN in the Past Month as of First Quarter 2018 by Region*, STATISTA (Jul. 22, 2019), https://www.statista.com/statistics/306955/vpn-proxy-server-use-worldwide-by-region/ [https://perma.cc/76KK-N28F].

[304] *Consular Affairs By the Numbers*, U.S. DEP'T OF STATE (Jan. 2020), https://travel.state.gov/content/dam/travel/CA-By-the-Number-2020.pdf [https://perma.cc/3G3D-GHMS].

[305] This response is useful for representing one key debate between civil liberties advocates and the U.S. government, i.e., according to the U.S. government, privacy harms only occur if an NSA analyst reviews the U.S. person data for a non-foreign intelligence purpose. Privacy and civil liberties advocates often argue the privacy harm is in the computer analysis and eventual storage of the data, regardless of whether an NSA analyst reviews the data.

[306] CLASSIFIED ANNEX AUTHORITY, *supra* note 168, at § 4(A)2(a).

the national affairs of the United States.[307] In the section 702 context, the NSA noted it is "difficult to determine . . . the foreign intelligence value of any particular piece of information."[308] In its section 702 report, the Privacy and Civil Liberties Oversight Board, concluded: "[I]n practice, this requirement rarely results in actual purging of data."[309] Thus, the foreign intelligence information restriction in the EO 12333 context likely has similarly limited efficacy to its application in the section 702 context.

Several other broad exceptions also exist. For example, all communications necessary to "maintain technical databases for cryptanalytic or traffic analytic purposes" may be retained.[310] As written, the scope of this exemption is massive because "technical database" is defined as "information retained for cryptanalytic, traffic analytic, or signal exploitation purposes."[311] Further, all encrypted communications are kept in perpetuity or until decrypted, regardless of foreign intelligence value.[312] USSID 18 does not impose a retention period for these categories of U.S. person communications, but does require replacing or deleting the U.S. person identity if it is not necessary to understand the foreign intelligence information.[313] The exception likely continues despite the passage of section 309 limitations, since section 309 exempts communications "enciphered or reasonably believed to have a secret meaning."[314]

Outside of the communications collected, metadata and other non-content information can be retained from U.S. person communications so long as the information is used to establish or otherwise maintain an intercept, minimize an unwanted intercept, or "[s]upport cryptologic operations related to foreign communications."[315] Practically, these metadata exemptions are used, in part, to conduct social-contact chaining under the NSA's Supplemental Procedures Concerning Metadata Analysis ("SPCMA") guidelines.[316] These guidelines allow for the NSA to "contact chain,"[317] and conduct "pattern of life" analyses to create

---

[307] *See supra* Part III.
[308] *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act Before the Privacy and Civil Liberties Oversight Board* 46 (Mar. 19, 2014), https://permanent.fdlp.gov/gpo87084/20140319-Transcript.pdf [https://perma.cc/8DPJ-T9XV].
[309] PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 62.
[310] USSID 18, *supra* note 20, § 6.1(a)(2).
[311] *Id.* at Annex A, Appendix 1, § 2(i).
[312] *Id.* § 6.1.
[313] *Id.*
[314] Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309(b)(3)(B)(iii), 128 Stat. 3990, 3999 (2014). It is also important to note that section 309 only applies to specific covered communications and not to metadata. *See supra* Part II.C.
[315] USSID 18, *supra* note 20, § 5.4(b)(2).
[316] *See Documents on N.S.A. Efforts to Diagram Social Networks of U.S. Citizens*, N.Y. TIMES (Sept. 29, 2013), https://archive.nytimes.com/www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html [https://perma.cc/M77A-5T89].
[317] *See, e.g.*, Matt Niessen, *IBM i2 Analyst's Notebook-Esri Edition*, YOUTUBE (Dec. 20, 2012), http://youtu.be/MJ5CovDQDYU [https://perma.cc/RD8M-JBKW].

social maps of Americans.[318] Again, the broad definition of "foreign intelligence information" is critical to analyzing the oversharing of U.S. person information. The only requirement for analysis is that the chaining be for a foreign intelligence purpose.[319] A "SPCMA-enabled" program called CHALKFUN:

> [C]omputes the date, time, and network location of a mobile phone over a given time period, and then looks for other mobile phones that were seen in the same network locations around a one-hour time window. When a selector was seen at the same location (e.g., VLR) during the time window, the algorithm will reduce processing time by choosing a few events to match over the time period.[320]

Sometimes metadata can be even more revealing than the content of communications, and analysts are granted wide access to this U.S. person metadata.[321]

Processing procedures for non-U.S. persons are even more permissive and found in a document, titled "USSID 18: Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons."[322] Similar exceptions to those for U.S. persons exist for non-U.S. persons. For example, non-U.S. persons communications are also retained for up to five years unless the Director of the NSA determines the communications must be held longer for national security reasons.[323]

Once retained and analyzed, all of this information can be shared, or "disseminated" in intelligence community parlance. USSID 18's Section 7 provides guidelines for sharing communications resting in EO 12333 databases.[324] Section 7 allows for the dissemination of information—both foreign and domestic—so long

---

[318] *Justice Department and NSA memos proposing broader powers for NSA to collect data*, THE GUARDIAN (Jun. 27, 2013), http://www.guardian.co.uk/world/interactive/2013/jun/27/nsa-data-collection-justice-department [https://perma.cc/8ZFG-H4DS]; *see also* U.S. DEP'T OF DEF., SUPPLEMENTAL PROCEDURES GOVERNING COMMUNICATIONS METADATA ANALYSIS 1–2 (Nov. 11, 2004), https://www.dni.gov/files/documents/0909/DoD%20Supplemental%20Procedures%2020080314.pdf [https://perma.cc/ART6-STNZ].

[319] *See, e.g.*, Niessen, *supra* note 317.

[320] NAT'L SEC. AGENCY, SUMMARY OF DNR AND DNI CO-TRAVEL ANALYTICS 5 (Oct. 1, 2012), https://www.eff.org/files/2013/12/11/20131210-wapo-cotraveler_overview.pdf [https://perma.cc/W9UL-LAEG].

[321] *See* David Cole, *We Kill People Based on Metadata*, N.Y. REV. BOOKS (May 10, 2014), https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/ [https://perma.cc/BLQ9-ZXXR]; *see also* Kurt Opsahl, *Why Metadata Matters*, ELEC. FRONTIER FOUND. (Jun. 7, 2013), https://www.eff.org/deeplinks/2013/06/why-metadata-matters [https://perma.cc/Z5GB-342Q].

[322] USSID 18 Non-U.S. Persons Supplemental, *supra* note 195, § 4.1.

[323] *See id.* § 6.1(a).

[324] *See* USSID 18, *supra* note 20, § 7.

as the United States person information is substituted for a generic term like "U.S. firm" or "U.S. corporation."[325] The deleted identities used in an analyst's report are kept for one year and can be revealed to other government employees if requested.[326] USSID 18 allows the United States person information to be included in the report if the person consented to the dissemination of her communications, if the information is publicly available, or if the information is necessary to understand the foreign intelligence information or assess its importance.[327] Essentially, any unmasked information can be disseminated if relevant to a U.S. government agency or if the recipient believes the agency may need the masked information. The Director of the NSA must approve dissemination if the information is the identity of a senator, representative, or other employee of the Legislative Branch or if the information is being used for law enforcement purposes.[328] Non-U.S. person sharing is permitted in almost all circumstances, so long as the sharing is not solely based on the foreign person's status as a non-U.S. person.[329] The requirement allows for sharing anything related to foreign intelligence.[330]

E. *Overview*

Although permissive targeting standards are intended to target non-U.S. persons outside the U.S. for foreign intelligence information, EO 12333 surveillance is analyzing, collecting, and storing substantial amounts of U.S. person information. While the NSA admits that "[t]he collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons,"[331] the exact number of such communications collected is unknown.

Further, any U.S. person information that is collected is not protected by processing procedures because the processing, minimization, and dissemination "protections" are littered with broad exceptions. The foreign intelligence information mandate is essentially meaningless, while the technical database and encrypted data retention clauses allow for a significant number of communications to be retained. The use of stored metadata for analysis is particularly notable because known U.S. person metadata is being used under SPCMA guidelines to analyze social networks. SPCMA is the only declassified use of both section 702

---

[325] *See id.* § 7.2.
[326] *See id*.
[327] *See id.*; CLASSIFIED ANNEX AUTHORITY, *supra* note 168, § 4(A)(4).
[328] *See* USSID 18, *supra* note 20, § 7.3(a).
[329] *See* USSID 18 Non-U.S. Persons Supplemental, *supra* note 195, § 7.2.
[330] Even if the NSA argues the information contains "foreign intelligence information," the definition of foreign intelligence information used for such an argument is so broad that it may be meaningless.
[331] *See* Alexander W. Joel, *The Truth About Executive Order 12333*, POLITICO MAG. (Aug. 18, 2014), https://www.politico.com/magazine/story/2014/08/the-truth-about-executive-order-12333-110121 [https://perma.cc/8K3R-BETE].

and EO 12333 metadata. It is likely more uses of metadata are occurring under SPCMA or other policies.

VI. Reforming Executive Order 12333

The NSA's use of EO 12333 as its primary collection authority should itself be sufficient to invite greater congressional oversight and public concern. In spite of NSA's claim that EO 12333 is a strictly regulated regime collecting information from only "valid foreign intelligence targets,"[332] collection of U.S. person information under EO 12333 electronic surveillance programs presents ripe opportunities for reform. This Article squarely confronts the NSA's claim by showing that permissive targeting standards allow for the substantial collection of information from non-targeted U.S. persons, and that many collected communications potentially have no foreign intelligence information.[333] Further, although EO 12333 electronic surveillance programs ostensibly only provide for U.S. person collection in "very limited circumstances," the intelligence community has been unwilling to comment on the scope of such collection or provide hard figures on the number of U.S. person communications collected (incidentally or otherwise).[334] Even if U.S. person information is mistakenly collected, this Article shows that the permissive processing procedures found in USSID 18 do not adequately preserve U.S. person privacy.[335]

This Article argues for five categories of possible reforms to EO 12333 and the surveillance programs it authorizes. The first category aims to clarify how EO 12333 is used to electronically surveil U.S. persons. These proposals argue that more information must be revealed on the "limited circumstances" where U.S. persons are surveilled under EO 12333, and that FISA should oversee all U.S. person surveillance. The second category of reforms focuses on the aperture of surveillance and argues the NSA should engage in surveillance in a more targeted manner rather than at access points along the telecommunications backbone. The third category of reforms focuses on target selection and suggests heightening the current standard used for initiating surveillance from a reasonable suspicion tied to foreignness factors to a more robust requirement of specific and articulable facts. The fourth category of reforms focuses on a robust system of post-acquisition and post-collection checks, which bulk acquisitions necessarily rely on to ensure compliance. More can be done in this regard, and EO 12333 should, at minimum, impose the same post-collection checks as section 702 surveillance. Other processing standard reforms include more deletions of U.S. person information and

---

[332] Office of the Director of Nat'l Intel., *supra* note 21.

[333] Often referred to collectively as "information."

[334] For collection on U.S. targets, *see* U.S. DEP'T OF DEF. MANUAL 5240.1-R, *supra* note 163; see also Office of the Director of Nat'l Intel, *supra* note 21.

[335] In contrast, the intelligence community argues USSID 18 preserves privacy because the procedures only allow analysts to intentionally target a U.S. person selector with Attorney General (AG) approval and mandate the use of generic labels to "minimize" U.S. person information, like substituting a person's name with "U.S. Person One." Office of the Director of Nat'l Intel., *supra* note 21.

shorter retention periods. The Section concludes with transparency and accountability reforms focusing on increasing public awareness of EO 12333 through disclosure of the number of U.S. persons communications collected and publication of reports on EO 12333 to further public debates on EO 12333 activities.

A. *All U.S. Person Surveillance Must Fall Under FISA or an Amended FISA Statute*

One potential EO 12333 reform is for the Executive Branch to publicly clarify what U.S. person targeting occurs under the order's authority. Section 2.5 of EO 12333 authorizes the surveillance of U.S. persons outside the definitions of FISA.[336] The authorization is reflected in USSID 18, which authorizes collection of U.S. person information by the Attorney General and Director of the NSA in a variety of situations; however, the extent to which U.S. person collection occurs under section 2.5 is almost entirely classified.[337] In some instances in USSID 18, the authorization imposes the same standards as FISA by requiring the Attorney General find the U.S. person is an agent of a foreign power.[338] Other instances are redacted and provide little to no clarity.[339] For example, one redacted section states that U.S. persons can be targeted if surveillance is directed against "international communications to, from…"; however, the rest of the clause is redacted.[340] Another clause notes targeting can occur if the communication is about U.S. persons even if located in the U.S.[341] While the Executive Branch may argue that EO 12333 authorized surveillance cannot effectively be overseen by Congress, the breadth of surveillance authorized by EO 12333 should encourage Congress to ensure that any U.S. person surveillance is overseen by FISA.[342] Congress has already regulated some electronic surveillance occurring overseas on U.S. persons previously overseen by the Executive Branch by legislating sections 703, 704, and 705 of FISA.[343] Congress should ensure all EO 12333 electronic surveillance programs

---

[336] As noted in previous sections, electronic surveillance is defined by the statute while other requirements are only imposed when U.S. persons have a reasonable expectation of privacy. *See supra* Part II.A.

[337] *See* NAT'L SEC. AGENCY, OVSC1100, LESSON 2, *supra* note 8; While section 309 applies as a regulation on top of USSID 18, section 309 requirements only apply to communications and codified USSID 18 exceptions, like the cap on all storage of communications to five years. *See* Intelligence Authorization Act for Fiscal Year 2015, Pub. L. No. 113-293, § 309, 128 Stat. 3990, 3998–99 (2014).

[338] *See* USSID 18, *supra* note 20, § 4.1(b)(1)(a).

[339] *See id.* § 4.1(b)(1)(b)–(c).

[340] *See id.* § 4.1(b)(1)(b).

[341] *See id.* § 4.1(b)(1)(c).

[342] While this paper does not engage with separation of powers issues, persuasive arguments exist for Congressional action on any Executive Branch surveillance of U.S. persons. *See* Am. Civ. Liberties Union, Comment Letter to the Privacy and Civil Liberties Oversight Board on its Review of Executive Order 12333, (Jan. 13, 2016), https://www.aclu.org/letter/aclu-comments-privacy-and-civil-liberties-oversight-board-its-review-executive-order-12333 [https://perma.cc/232E-A2CB].

[343] *See* 50 U.S.C. § 1881(b), (d).

collecting U.S. person information occurs under the FISA regime, absent consent or a dire emergency.

Clarifying each of these points is critical as declassified documents concerning EO 12333 are unclear as to the status of section 2.5 of EO 12333, the Classified Annex Authority's "limited circumstances" surveillance, and USSID 18's authorization for certain U.S. person surveillance.[344]

B. *Narrowing the Scope of Surveillance*

Clarifying the extent to which EO 12333 is used to surveil U.S. persons is only a first step to reforming EO 12333's electronic surveillance programs. The aperture for signals intelligence should also be narrowed. This means the NSA should put more resources towards individualized/targeted surveillance —such as laptops, mobile devices, and even government buildings—instead of telecommunications switches or major telecommunications access points like the ones feeding XKEYSCORE. Narrowing the aperture of surveillance would mitigate the risk of overcollection and potentially lower the cost of compliance. Other possible constraints could include temporal or geographical limits. That is, surveillance might be permissible for a finite amount of time (e.g., hours not days) and then be reviewed through rigorous post-collection checks. Such a narrowing would also limit the raw data available to other agencies without a foreign intelligence or signals intelligence mission.

In response to these proposals, NSA is likely to argue that EO 12333's surveillance aperture is narrow enough because NSA focuses "on targeting the communications of those targets, not on collecting and exploiting a class of communications or services that would sweep up communications that are not of bona fide foreign intelligence interest."[345] Unfortunately, the permissive targeting standards and bulk acquisition programs belie such a response. If taken at its word, the class of communications of bona fide foreign intelligence include substantial amounts of information travelling along the telecommunications backbone that likely does not contain valuable foreign intelligence. If it is the case that valuable foreign intelligence is being gathered by bulk acquisitions, then that provides sufficient impetus for Congress to reevaluate EO 12333's electronic surveillance programs. At minimum, it encourages the executive to impose stricter standards on when analysts can initiate surveillance and what type of information analysts can collect.

C. *Heightening Surveillance Standards*

Narrowing the scope of surveillance should be complimented by increasing the standard required to initiate EO 12333 electronic surveillance. Currently, analysts must only reasonably believe a selector is a non-U.S. person outside the

[344] A sampling of declassifications heavily redacts any potential for insight into the activities. *See* OFFICE OF THE DIRECTOR OF NAT'L INTEL., *supra* note 168.
[345] Office of the Director of Nat'l Intel., *supra* note 21.

U.S. and that surveillance will collect foreign intelligence information.[346] It is also presumed a selector is foreign so long as an analyst does not definitively know the selector is a U.S. person.[347] Those standards may make sense in an idealized world where NSA nearly always targets agents of a foreign power and collects from devices or servers those agents operate. Such a world is far from reality, especially in light of the modern communications architecture. In particular, agents of a foreign power and other valid foreign intelligence targets are not the only ones communicating along the telecommunications backbone. U.S. person traffic may be routed internationally in a variety of instances and as a result of a variety of typical user behaviors. Further, in other contexts—like the FBI's searching of section 702 databases—surveillance standards were frequently violated.[348] Under Section 702, FBI analysts are required to limit themselves to queries where they have a "reasonable belief" the search would retrieve foreign intelligence information or evidence of a crime. Analysts' searches violated that standard, including queries to vet a potential source, a local police officer's application, college students participating in a "Collegiate Academy," and visitors of the FBI office.[349] In August 2019, the FBI made queries into approximately 16,000 persons—only seven were found to meet the reasonable belief standard by the National Security Division.[350]

Reforms heightening the "reasonable belief" standard for surveillance would ensure a lower number of MCTs and less information collected about U.S. persons. In other contexts—like at the FBI—agents routinely violated a requirement that they had a reasonable belief a search of section 702 databases was related to a foreign intelligence or criminal purpose.[351] One solution for NSA analysts would be to require that analysts possess specific and articulable facts showing the target and associated selectors are and belong to a non-U.S. person outside the U.S. and that foreign intelligence information will be collected. NSA could draw from the Targeting Analyst Rationales (TAR) used in section 702

---

[346] *See* NAT'L SEC. AGENCY, *supra* note 4.

[347] A person can be considered foreign when: the person has stated that he is located outside the U.S.; a human intelligence source indicates the person is located outside the U.S.; the person is a user of storage media outside the U.S.; a foreign government indicates that the person is located outside the U.S.; the phone number country code indicates the person is located outside the U.S.; the phone number is registered in a country other than the U.S.; SIGINT reporting confirms the person is located outside the U.S.; open source information indicates the person is located outside the U.S.; a network machine or technological information indicates the person is outside the U.S.; there is direct contact with a target overseas and there is no information to show the proposed target is in the U.S. There are a few more options that have been redacted, and are thus unable to be read. *See* Greenwald, *supra* note 186; OVSC1100, LESSON 2, *supra* note 8.

[348] *See* Memorandum Opinion and Order, at 69 (FISA Ct. Dec. 6, 2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf [https://perma.cc/Z23J-E5M5].

[349] *Id.* at 65–66.

[350] *Id.* at 67.

[351] *Id.* at 65–67. The subject at issue was whether FBI agents complied with the requirement that "the targeting of non-United States persons reasonably believed to be located outside the United States to acquire foreign intelligence information." *Id.* at 4.

surveillance.[352] A TAR contains a written statement describing the link between the user and the selector, the applicable section 702 certification the targeting falls under, the foreign intelligence expected to be obtained, and an explanation of the information leading to a conclusion that the selector belongs to a non-U.S. person who is reasonably believed to be located outside the United States.[353] In the section 702 context, two governments officials review the TAR.[354] If, in the EO 12333 context, analysts already perform such checks, then the government should publicize those checks to the greatest extent practicable just as it did for section 702.[355]

Imposing a heightened standard and ensuring rigorous post-collection checks would force the NSA to move away from "foreignness factors" that do not necessarily correspond to a non-U.S./U.S. person distinction. This would decrease the chances of targeting a U.S. person. Imposing a heightened standard is also more favorable than imposing a FISA warrant standard, which is likely untenable in the EO 12333 context.[356]

D. *Permissive Processing Reforms*

As shown, NSA's permissive processing procedures allow for extensive retention of U.S. person information for uses including: forwarding it to other federal agencies, pursuing criminal activities, and analyzing social networks.[357]

---

[352] *See generally* NAT'L SEC. AGENCY, CRSK1304, LESSON 2: HOW DO I CREATE TAR STATEMENTS, https://www.aclu.org/sites/default/files/field_document/FAA702PracticalApplications000917-001000.pdf [https://perma.cc/VK3V-79SJ].

[353] *Id.* at 11; In the EO 12333 context, the reasonable belief standard would be increased. Due to redactions, it's unclear if the TAR was shared by NSA to the FBI, which technically conducted the upstream and downstream acquisitions. A recently declassified FISA Court opinion indicates the post-tasking protections only occur "'in those cases in which [NSA] is technically capable of' performing them." *See* Memorandum Opinion and Order, *supra* note 348, at 14.

[354] *See* NAT'L SEC. AGENCY, PRISM TASKING PROCESS 1 https://www.eff.org/files/2013/11/15/20130629-wapo-prism.pdf [https://perma.cc/8UMN-3WX8] ("S2 FAA Adjudicators in Each Product Line" and "Targeting and Mission Management (S343)").

[355] *See generally* NAT'L SEC. AGENCY, OVSC1203 FISA AMENDMENTS ACT SECTION 702 (Aug. 18, 2016), https://www.intel.gov/assets/documents/702%20Documents/declassified/ACLU%2016-CV-8936%20RMB%20001001-001049%20-%20Doc%2017%20NSA-s%20Training%20on%20FISA%20Amendments%20Act%20Section%20702_OCR.pdf [http://perma.cc/Z6Q3-WLW9].

[356] It is likely an analyst would never meet such a burden since an analyst cannot be sure a selector is an agent of a foreign power until undertaking a holistic review of incoming communications. It is likely untenable in the EO 12333 realm because intelligence officials have said is untenable in the section 702 context for U.S. persons. *See Protect America Act of 2017: Hearing Before the House Permanent Select Committee on Intelligence*, 110th Cong. (2007) (Statement of Kenneth L. Wainstein, Assistant Attorney General National Security Division, Dep't of Justice), https://www.justice.gov/archive/ll/docs/aag-wainstein-hpsci-statement092007.pdf [https://perma.cc/JS35-5AYY]; Press Release, Dep't of Justice and Office of the Director of National Intelligence, (Mar. 11, 2008), https://www.dni.gov/files/documents/Newsroom/Press Releases/2008 Press Releases/20080311_statement.pdf [https://perma.cc/7HKF-L48S]. This suggestion assumes section 702 analyses can be applied to EO 12333 on the basis that section 702 is a much stricter regime than EO 12333.

[357] *See supra* Part IV.D.

While reforms to EO 12333's permissive processing procedures are required, they must be made with the full acknowledgement that the NSA is currently unable to comply even with existing processing procedures.[358] The inability for NSA to comply with current standards leaves any discussion of potential future reforms wanting. With that caveat, there is still ample room for improvement of NSA's permissive processing procedures.

First, the NSA can limit the categories of communications it retains. Currently, NSA can keep a number of U.S. person communications: communications to, from, or about a U.S. person can be retained if they are encrypted, if the person provides consent, if the information is publicly accessible, or if the information is necessary to understand "foreign intelligence information" or to assess its importance.[359] One of the few categories of communications that are deleted with few exceptions are wholly domestic communications—a communication where all parties are known U.S. persons.[360] Some existing categories, like the provision of consent, are justifiable. However, the declassified foreign intelligence information examples allow for broad collection of U.S. person communication. For example, foreign intelligence information includes international narcotics activity, any criminal activity, a threat to safety of a U.S. person, and other exceptions.[361] Outside of these defined types of communications, documents also indicate that encrypted communications and communications needed to "maintain technical databases" can be retained in addition to other U.S. person metadata maintained for social network analysis or metadata analysis.[362]

A broader range of information deserves a right to deletion when collected by EO 12333 electronic surveillance programs. This Article proposes narrowing the ability to retain communications to, from, and about U.S. persons for foreign intelligence information. It proposes narrowing the criminal activity exception to only include crimes listed in the foreign intelligence information definition of FISA.[363] This would ensure non-foreign intelligence criminal activity is protected, while allowing retention of criminal activity like sabotage and other clearly defined crimes with a congressionally-legislated nexus to foreign intelligence.[364] Such a reform could coincide with congressional debates on whether or not there is a

---

[358] *See* NAT'L SEC. AGENCY, *supra* note 33.
[359] *See* USSID 18, *supra* note 20, § 7.2.
[360] The retention procedures for non-U.S. persons are cause for such an even greater concern that a dedicated paper is suitable for such an analysis.
[361] *See* USSID 18, *supra* note 20, § 7.2.
[362] *Id.* § 6.1(a)(2).
[363] This Article does not engage with whether a foreign intelligence exception exists to the Fourth Amendment of the U.S. Constitution, as it is a topic for a dedicated paper.
[364] *See* 50 U.S.C. § 1801(e)(1). The statute references "grave hostile acts," 50 U.S.C. § 1801(e)(1)(A), which includes crimes like "domestic terrorism," 18 U.S.C. § 2331; "weapons of mass destruction," 18 U.S.C. § 2332a; "material support" 18 U.S.C. §§ 2339a and b; "sabotage," 18 U.S.C § 105, 50 U.S.C. § 1801(e)(1)(B); and clandestine intelligence activities. This last crime includes unauthorized disclosure statutes like 18 U.S.C. § 37 (Espionage Act), 18 U.S.C. §§ 792–798 (Espionage), and 18 U.S.C. §§ 1831–39 (Economic Espionage), among others; *see also* 50 U.S.C. § 1801(e)(1)(C).

foreign intelligence exception to the warrant requirement.[365]. This reform should be applied to any other U.S. person information; i.e., the only U.S. information retained by EO 12333 electronic surveillance programs would be for consent, emergencies, already public information, and other foreign intelligence information—but not to pursue "any criminal activity."[366] The amount of incidental information occurring under programs authorized by EO 12333 makes the potential U.S. person incidental collection far more likely than incidental collection occurring under traditional FISA-authorized programs, and thus problematic. Further, encrypted communications should only be retained if the U.S. person is found to be an agent of a foreign power. All retention of communications for *technical database* purposes should also be deleted. Indeed, a recent FISA Court decision revealed that NSA concluded such language was incredibly broad and narrowed its ability to retain section 702-acquired domestic communications for "technical database" purposes by eliminating the term and narrowing a definition to only information needed for "decryption and decipherment efforts."[367] Such a change should be made to USSID 18 and declassified as soon as possible.

To enforce such reforms, rigorous post-collection checks must be instituted. For instance, the NSA could impose post-EO 12333 collection protections similar to the processes implemented in section 702 surveillance.[368] One example of a section 702 post-collection check that can be applied to EO 12333 surveillance is a process called "Obligation to Review," or "OTR."[369] In the section 702 context, OTR mandates that the NSA analyst who initiated section 702 tasking must review the incoming surveillance from their tasking and verify that (1) the user of the selector is the intended target; (2) the target remains appropriate under the certification; (3) the target remains outside the United States; (4) there is no information revealing the target is inside the United States; and (5) the data collected is not subject to immediate destruction requirements (i.e., that the data contains a known domestic communication where all recipients are U.S. persons).[370] The analyst must detask the selector immediately using the appropriate detask reason if the review triggers any of the above criteria.[371] One document

---

[365] This Article does not engage in whether or not there is a foreign intelligence exception to the warrant requirement because it intends only to present an overall synopsis of EO 12333, how it is implemented, the surveillance programs it authorizes, and potential reforms. This particular reform is suggested, but requires a discussion for a dedicated paper: an in depth look at whether or not a foreign intelligence exception should or already exists.

[366] USSID 18, *supra* note 20, § 7.2.

[367] *See* Memorandum Opinion and Order, *supra* note 348, at 51.

[368] For the post-collection checks, see OFFICE OF THE DIRECTOR OF NAT'L INTEL., ANALYSIS AND PRODUCTION – DRAFT FAA 702 GUIDANCE 3 (2017), https://www.dni.gov/files/icotr/ACLU%2016-CV-8936%20(RMB)%20000911-001000%20-%20Doc%2010.%20NSA%E2%80%99s%20702%20Targeting%20Review%20Guidance.pdf [https://perma.cc/XSH2-SVU6].

[369] *Id.*

[370] *See* NAT'L SEC. AGENCY, CRSK1304, LESSON 1: OVERVIEW OF FAA702 AUTHORITY 1–2, https://www.aclu.org/sites/default/files/field_document/FAA702PracticalApplications000917-001000.pdf [https://perma.cc/39XS-VHUK].

[371] *See generally* NAT'L SEC. AGENCY, NSAW SID INTELLIGENCE OVERSIGHT (IO) QUARTERLY REPORT – FIRST QUARTER CALENDAR YEAR 2012 (1 JANUARY – 31 MARCH 2012) – EXECUTIVE

alludes to OTR being implemented for EO 12333 surveillance; however, the detailed processes are classified.[372] If protections are similar or already exist, such practices should be confirmed, declassified, and published to the greatest extent practicable similar to the documents NSA declassified for section 702.[373] At minimum, NSA should impose similar oversight requirements for EO 12333 acquisitions with additional reporting to Congress. Indeed, the NSA's own Office of Inspector General recommended as recently as fall 2019 that the Agency "develop a strategy for executing periodic verification of E.O. 12333 procedures that comprehensively addresses all stages of the SIGINT production cycle."[374]

Post-collection reforms also include ensuring shorter retention periods for U.S. person information.[375] For instance, the current retention period of five years must be re-evaluated.[376] The number of years was likely chosen to codify current practice: USSID 18 authorizes the retention of intentionally intercepted U.S. person communications for evaluation for up to five years.[377] No reasons were provided by Congress as to the rationale of a five-year retention period.[378] Further, no external studies or public debate surrounded the retention period's selection.[379] One possible origin of the time period may derive from the retention requirements imposed by the FISA court on the calling records obtained by NSA in its section 215 program.[380] Alternatively, it may be due to a finding by the intelligence community that data decreases in enough value to be disposed of after five years.[381] In 2015, the PCLOB recommended retention periods of three years for the section 215 program's calling records data.[382] Such a recommendation could be a starting point for metadata records, while more extensive analysis may need to be required for communications. Regardless of the exact time period, greater transparency and

---

SUMMARY (MAY 3, 2012), https://www.eff.org/files/2013/11/15/20130816-wapo-sid_oversight.pdf [https://perma.cc/C3TH-2EQ4].

[372] *See generally* REBECCA J. RICHARDS, *supra* note 208.

[373] *See generally* OFFICE OF THE DIRECTOR OF NAT'L INTEL., *supra* note 368.

[374] NAT'L SEC. AGENCY, OFFICE OF THE INSPECTOR GENERAL, SEMI-ANNUAL REPORT TO CONGRESS 30 (APR. 1, 2019 – SEPT. 30, 2019), https://oig.nsa.gov/Portals/71/Reports/SAR/APR-SEP%202019%20OIG%20SAR.pdf?ver=2020-01-23-095540-317 [https://perma.cc/A6DZ-7EDD].

[375] It is important to note that even today NSA does not comply with its current retention standards. As the OIG reported, "NSA has not fully implemented age-off calculations that use the most specific retention requirement with which data objects are labeled." NAT'L SEC. AGENCY, *supra* note 33, at 3.

[376] *See* Robert Eatinger, *Technology Advances Prompt Changes in CIA Collection Procedures*, CIPHER BRIEF (Feb. 22, 2017), https://www.thecipherbrief.com/column_article/technology-advances-prompt-changes-in-cia-collection-procedures [https://perma.cc/MSW7-EUT9].

[377] USSID 18, *supra* note 20, § 6.1(a)(1).

[378] *Cf.* S. REP. NO. 113-233 (2014); H.R REP. NO. 113-463 (2014).

[379] *Cf. supra* note 378.

[380] *See* In Re Application of the Federal Bureau of Investigation for an order requiring the production of tangible things from [redacted], No. BR-3-80, at 14 (FISA Ct. Apr. 25, 2013); *see also id.* at 3.

[381] OFFICE OF THE DIRECTOR OF NAT'L INTEL., SAFEGUARDING THE PERSONAL INFORMATION OF ALL PEOPLE: A STATUS REPORT ON THE DEVELOPMENT AND IMPLEMENTATION OF PROCEDURES UNDER PRESIDENTIAL POLICY DIRECTIVE 6 (2014), https://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf [https://perma.cc/K34B-NARV].

[382] PRIV. AND C. L. OVERSIGHT BD., *supra* note 241, at 17.

accountability must be provided to the public by explaining to the greatest extent possible why five years is an acceptable time period for retention. The intelligence community should also explore decreasing the time period.

E. *Transparency and Accountability*

Lastly, reforms to promote rigorous transparency and oversight are required. As this Article shows, the public does not know basic information about EO 12333 electronic surveillance programs.[383] Important aspects of the program, like its definitions for basic terms or how much U.S. person information is collected,[384] escape public attention. The public should not be forced to decipher such elementary information from obscure, dense documents containing numerous redactions.[385] Further, recommendations from the Office of Inspector General and PCLOB must be implemented and relevant documents must be publicly released to the greatest extent practicable.[386]

Greater public awareness begins with the ability to understand EO 12333 electronic surveillance programs' terms and definitions. EO 12333 and its implementing procedures have been in use since the 1980s, but only recently has enough information been released to even begin tackling basic definitions.[387] Critical terms of art must be defined. For example, when using selectors to intercept a communication based on content, analysts must use selectors "reasonably likely" to not intercept communications to or from a U.S. person located anywhere in the world.[388] One may assume analysts perform a totality of the circumstances analysis, but the standard is undefined across the intelligence community literature.[389] An analyst is also not supposed to use selectors that will return a "significant" number of U.S. person communications; however, the term is also undefined.[390] Even

---

[383] *See supra* Part III.B.

[384] A good start on this front would be to release the number of U.S. person communications collected under EO 12333.

[385] To its credit, the NSA through its Privacy and Civil Liberties Office (PCLO) has declassified some helpful materials. Whether at the behest of FOIA lawsuits or not, the PCLO at NSA is one of the few intelligence community departments declassifying and releasing relevant information to further public discussion and insight into intelligence programs. *See, e.g.*, REBECCA J. RICHARDS, *supra* note 208, at 4.

[386] For a smattering of reports and recommendations, *see* NAT'L SEC. AGENCY, OFFICE OF THE INSPECTOR GENERAL, *Reports*, https://oig.nsa.gov/reports/ [https://oig.nsa.gov/reports/]; in particular, the intelligence community may want to focus on PCLOB's recommendation 10 from its section 702 Report: "The government should develop a comprehensive methodology for assessing the efficacy and relative value of counterterrorism programs." *See* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 148. Again, developing, implementing, and executing such a recommendation is a ripe topic for a dedicated paper.

[387] *See, e.g.*, Diana Lee, Paulina Perlin, & Joseph Schottenfeld, *Gathering Intelligence: Drifting Meaning and the Modern Surveillance Apparatus*, 10 J. NAT. SEC. L. & POL'Y 77, *passim* (2019) (endeavoring to clarify such definitions and offering thoughtful proposals to ensure a shared nomenclature throughout the intelligence community), https://jnslp.com/wp-content/uploads/2019/04/Gathering_Intelligence_2.pdf [https://perma.cc/23V3-ZZH7].

[388] USSID 18, *supra* note 20, § 5.1.

[389] *Id.* § 5.1(b).

[390] *Id.*

colloquial terms like "passive" and "active" are used as unique terms of art by the NSA that the public can only guess at.[391] Analyses, like this Article's analysis of XKEYSCORE and EO 12333's bulk acquisitions, attempt to incorporate and explain basic definitions; however, critical details are missing and the analyses suffers as a result.

The lack of definitions for elementary terms is compounded by the lack of basic document management by the Executive Branch. For example, it is unclear to the public why the Classified Annex to DoD 5240.01 first appeared publicly in an annex to DoD Regulation 5240.01-R (the predecessor to DoD 5240.01); yet, in more recent declassifications it was released as an annex to NSA/CSS Policy 1-23.[392] While a highly technical point, the distinction is important to understanding fundamental questions about the scope, authority, and context of the document.

Document management will also compel the Executive Branch to release the most up-to-date documents. Even today some EO 12333 documents are severely outdated. For example, until it was released by the Obama administration in 2016, the latest DoD 5240.01 procedures were from the 1980s.[393] The Classified Annex Authority also appears to be from 1988: it was signed by Attorney General Edwin Meese III during that year and has no additional updates or signatures.[394] The Executive Branch should review and update all relevant EO 12333 policies and procedures, and release them to the greatest extent practicable.

The lack of definitions and the lack of document management breeds confusion about EO 12333's more advanced problems. For instance, the public does not know the answers to basic questions around MCTs.[395] MCTs are particularly invasive since they are not about a tasked selector and may have no relationship to the targeted selector aside from temporal proximity when the targeted selector sent their communication.[396] The Executive Branch has declassified section 702's collection of MCTs, and should also acknowledge the collection of MCTs under EO 12333. At minimum, the government should impose

---

[391] NSA likely has thousands of passive hosts around the internet and some of those hosts are feeding information into XKEYSCORE. *See, e,g.* NAT'L SEC. AGENCY, *SPINALTAP: Making Passive Sexy for Generation Cyber*, *passim*, *https*://www.eff.org/document/20150117-spiegel-spinaltap-nsa-project-combine-data-active-operations-and-passive-signals [https://perma.cc/QQT4-HSNP] (last visited Jan. 30, 2021).

[392] *See* U.S. DEP'T OF DEF, *supra* note 168, § C5.3.1.2. For the more recent declassification, see OFFICE OF THE DIRECTOR OF NAT'L INTEL., *supra* note 168, at 118.

[393] *See, e.g.*, U.S. DEP'T OF DEF, DIR. 5240.1-R, *supra* note 168 (listing its publication date as "4 April 1988").

[394] *See id.* at 422.

[395] They are almost definitely being collected by EO 12333 because it is known that EO 12333 electronic surveillance techniques replicate section 702 techniques known for collecting MCTs, wholly domestic communications, and vast amounts of U.S. person information. *See* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 39.

[396] *See* PRIV. AND C. L. OVERSIGHT BD., *supra* note 3, at 39.

the same requirements it imposes for FISA's MCTs and at maximum it can stop collecting MCT across the surveillance landscape.[397]

In addition to MCTs, it is still unknown how many U.S. person communications collected via intentional targeting, incidental collection, or inadvertent collection. The Executive Branch has been incredibly reluctant to release the information under section 702 and there is no doubt the reluctance extends to EO 12333.[398] Many stakeholders have pushed for the release of the number of US persons collected in order to understand vital information important to a public debate on section 702 authorities.[399] Similar rationale exists for EO 12333. Such information is required in order to understand the extent of U.S. person collection occurring under EO 12333—especially in light of bulk acquisition techniques described in this Article.

Lastly, rigorous transparency and accountability initiatives must be actively promoted. The Privacy and Civil Liberties Oversight Board (PCLOB) conducted reviews of section 215 and section 702 in order to analyze the surveillance authorities, provide recommendations to enhance privacy and civil liberties, and provide critical information for public discussion.[400] The Board announced two ongoing investigations into EO 12333 in 2015: one targeting a classified counterterrorism activity conducted by the CIA and another targeting NSA's XKEYSCORE.[401] Both "deep dive reviews" should shed light on EO 12333 activities, including how "soft selectors" are used and the relevant standards for surveillance.[402] Such revelations must be used to galvanize real reforms.

Aside from PCLOB, Congress already possesses the tools to request more information and conduct rigorous oversight. Senator Dianne Feinstein conducted a classified review of unknown scope in 2013 and that review should be published.[403]

---

[397] *See* NAT'L SEC. AGENCY, *supra* note 8.

[398] *See, e.g.*, Letter from Ron Wyden, Ranking Member of Senate Committee on Finance, to Daniel R. Coats, Director of National Intelligence (Aug. 3, 2017), https://www.wyden.senate.gov/imo/media/doc/Letter%20to%20DNI%20Coats%20on%20702%20Surveillance%20August%203,%202017.pdf [https://perma.cc/82QQ-7PFN].

[399] *See, e.g.*, Neema Singh Guliani, *Questions Congress Should Ask About Section* 702, AM. CIV. LIBERTIES UNION (Feb. 4, 2016), https://www.aclu.org/blog/national-security/privacy-and-surveillance/questions-congress-should-ask-about-section-702 [https://perma.cc/2CWE-CC57].

[400] PRIV. AND C. L. OVERSIGHT BD., *supra* note 241; PRIV. AND C. L. OVERSIGHT BD., *supra* note 3.

[401] *See* PRIV. AND C. L. OVERSIGHT BD., PCLOB EXAMINATION OF E.O. 12333 ACTIVITIES IN 2015, https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf [https://perma.cc/Q22Z-9U82]; *PCLOB Announces its Short-Term Agenda*, Privacy and Civil Liberties Oversight Board (Aug. 7, 2014) ("The Board will examine EO 12333 and its implications for privacy and civil liberties."), https://web.archive.org/web/20200610093533/https://www.pclob.gov/newsroom/20140807.html [https://perma.cc/X52T-MQCG].

[402] *See id.*

[403] *See* Press Release, Sen. Dianne Feinstein, Feinstein Statement on NSA Compliance, (Aug. 16, 2013), https://www.feinstein.senate.gov/public/index.cfm/press-releases?ID=9E2E8297-2968-40C9-8001-321E7A9A5079 [https://perma.cc/Q294-86AL] (noting that the Senator's committee held "briefings and hearings" and dealt with FISA compliance issues by "ending or adapting the activity").

Her review may have touched on critical information, like the number of U.S. person communications being collected or the international legal frameworks for sharing EO 12333 information with foreign intelligence partners.[404] At minimum, more information about compliance recommendations from the Office of Inspector General must be released.[405]

This Article shows that the public can only fully understand EO 12333 once sufficient transparency and accountability has been achieved. Not only is it necessary for the public, but for lawmakers that must tackle complex electronic surveillance and separation of powers issues.

F. *Overview*

Combined, these reforms can contribute to fewer privacy intrusions on U.S. person information, narrow the vast amounts of information collected by NSA, and initiate robust public discussion of electronic surveillance occurring outside the purview of FISA. There is no doubt significant work must be done by Congress in conjunction with the Executive Branch. However, this is not an insurmountable obstacle. Both branches have tackled similar problems in the past.

VI. Conclusion

Despite the information that can be deduced from public documents, there is still a tremendous amount of information unknown to the public about Executive Order 12333. Some academics are only beginning to scratch the surface of EO 12333 programs.[406] This Article creates a foundation for further research into the Executive Branch's use of unilateral surveillance, the use and nonuse of congressional oversight, and the poorly understand authorities that NSA uses to conduct the majority of its electronic surveillance. Additionally, this Article contributes to the body of literature arguing for a rethinking of the electronic surveillance landscape. As shown, EO 12333 and section 702 frustrate fundamental aspects of electronic surveillance like distinguishing between the content and non-content of communications and targeting an entity based solely on geography.

---

[404] *See* Scarlet Kim, Paulina Perlin & Diana Lee, *The "Backdoor Search Loophole" Isn't Our Only Problem: The Dangers of Global Information Sharing*, JUST SEC. (Nov. 28, 2017), https://www.justsecurity.org/47282/backdoor-search-loophole-isnt-problem-dangers-global-information-sharing/ [https://perma.cc/BS5X-6JS4].

[405] For instance, a March 2019 NSA Inspector General Report evaluated NSA's controls for removing data from EO 12333 searchable-databases and found NSA retaining data in violation of legal and policy rules and a lack of verifying data could be stored in EO 12333 databases. *See* NAT'L SEC. AGENCY, *supra* note 33, at 3–4.

[406] *See, e.g.*, Steven Englehardt, Dillon Reisman, Christian Eubank, Peter Zimmerman, Jonathan Mayer, Arvind Narayanan & Edward W. Felten, *Cookies That Give You Away: The Surveillance Implications of Web Tracking*, INT'L WORLD WIDE WEB CONF. COMM. (May 18, 2015), https://web.archive.org/web/20170812183130/https://senglehardt.com/papers/www15_cookie_surveil.pdf [https://perma.cc/CNX8-X2LT] (exploring programs that could steer certain traffic to filters and collect United States person data without using FISA).

These topics are left to other scholarship as this paper only seeks to introduce readers to fundamental aspects of EO 12333 and potential reforms.

This Article provides a basic foundation to understand how Presidential spying occurs under EO 12333 and the policy documents that authorize and implement the NSA's EO 12333 electronic surveillance programs. The documents are dense, lengthy, and confusing—perhaps intentionally so.

Fortunately, with recent disclosures, the public can glean insight into the policy documents that enable and implement EO12333 authorized surveillance. In order to allow readers to better understand the full extent of surveillance occurring under EO 12333, this Article first introduced foundational concepts. It discussed critical intelligence community definitions, how surveillance practically occurs through the use of selectors, and the categories of bulk acquisitions. Afterwards, it discussed the antecedents of EO 12333 and an overview of the executive order. The Article then discussed the permissive targeting standards that allow for the immense amount of surveillance authorized by EO 12333. Billions of communications and metadata are collected in order to both understand foreign adversaries and create social networks of Americans. The Article explored the various EO 12333 electronic surveillance programs by pairing EO 12333 with the known programs it authorizes. This Section made it clear that the outcomes of permissive targeting standards and bulk acquisitions programs are the inevitable acquisition, analysis, and collection of substantial quantities of U.S. person information. These potential privacy harms are only exacerbated by permissive retention, searching, and sharing standards.

Lastly, this Article argued that the significant amount of U.S. person information acquired and incidentally collected should catalyze reforms of EO 12333 surveillance programs. Recommended reforms include targeting surveillance at higher layers of a communications stream like laptops and mobile devices, heightening the standard for conducting surveillance, enhancing transparency on post-collection audits, reevaluating the five-year minimization procedure, and requiring more rigorous transparency and oversight.

Despite the information that can be deduced from public documents, there is still a tremendous amount of information unknown to the public about Executive Order 12333. Some academics are only beginning to scratch the surface of EO 12333 surveillance, like programs that could steer certain traffic to filters and collect United States person data without using FISA.[407] This Article lays the foundation for further research into the Executive Branch's use of unilateral surveillance, the existence or lack thereof of congressional oversight, and the poorly understood authorities that NSA uses to justify its surveillance programs. These

[407] *See e.g.*, Steven Englehardt *et al.*, *Cookies That Give You Away: The Surveillance Implications of Web Tracking*, *International World Wide Web Conference Committee*, May 18, 2015, https://senglehardt.com/papers/www15_cookie_surveil.pdf, [https://perma.cc/26R3-NFPD] (exploring programs that could steer certain traffic to filters and collect United States person data without using FISA).

areas of inquiry will be ripe for future questions concerning if, and how, the public should learn more about the categories of surveillance occurring unilaterally within the Executive Branch, whether and how Congress will exercise its oversight function, and just how much surveillance actually occurs under the auspices of this little-known authority. This Article also contributes to a growing body of literature arguing for a potential rethinking of the electronic surveillance landscape. As shown, EO 12333 and section 702 frustrate fundamental characteristics of electronic surveillance like distinguishing between the content and non-content of communications and targeting an entity based solely on geography. This Article leaves the questions created by that frustration to future scholars while focusing on introducing readers to fundamental aspects of EO 12333 and potential ways in which its mechanisms might be reformed.