COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD

Request for Public Comment on Activities Under Executive Order 12333

[Notice—PCLOB—2015—01; Docket No. 2015—0001; Sequence No. 1]

June 16, 2015

In 2014, the Electronic Privacy Information Center ("EPIC") urged the Privacy and Civil Liberties Oversight Board ("PCLOB") to expand its agenda beyond Sections 215 and 702 of the Foreign Intelligence Surveillance Act and to focus on surveillance activities carried out under Executive Order 12333.[1] EPIC stated, "[i]t is clear that the surveillance programs and activities under Executive Order 12333 require further scrutiny and these activities fall squarely within the Board's jurisdiction."[2] EPIC recommended that the Board oversee: (1) the extent to which surveillance activities under EO 12333

[1] Jeramie D. Scott, Nat'l Sec. Counsel, EPIC, Prepared Statement for the Record Before the Privacy and Civil Liberties Oversight Board (Jul. 23, 2014), *available at* https://epic.org/news/privacy/surveillance_1/EPIC-Statement-PCLOB-Review-12333.pdf [hereinafter EPIC 2014 PCLOB Statement].
[2] *Id*. at 3.

capture information on United States Persons; (2) the extent EO 12333 data collection results in the retention and/or dissemination of non-target data; and (3) current oversight and minimization procedure effectiveness.[3] EPIC further recommended that the Board publish its findings.[4]

By notice published on March 23, 2015, the Privacy and Civil Liberties Oversight Board adopted EPIC's recommendations and accordingly seeks public comment on activities under Executive Order 12333.[5] As the Board reviews activities under EO 12333, the Board will examine two E.O. 12333 counterterrorism-related activities.[6] The Board will concentrate on Central Intelligence Agency and National Security Agency's activities and "activities that involve one or more of the following: (1) bulk collection involving a significant chance of acquiring U.S. person information; (2) use of incidentally collected U.S. person information; (3) targeting of U.S. persons; and (4) collection that occurs within the United States or from U.S. companies."[7] The Board will review the privacy and civil liberties implications of E.O. 12333 surveillance activities.[8]

The Board will then produce two separate reports by the end of 2015 and "if appropriate, recommendations for the enhancement of civil liberties and privacy."[9] Although the Board anticipates that the reports will largely be classified, the Board "will assess whether particular

[3] *Id*.
[4] *Id*.
[5] Request for Public Comment on Activities Under Executive Order 12333, 80 Fed. Reg. 15,259 (Mar. 23, 2015).
[6] Privacy and Civil Liberties Oversight Bd., *PCLOB Examination of E.O. 12333 Activities in 2015* (2015), *available at* https://pclob.gov/library/20150408-EO12333_Project_Description.pdf.
[7] *Id*.
[8] *Id*.
[9] *Id*.

information about the activities under review warrants public-interest declassification [.]"[10] The Board will also issue a public report explaining how E.O. 12333's legal framework and implementing procedures govern the collection, use, retention, and dissemination of U.S. person information.[11]

EPIC submits these comments and recommendations to describe the privacy and civil liberties implications of EO 12333 and to urge the Board to provide meaningful oversight, accountability, and transparency in EO 12333 surveillance activities.

EPIC's Interest in Meaningful Oversight, Transparency, and Accountability of Government Surveillance Programs

EPIC is a non-profit research and educational organization established in 1994 to focus public attention on emerging privacy and civil liberties issues.[12] We work with a distinguished panel of advisors in the fields of law, technology and public policy.[13] For many years, EPIC has urged Congress, federal courts, and federal agencies to curtail surveillance activities and provide meaningful oversight, transparence, and accountability for government surveillance programs.[14] For example, in 2005, EPIC filed the first Freedom of Information Act ("FOIA") request seeking records on the Department of Justice's warrantless wiretapping program.[15] EPIC filed the request within hours after the New York Times reported that President Bush authorized warrantless wireless through an executive order.[16]

[10] *Id*.
[11] *Id*.
[12] *About EPIC*, https://epic.org/epic/about.html (2015).
[13] *EPIC Advisory Board*, https://epic.org/epic/advisory_board.html (2015).
[14] *See* EPIC, *Executive Order 12333*, https://epic.org/privacy/surveillance/12333/ (2015).
[15] *EPIC v. DOJ - Warrantless Wiretapping Program*, https://epic.org/privacy/nsa/foia/#foia (2015).
[16] *Id*.

In 2006, EPIC urged the Federal Communications Commission to investigate "American telephone companies, subject to FCC regulation, [that] have improperly released call detail information to the National Security Agency."[17] EPIC stated, "[w]e appreciate that there are circumstances under which the government may properly obtain customer information from telephone companies. But it is vital that such disclosures are undertaken pursuant to legal authority."[18]

In EPIC's 2007 testimony before the Senate Committee on Commerce, Science and Transportation, EPIC stated, "[we] would also like to bring to the Committee's attention our concern that the National Security Agency may have constructed a massive database of telephone toll records of American consumers."[19]

In 2012, EPIC testified before the House Judiciary Committee on the need to reform the Foreign Intelligence Surveillance Court, including "public reporting procedures for FISC opinions, published statistics for FISC orders, and a provision for an increased web presences, or other source of data tat can be easily accessed."[20] EPIC urged the FISC to publish past orders and opinions, while redacting sensitive materials to increase accountability.[21] EPIC also called on

[17] Letter from EPIC to Kevin Martin, Fed. Commc'n Comm'n (May 17, 2006), *available at* https://epic.org/privacy/phone/fcc-letter5-06.html.
[18] *Id*.
[19] *The Truth in Caller ID Act of 2007, S. 704, Hearing Before the S. Comm. on Commerce, Sci. and Transp.*, 110th Cong. (2007) (Testimony of Allison Knight, Staff Counsel, EPIC), *available at* https://epic.org/privacy/iei/s704test.pdf.
[20] The FISA Amendments Act of 2008, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. at 7 (May 31, 2012) (Statement of Marc Rotenberg, Exec. Dir., EPIC), *available at* https://epic.org/privacy/testimony/EPIC-FISA-Amd-Act-Testimony-HJC.pdf.
[21] *Id*.

Congress to strengthen "the authority of the FISA Court to review the government's use of FISA authorities."[22]

In 2013, EPIC, joined by over 3,000 members of the public, leading privacy experts, and journalists, petitioned the NSA to conduct a public rulemaking on the agency's monitoring and collection of communications traffic within the United States.[23] EPIC stated, "the NSA's collection of domestic communications contravenes the First and Fourth Amendments to the United States Constitution, and violates several federal privacy laws, including the Privacy Act of 1974, and the Foreign Intelligence Surveillance Act of 1978 as amended."[24]

Later that year, EPIC petitioned the Supreme Court to halt the disclosure of the telephone of the telephone records of millions of Americans, arguing "it is simply not possible that every phone record in the possession of a telecommunications firm could be relevant to an authorized investigation."[25]

And more recently, EPIC has urged the Board to prioritize Privacy Act enforcement. EPIC stated, "[g]overnment agencies within the Board's purview, like the DHS and NSA, routinely collect personal records without granting individuals basic Privacy Act protections."[26] EPIC noted that the Board's first public solicitation of comments in 2006 prioritized the privacy

[22] *Id*. at 8.
[23] Petition from EPIC et al. to Keith B. Alexander, Director, Nat'l Sec. Agency & Chuck Hagel, Sec. of Defense (June 17, 2013), *available at* https://epic.org/NSApetition/.
[24] *Id*.
[25] Petition for a Writ of Mandamus and Prohibition, or a Writ of Certiorari, *In re EPIC*, 134 S. Ct. 638 (2013) (No. 13-58), *available at* https://epic.org/privacy/nsa/in-re-epic/EPIC-FISC-Mandamus-Petition.pdf.
[26] Letter from Marc Rotenberg, EPIC President, Khaliah Barnes, EPIC Administrative Counsel, EPIC to PCLOB on "Defining Privacy," at 4 (Nov. 11, 2014), *available at* https://epic.org/open_gov/EPIC-Ltr-PCLOB-Defining-Privacy-Nov-11.pdf.

and civil liberties implications arising from the Terrorist Screening Database, which is one of the largest government national security databases.[27]

Executive Order 12333 was Adopted to Limit Domestic Surveillance Activities by the Intelligence Communities

Since 1976, the activities of the U.S. Intelligence Community ("IC") have been regulated by Executive Orders.[28] These restrictions on IC activities were adopted in the wake of widespread abuses uncovered by the Church Committee.[29] For example, the Committee uncovered illegal "mail opening programs" that were conducted by the CIA and FBI for more than thirty years, and an illegal NSA program codenamed SHAMROCK through which the agency collected copies of all "international telegrams leaving the United States between August 1945 and May 1975."[30] The agencies "knew that the programs of opening mail, conducting electronic surveillance and physical searches, reading telegrams, and administering LSD were illegal," but the activities nevertheless persisted and, as a result of these abuses, Presidents issued executive orders strictly limiting IC activities and Congress passed the Foreign Intelligence Surveillance Act of 1978.[31] Executive Order 12333 established "special protections for United States persons" in order to prevent the type of abuses that occurred prior to the Church Committee. The purpose of the Order "is to 'balance' the 'acquisition of essential information' and the 'protection of individual interest.'"[32]

[27] *Id*.
[28] The first such order was issued by President Ford and was replaced by subsequent orders issued by President Carter and President Reagan. 1 David S. Kris & J. Douglas Wilson, *National Security Investigations & Prosecutions* § 1:4 (2d ed. 2012). The Order issued by President Reagan, E.O. 12333, remains in effect today (with some modifications). *Id*.
[29] *See* 1 Kris & Wilson § 2:1.
[30] *Id*. § 2:3.
[31] *Id*. § 2:7.
[32] *Id*. (citing Exec. Order No. 12333 § 2.2).

But the Intelligence Community has broadly interpreted Executive Order 12333 to permit unbounded collection of personal records, contrary to the original purpose of the Order. To effectively carry out its mandate to protect privacy and civil liberties, the Board must provide meaningful oversight, transparency, and accountability concerning EO 12333 surveillance activities.

Summary of EPIC's Comments on EO 12333

Section I of the comments explain how NSA acquires a significant amount of U.S. person information through EO 12333 surveillance programs. Section I describes how EPIC has long advocated for limits on collection and discusses various recommendations for limiting collection of US persons and other non-target data under EO 12333, including uniformly defining collection as "the acquisition of information" and publishing guidelines and policies on EO 12333 collection. Section I concludes by raising several questions PCLOB should ask as part of its inquiry into the NSA's and CIA's collection programs.

Section II describes the need to minimize data collection and to limit dissemination of collected data to comply with the Code of Fair Information Practices and the Privacy Act of 1974. Section II makes several recommendations, including that: (1) agencies publicly disclose how data collected under EO 12333 will be retained, minimized, used, and disseminated; (2) data collected under EO 12333 must be minimized using robust privacy enhancing techniques to limit the retention of personally identifiable information; (3) data collected pursuant to EO 12333 should only be retained as long as strictly necessary to serve the purpose of collection; and (4) dissemination of incidentally collected data on U.S. persons should be limited to necessary and lawful purposes. Section II concludes with several questions for the Board to consider.

Section III describes the critical need for transparency and oversight in EO 12333 surveillance activities and recommends: (1) the Intelligence Community publish legal justifications for surveillance programs conducted under EO 12333; (2) the Board ensure that that the Intelligence Community acting in pursuance to EO 12333 comply with the Privacy Act and the Principles of Intelligence Transparency for the Intelligence Community; (3) agencies conducting activities under the authority of EO 12333 must publically issue regular statistical reports that include all relevant, non-classified information; (4) PCLOB require audit trails for EO 12333 surveillance activities to ensure accountability; (5) PCLOB maintain independence from the Intelligence Community in the Executive Branch; and (6) PCLOB develop its enforcement authority to compel agency cooperation and supervise the implementation of internal recommendations.

I. The NSA Acquires a Significant Amount of U.S. Person Information Through The Bulk Collection Programs Conducted Pursuant to EO 12333

Despite the restrictions placed on the Intelligence Community by Executive Order 12333 and the foreign intelligence surveillance laws, the NSA and CIA continue to engage in bulk collection and interception of communications and sensitive information about United States Persons.[33] As Senate Intelligence Committee member Senator Ron Wyden recently noted, "Today there's a global communications infrastructure, so there's a greater risk of collecting on Americans when the NSA collects overseas."[34] EPIC also raised this issue during a PCLOB's public meeting last year, pointing out that, "Although 12333 requires a court order to target a

[33] *See generally* EPIC 2014 PCLOB Statement, *supra*.
[34] Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, Wash. Post (Oct. 30, 2013), http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html [hereinafter Gellman & Soltani, *NSA Infiltrates Links*].

United States Person, this is of little comfort. Given the global nature of communications, the indiscriminate mass surveillance the NSA conducts overseas captures the information of United States Persons."[35] Now that communications are transmitted via a global telecommunications network, the territorial restrictions of EO 12333 do not meaningfully limit the bulk collection of U.S. person information and private communications transmitted via U.S. companies.

These programs significantly infringe citizens' rights under both the Privacy Act and the Fourth Amendment. Yet there is very little independent oversight of these programs; collection activities of the IC are difficult to monitor. As EPIC previously stated in a letter to PCLOB, "[t]he Privacy Act defines the right to privacy with regard to the collection and use of personal information by federal agencies . . . . Much has happened since 9-11 that is clearly contrary to the purposes of Privacy Act and the expectation of many Americans who rightly believe that the U.S. government would not develop massive databases to secretly profile Americans."[36] The Supreme Court recently issued a landmark ruling on digital privacy rights, finding that the Fourth Amendment requires officers to obtain a warrant prior to searching an individuals' cell phone incident to arrest.[37] The Court emphasized that "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search of evidence of criminal activity."[38] The Court also held that the Fourth Amendment requires

[35] EPIC 2014 PCLOB Statement, *supra*, at 3.
[36] EPIC Letter to PCLOB on "Defining Privacy," Marc Rotenberg, President, Khaliah Barnes, EPIC Administrative Counsel, EPIC 3-4 (Nov. 11, 2014), *available at* https://epic.org/open_gov/EPIC-Ltr-PCLOB-Defining-Privacy-Nov-11.pdf.
[37] *Riley v. California*, 134 S. Ct. 2473, 2494 (2014).
[38] *Id.*

heightened protections for digital content and communications, finding digital files are fundamentally different than analog records.[39]

Government programs of mass surveillance that indiscriminately collect data about U.S. Persons are similar to the reviled "general warrants" that the Founders sought to abolish.[40] However, in the context of foreign intelligence collection, it is difficult to ensure that collection is properly targeted and limited. As EPIC has emphasized, "the only check on surveillance under EO 12333 comes from Executive oversight. This type of self-regulation has proven to be ineffective at best in limiting surveillance overreach. The minimal oversight in place does not even give the appearance of the checks and balances provided by judicial or congressional oversight."[41]

It is urgent that PCLOB examine the scope of collection currently conducted under EO 12333, given that courts have already ruled that other NSA bulk collection programs were illegal.[42] EPIC previously reported on one of these other agency programs: "On October 3, 2011, the FISC ruled that the NSA 'upstream collection' of Internet communications violated the Fourth Amendment and the FISA. Specifically, the targeting and minimization procedures adopted by the NSA were not sufficient to protect the significant number (more than 50,000 per year) of wholly domestic communications obtained via 'upstream collection.'"[43] Courts have already imposed new restrictions on these narrower surveillance programs conducted under

[39] *Id*.
[40] *Id.*
[41] EPIC 2014 PCLOB Statement, *supra*, at 3.
[42] *See ACLU v. Clapper*, ___ F.3d ___, 2015 WL 2097814 (2d Cir 2015).
[43] EPIC, Foreign Intelligence Surveillance Court, https://epic.org/privacy/terrorism/fisa/fisc.html (2015).

Congressional and Judicial oversight, and the much broader EO 12333 bulk collection programs present an even more pressing need for new oversight and limitations.

The privacy impact of these surveillance programs is not limited to the collection of the contents of U.S. persons' communications; the collection of metadata can be even more intrusive. In an *amicus curiae* brief in the U.S. Court of Appeals for the Ninth Circuit, EPIC emphasized that "Analysis of large metadata sets equivalent to those created by the NSA can reveal even more personal information including the identities of our friends and associates, the identities of our loved ones, and even our political, religious, or social affiliations."[44] EPIC stressed that "[a]ll metadata can be used to make inferences about our daily activities, but location data is particularly sensitive since it can uniquely identify individuals, reconstruct a person's movements across space and time, predict future movements, and determine social interactions and private associations."[45] Collection of metadata can be a massive invasion of privacy, especially if the procedures for collection are too expansive.

A. The Scope of NSA's EO 12333 Collection Programs

Former NSA Director General Keith Alexander declared in a prepared statement before the Senate Judiciary Committee that the "NSA conducts the majority of its SIGINT[46] activities solely pursuant to the authority provided by EO 12333."[47] While the agency does not discuss most of the sources and methods of SIGINT collection publicly, disclosures in recent years have

[44] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Thirty-Three Technical Experts and Legal Scholars in Support of Appellant at 21, Smith v. Obama, 14-35555 (D. Idaho Sept. 9, 2014), *available at* https://www.epic.org/amicus/fisa/215/smith/EPIC-Amicus-14-35555.pdf.
[45] *Id*.
[46] "SIGINT" stands for signals intelligence.
[47] *Continued Oversight of the Foreign Intelligence Surveillance Act: Hearing Before the S. Judiciary Comm.*, 113th Cong. 4 (2013) (statement of Gen. Keith Alexander, Dir., NSA), *available at* http://www.judiciary.senate.gov/imo/media/doc/10-2-13AlexanderTestimony.pdf.

exposed some details of the broad surveillance conducted under EO 12333. Under these programs, the NSA collects a broad range of U.S. Person ("USP") information.. These bulk collection programs also result in collection of a massive amount of communications and information unrelated to surveillance targets.

For example, NSA's MYSTIC program is capable of recording and storing all calls transmitted to or from a given country.[48] The MYSTIC program has been used to collect and store all of the audio from phone calls made in the Bahamas as well as an unnamed country for thirty days.[49] Under MYSTIC, the NSA also collected the associated metadata for all phone calls made in above countries as well as the metadata from Mexico, Kenya, and the Philippines.[50]

Using SOMALGET, a tool utilized by the MYSTIC program to help collect and store the audio content of conversations, the NSA is able to processes over 100 million call events per day.[51] SOMALGET can store and manage approximately five billion call events.[52] Using its retrospective retrieval ("RETRO") tool analysts in the NSA, as well as other undisclosed agencies, can listen to audio from phone calls that were not flagged as of interest at the time of the original conversation.[53]

---

[48] Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, Wash. Post (Mar. 18, 2013), http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html [hereinafter Gellman & Soltani, NSA Surveillance Program].
[49] Presentation Slides on SOMALGET, *available at* https://firstlook.org/theintercept/document/2014/05/19/somalget-memo/.
[50] Presentation Slides on MYSTIC Reports (Excluding Scalawag), *available at* https://www.documentcloud.org/documents/1164079-02may2013-sso.html; Presentation Slides on Black Budget, *available at* https://firstlook.org/theintercept/document/2014/05/19/black-budget/.
[51] Presentation Slides on SSO Dictionary Excerpt, *available at* https://firstlook.org/theintercept/document/2014/05/19/sso-dictionary-excerpt/.
[52] Presentation Slides on SOMALGET, *supra*.
[53] Gellman & Soltani, NSA Surveillance Program, *supra*.

The MYSTIC bulk collection program captures under EO 12333 information on every telephone call of an estimated 250 million residents in the four named countries.[54] An estimated five million U.S. citizens visit the Bahamas alone every year.[55] Because this bulk collection indiscriminately sweeps up all telephone calls in the Bahamas, USPs' phone calls' associated audio and metadata would necessarily be collected and stored under the MYSTIC program. Also some, if not the majority, of the foreign communications swept up are unrelated to any valid foreign intelligence target.

The NSA's programs under EO 12333 also include massive data collection from the links between Yahoo's and Google's internal data centers.[56] Under project MUSCULAR, a joint operation with the British Government Communications Headquarters ("GCHQ"), the NSA has specifically targeted U.S companies data center links for collection. MUSCULAR intercepts data, including e-mails and other private communications of users, that pass through the companies' internal networks en route to their overseas data centers.[57] These data centers are connected via fiber-optic cables, enabling synchronous storage of large amounts of corporate and user data all across the world. For instance, Yahoo is able to synchronize a Yahoo account holder's entire email archive from the U.S. to another data center across the world, and the NSA MUSCULAR program could capture those e-mail contents en route.

As of January 2013, the NSA sent millions of records a day to its Fort Meade headquarters that it collected from Yahoo's and Google's internal networks.[58] In December

[54] Ryan Deveraux, *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, The Intercept (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.
[55] *Id.*
[56] Gellman & Soltani, NSA Infiltrates Links, *supra.*
[57] *Id.*
[58] *Id.*

2012, over 181 million new records, including metadata, were processed and sent to Fort Meade.[59] The full extent of USP information collected under MUSCULAR is unknown. However, the bulk collection program would necessarily sweep up irrelevant and personal information from USP and non-targeted foreign person.

The NSA has also worked with GCHQ on another bulk collection program under EO 12333. The unnamed program intercepts address books from email and "buddy lists" from instant message services from non-US access points.[60] On average, NSA collects approximately a half million buddy lists and inboxes per day (over 180 million each year).[61] On January 10, 2012, NSA's Special Source Operations branch collected 444,743 email address books from Yahoo, 105,068 from Hotmail, 82,857 from Facebook, 33,697 from Gmail and 22,881 from other, unspecified providers.[62] At this rate, an estimated 250 million email address books are collected every year. At least one email address book the NSA collected contained multiple group emails lists, which led to the collection of "many hundreds or thousands" of contacts from a single collection source.[63]

Inevitably, this bulk collection program sweeps up Americans' contacts as well. When questioned by the Washington Post, two senior U.S. intelligence officials admitted as much.[64] They did not dispute that the program may have already swept in millions or tens of millions of

[59] *Id*.
[60] *Id*.
[61] Presentation Slides by Special Source Operations on Content Acquisition Optimization 4, *available at* http://apps.washingtonpost.com/g/page/world/the-nsas-overcollection-problem/517/.
[62] *Id*. at 3.
[63] *Id*. at 6.
[64] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, Wash. Post (Oct. 14, 2013), http://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 [hereinafter Gellman & Soltani, NSA Collects Millions].

American's contacts.[65] One official went on to state that any information collected from "the overseas collection apparatus" is presumed not to be from a USP.[66] This raises significant privacy concerns for USPs, as address books contain sensitive data, such as telephone numbers, street addresses, business information, family association, names and email addresses. The U.S. service providers have stated that they were unaware of NSA's mass interception and collection of their customers' contact lists.[67]

The NSA is also collecting trillions of device-location records in another large database known as FASCIA.[68] According to at least one source, the NSA has collected and stored more than 27 terabytes of location data.[69] The agency's information intake is so voluminous that it has far outpaced the NSA's "ability to ingest, process, and store" data according to a May 2012 internal NSA briefing.[70] An anonymous NSA senior collection manager has stated that the agency is collecting the location data by tapping into cables connecting mobile networks worldwide.[71] These cables serve both U.S. and foreign cell phones.[72] Tens of millions of records of USPs movements are also collected every year as they travel internationally with their cell

[65] *Id.*
[66] *Id.*
[67] *Id.*
[68] Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, Wash. Post (Dec. 4, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html [herenafter Gellman & Soltani, NSA Tracking Cellphone Locations].
[69] *Id.*
[70] *Id.*
[71] *Id.*
[72] *Id.*

phones.[73] The cell phone location data can be aggregated overtime to create a very detailed picture of a cell phone's owner's life, habits, and associations.[74]

Some have argued that the "scale, scope and potential impact on privacy" of location data collection and analysis is "unsurpassed" among NSA surveillance programs revealed between June and December 2013, which includes project MUSCULAR and the collection of contact lists.[75] Yet under Section 4.7 in NSA's United States Signals Intelligence Directives ("USSID") SP0018, the agency did not consider "direction finding" for a transmitter located outside of the U.S. to be a collection under EO 12333.[76] Thus, five billion cell phone location records a day,[77] from at least hundreds of millions of devices,[78] are not subject to internal EO 12333 procedural collection or minimization restraints.

[73] *Id.*
[74] Brief of Amici Curiae Electronic Privacy Information Center (EPIC) and Thirty-Three Technical Experts and Legal Scholars in Support of Appellant at 20–26, Smith v. Obama, No. 14-35555 (D. Idaho Sept. 9, 2014), *available at* https://www.epic.org/amicus/fisa/215/smith/EPIC-Amicus-14-35555.pdf [hereinafter EPIC Amicus Brief in Smith v. Obama].
[75] Gellman & Soltani, NSA Tracking Cellphone Locations, *supra*.
[76] USSID SP0018: Legal Compliance and U.S. Person Minimization Procedures, § 4.7 (Nat'l Sec. Agency Jan. 2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf [hereinafter USSID 18 (2011)]; *but cf.* USSID SP0018: Nat'l Sec. Agency, *Supplemental Procedures for the Collection, Processing, Retention, and Dissemination of Signals Intelligence Information and Data Containing Personal Information of Non-United States Persons* 6, (Jan. 12, 2015), *available at* http://www.dni.gov/files/documents/ppd-28/NSA.pdf [hereinafter USSID 18 (2015)] (The most recent supplement to USSID SP0018 lacks any reference to direction finding.).
[77] Presentation Slides of FASCIA: The NSA's Huge Trove of Location Records, *available at* http://apps.washingtonpost.com/g/page/world/what-is-fascia/637/.
[78] Gellman & Soltani, NSA Tracking Cellphone Locations, *supra*.

B. Recommendations for Limiting Collection of USP and Other Non-target Data Under EO 12333

1. Collection should be uniformly defined as the acquisition of information

There is no consistent interpretation as to what "collection" means under EO 12333. Each sub-agency has its own definition of "collection" published in its internal policies and procedures. Many of these definitions are not made public. As a result, it is difficult for the public to understand what the extent and limitations of the NSA's and CIA's collection programs are. For example, under EO 12333 the Department of Defense ("DoD") states that "[i]nformation shall be considered as 'collected' only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties . . . . Data acquired by electronic means is 'collected' only when it has been processed into intelligible form."[79] The NSA's definition differs under its USSID SP0018 internal guidelines. Under USSID SP0018, information is "collected" when "intentionally intercepted, or selected through the use of a selection term," with various exceptions.[80] The CIA does not define its "collection" interpretation in its publicly available policies and procedures.[81]

Both of these "collection" interpretations leave a large gap in which USPs' and non-targeted foreigners' data may be gathered and stored in information systems under EO 12333. As

[79] Dep't of Defense, DoD 5240.1-R C2.2.1 (1982), *available at* http://biotech.law.lsu.edu/blaw/dodd/corres/pdf/52401r_1282/p52401r.pdf; *but see* Memorandum from John P. Pede, Dir. for Def. Intelligence, Dep't of Def. to Sec'ys of the Military Dep'ts 2 (Jan. 26, 2015), *available at* http://www.dni.gov/files/documents/ppd-28/DoD.pdf (DoD stated that NSA's new USSID SP0018 "supplemental procedures apply to all DoD IC elements and govern the SIGINT activities undertaken by DoD IC elements," although it also noted that each agency should review and update "their existing policies and procedures.").

[80] USSID 18 (2011), *supra*, § 4.1.

[81] Central Intelligence Agency, Policy and Procedures for Signals Intelligence Activities, *available at* https://www.cia.gov/library/reports/Policy-and-Procedures-for-CIA-Signals-Intelligence-Activities.pdf; *see also* Cent. Intelligence Agency: Recent Reports, available at https://www.cia.gov/library/reports/ (The

detailed above, millions of persons have personal information collected by the NSA everyday that is of no value to NSA's national security efforts. This raises significant privacy concerns. Congress has found that collection of personal private information endangers citizens' rights to due process and other legal protections.[82] Congress enacted the Privacy Act of 1974 specifically to safeguard U.S. citizens' privacy from improper collection and use by federal agencies.[83]

Moreover, the public has a difficult time addressing privacy concerns highlighted by Congress when the interpretation of keywords within text of EO 12333 vary by agency and are often not disclosed. When Director National Intelligence James Clapper compared NSA's acquisition of data to a library, he analogized opening up and reading the books as "collection."[84] But as security technologist Bruce Schneier has noted, the average person considers the library acquiring the books themselves as its collection—the library's collection does not grow simply because a patron selected a book from the shelf.[85] The agency's use of the term "collection" does not match the everyday definition. This stymies public understanding and debate on the IC agencies' collection operations.

As noted by HEW's Secretary's Advisory Committee on Automated Personal Data Systems, upon which the Privacy Act was based, "[t]here must be no personal-data record-

---

CIA published detailed minimization procedures used under Section 702 of the Foreign Intelligence Surveillance Act of 1979 but notably failed to produce similarly detailed collection or minimization guidelines for information collected under EO 12333 to the public.).

[82] The Privacy Act of 1974, Pub. L. 93-579, § 2, 88 Stat. 1896 (Dec. 31, 1974).

[83] *Id*.

[84] Director James R. Clapper Interview with Andrea Mitchell, NBC (June 8, 2013 1 P.M.), *available at* http://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/874-director-james-r-clapper-interview-with-andrea-mitchell.

[85] Bruce Schneier, *NSA Robots are 'Collecting' Your Data, Too, and They're Getting Away With It*, The Guardian (Feb. 27, 2014), http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier.

keeping systems whose very existences is secret."[86] Yet IC agencies operate secret programs such as MYSTIC and MUSCULAR. These bulk collection programs incidentally acquire terabytes of personal information not subject to Privacy Act safeguards or even EO 12333's collection, minimization, or retention procedures. This gap would be closed if "collection" under EO 12333 was uniformly interpreted to mean acquisition of information, the common definition of the word.

2. All categories of information collected should be equally protected

All personal information collected on USP should be given the same protections. However, current EO 12333 procedures treat different categories of data differently. Radio direction-finding is specifically excluded under EO 12333's definition of electronic surveillance and not subject to EO 12333.[87] The rules do not address whether global positioning systems ("GPS") or metadata are similarly excluded from "electronic surveillance."[88] This is a significant concern, as privacy interests are not limited to the content of communications. Importantly, metadata can also reveal intimate information about a person, as it can reveal her religion, political affiliation, habits, and associations.[89] Yet because categories of information are treated differently, certain sensitive data may not be subject to the agency's EO 12333 privacy policies.

[86] U.S. Dep't. of Health, Educ. and Welfare, Sec'y's Advisory Comm. on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens, at ix (1973) [hereinafter HEW Report].
[87] Exec. Order No. 12333, U.S. Intelligence Activities, 3 C.F.R. 200. (1981) as amended by Exec. Order 13,284, 68 Fed. Reg. 4,075 (Jan. 23, 2003), and by Exec. Order 13,355, and further amended by Exec. Order 13,470, 73 Fed. Reg. 45,328 (July 30, 2008) [hereinafter EO 12333].
[88] *Id*.
[89] EPIC Amicus Brief in *Smith v. Obama*, *supra*, at 21–22.

3. Agency guidelines and policies regarding EO 12333 collection should be made public

The updated signals intelligence principles stated in Presidential Policy Directive 28 ("PPD-28") are not sufficient to promote transparency about collection practices. PPD-28 requires the intelligence community to "safeguard[] personal information collected from signals intelligence activities."[90] The focus of PPD-28 was to protect information already collected (i.e. through dissemination and retention procedures) rather than to minimize the amount of information collected in the first place. The ongoing collection of innocent and irrelevant USP information and communications is a violation of the basic principles underlying the Privacy Act and EO 12333 itself, regardless of how the data is subsequently used. The Director of National Intelligence should require agencies to update and publicly release their data collection policies, especially as it applies to incidental collection of USP information.

In response to the PPD-28, the intelligence community members prepared reports that did not sufficiently inform the public about their data collection policies. Some agencies did not disclose collection policies at all. The FBI and Coast Guard wrote that it would "collect (including through clandestine means), analyze, produce, and disseminate foreign intelligence and counterintelligence."[91] This phrase is vague and does not reveal whether collection includes, for example, the use of specific identifiers or terms to narrow collection. Other agency reports imply that some collection guidelines are still hidden. The NSA wrote that "collection will be

[90] Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive (PPD)-28, at § 4(a) (Jan. 17, 2014) [hereinafter PPD-28 Press Release], *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[91] Presidential Policy Directive 28 Policies and Procedures, Fed. Bureau of Investigation 1 (2015), *available at* http://www.dni.gov/files/documents/ppd-28/FBI.pdf; Coast Guard Implementation of Presidential Policy Directive/PPD-28—Policies and Procedures, Coast Guard 2 (2015), *available at* http://www.dni.gov/files/documents/ppd-28/Coast%20Guard.pdf.

handled in accordance with these procedures and USSID SP0018, including its Annexes."[92] However, the Annexes are not released, though they may provide more detail as to how the NSA handles collection. A DoD document stated that the CSA, DIA, NGA, NRO, and NSA must update "their existing policies and procedures" to comply with PPD-28, but very little of these internal policies and procedures have been published.[93] The documents should be published, or more details given, to provide for more transparency and oversight about collection.

Some agency reports are also inconsistent in their definitions of collection, which detracts from transparency and oversight. It is unclear whether each agency simply has a different definition of "collection" or whether the uniform definition of collection simply is not public. Some agencies use selectors in the definition of collection while others do not. The CIA reported that "SIGINT collected in bulk - means the authorized collection of large quantities of signals intelligence data . . . acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."[94] On the other hand, the NSA stated that "[w]henever practicable, collection will occur through the use of one or more selection terms."[95] It is still unclear whether the definition of collection includes the use of selectors. In addition, the Coast Guard defines collection as not including processing, through the rule of surplusage (*i.e.* "collection" and "processing" in a list means that their definitions are not redundant and repetitive).[96] However, the DHS states that "[c]ollection means the gathering or receipt of information . . . coupled with an affirmative act

[92] USSID 18 (2015), *supra*, at 6.
[93] Memoranda for Director of National Intelligence, DoD Compliance with Section 4 of Presidential Policy Directive-28, "Signals Intelligence Committee" 2 (Jan. 20, 2015), *available at* http://www.dni.gov/files/documents/ppd-28/DoD.pdf.
[94] Signals Intelligence Activities, Central Intelligence Agency 1, *available at* http://www.dni.gov/files/documents/ppd-28/CIA.pdf.
[95] USSID 18 (2015), *supra*, at 6.
[96] Coast Guard Implementation of Presidential Policy Directive/PPD-28—Policies and Procedures, Coast Guard 2 (2015).

demonstrating intent to use or retain that information for intelligence purposes."[97] The DHS definition of collection appears to require an additional step beyond the NSA definition of collection. These policies should be made public and updated to provide for clarity and better oversight.

4. The government should only search U.S. persons' communications with a warrant or as necessary to prevent imminent harm

As noted above, some intelligence agencies only consider incidental information to be "collected" under EO 12333 when it has been selected via a search term. The NSA and CIA should improve their privacy protections for incidentally collected data by implementing the President's Review Group on Intelligence and Communications Technology's ("Review Group") Recommendation 12:

> We recommend that, if the government legally intercepts a communication under section 702, or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United States, and if the communication either includes a United States person as a participant or reveals information about a United States person:
>
> (1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others;
>
> (2) any information about the United States person may not be used in evidence in any proceeding against that United States person;
>
> (3) the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism. [98]

[97] Safeguarding Personal Information Collected from Signals Intelligence Activities, Department of Homeland Security 14 (Jan. 16, 2015), *available at* http://www.dni.gov/files/documents/ppd-28/DHS.pdf.
[98] President's Review Grp. on Intelligence and Commc'ns Techs., *Liberty and Security in a Changing World: Report and Recommendations* 28–29 (Dec. 12, 2013), *available at*

After a thorough review of various intelligence programs, the Review Group determined that the government should not be able to search (or "collect") any information in its databases about a USP.[99] Narrow exceptions to the search restriction apply when the search is necessary to prevent death or serious bodily harm or when the government obtains a warrant based on probable cause that the USP is planning or engaged in international terrorism.[100] A member of the Review Group confirmed that Recommendation 12 was specifically written with EO 12333 in mind, and White House staffers reported that they interpreted it as such.[101] Although the President declined at the time to adopt Recommendation 12, that stance should be changed.

As EPIC has previously stated, when collecting foreign intelligence, the U.S. "should acquire and monitor communications, personal information, metadata and other personal and sensitive data only when the information is necessary for the protection of specifically articulated U.S. national security interests, and only in a manner that produces the least intrusion on rights necessary to secure those interests."[102] Limiting searches of USPs' acquired data to specific and limited reasons will reconcile President's recent PPD-28 with the agencies' current interpretations of EO 12333. In PPD-28, the President stated that all SIGINT activities "must take into account that all persons should be treated with dignity and respect, regardless of their

---

http://www.scribd.com/doc/192387819/NSA-review-board-s-report [hereinafter President's Review Group Report].

[99] *Id*.

[100] *Id*.

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

[102] Joint Submission by EPIC, et al., National Security Surveillance and Human Rights in a Digital Age: U.S.A., to the United Nations 13, (Apr.–May 2015), *available at* https://epic.org/privacy/intl/Joint-UPR-Submission-to-UN-HRC.pdf

nationality or wherever they might reside."[103] Restricting NSA's ability to search incidentally collected data also fulfills the requirements set out in EO 12333 that intelligence agencies "use the least intrusive collection techniques feasible within the United States or directed at U.S. persons abroad."[104] As NSA can still search the incidentally collected information with a warrant or under the exception of a threat of serious harm, allowing it to search through the sensitive information for any other reasons does not meet the "least intrusive" standard.

C. Questions the PCLOB Should Ask As Part of Its Inquiry Into the NSA and CIA's Collection Programs

EPIC proposes several questions that the PCLOB should ask as part of its inquiry into the NSA and CIA collection programs:

- To what extent is information on USPs is captured by surveillance conducted under EO 12333?
- What changes have the CIA and NSA made to their policies and regulations in response to PPD-28?
- How do agencies ensure that they are complying with EO 12333 in using the "least intrusive collection techniques feasible within the United States or directed at U.S. persons abroad"?
- To what extent is the NSA or CIA collaborating with foreign countries in the collection of USPs data?
- How is "foreign intelligence" defined? Is it consistent throughout all agencies?

II. The NSA and CIA Do Not Adequately Protect the Sensitive Personal Information Collected Under EO 12333

[103] PPD-28 Press Release, *supra*.
[104] EO 12333.

As a result of surveillance operations carried out under EO 12333, the NSA, CIA, and other IC agencies collect massive amounts of sensitive personal information about USPs and other foreign individuals with no connection to international terrorism or any other national security threat. In most cases, agencies store this data for at least five years—or longer, if continued retention "is in the national security interest of the United States."[105] This long-term data retention is especially alarming in the case of EO 12333, which permits some forms of USP information to be used and shared "without any order from a judge or oversight from Congress."[106] IC agencies do not currently have sufficient privacy and accountability mechanisms to ensure that this sensitive personal information is properly minimized, and that it is only disseminated as far as is strictly necessary to serve the foreign intelligence purpose.

As the White House has acknowledged, there is a need for greater transparency and tighter controls on the use, retention, and dissemination of data obtained under authorities like EO 12333. In January 2014, President Obama announced his intention to "reform programs and procedures in place to provide greater transparency to our surveillance activities, and [to] fortify the safeguards that protect the privacy of U.S. persons."[107] Presidential Policy Directive 28 ("PPD-28"), released at the same time, instructed agencies in the Intelligence Community to

[105] Nat'l Sec. Agency Dir. of Civil Liberties and Privacy Office, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333* 14 (2014), *available at* https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf.
[106] *See* EPIC 2014 PCLOB Statement, *supra*, at 3.
[107] Barack Obama, President of the U.S., Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence [hereinafter Obama January 2014 Remarks]..

"establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information collected from signals intelligence activities.[108]

Making good on these commitments is both critical as a matter of policy and required as a matter of law. The Code Fair Information Practices ("FIPs"), established in 1973 by Secretary's Advisory Committee on Automated Personal Data Systems, calls on institutions to tightly regulate their retention, use, and dissemination of personally identifiable information ("PII"). The Privacy Act of 1974, to which the NSA is subject,[109] essentially codified the committee's recommendations,[110] promoting "accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems data of the Federal Government."[111] Subsequent formulations of FIPs, including those issued by the White House, have been even more explicit in imposing data handling requirements on public and private entities alike.[112]

[108] Presidential Policy Directive/PPD-28, 2014 Daily Comp. Pres. Doc. 31 (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28].
[109] *See* 5 U.S.C. § 552a(a)(1).
[110] HEW Report, *supra*, at 40–41.
[111] S. Rep. No. 93-1183, at 1 (1974).
[112] *See, e.g.*, Nat'l Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy 45 app. A (2011), *available at* http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

A. Recommendations

1. Agencies should publicly disclose rules regarding minimization, dissemination, and retention of data collected under EO 12333

Transparency is a key component of a functioning, healthy democracy.[113] The need for transparency is particularly acute where, as with EO 12333, the federal government is engaged in the mass collection and retention of PII—including data from USPs.[114]

This principle of transparency is enshrined in the Privacy Act, which requires that each agency publish "notice of any new use or intended use" of identifying information contained in its "system[s] of records."[115] It further requires that the agency "provide an opportunity for interested persons to submit written data, views, or arguments" about such planned uses.[116] As an "agency" under the Privacy Act,[117] the NSA is subject to these transparency mandates. Its use of data collected under EO 12333 is no exception.

The White House has underscored the need for transparency in this arena, as well. As discussed above, President Obama announced his commitment to greater transparency of surveillance activities.[118] Additionally, the President directed the Intelligence Community to establish privacy protecting policies and minimization procedures.[119] These polices and procedures were to be "publicly released to the maximum extent possible, consistent with classification requirements."[120]

---

[113] Lillie Coney, Associate Director, EPIC, Statement to the 2007 Post Election Audit Summit 2 (Oct. 26, 2007), *available at* https://epic.org/epic/staff/coney/audit.pdf.
[114] *See* EPIC 2014 PCLOB Statement, *supra*, at 3.
[115] 5 U.S.C. § 552a(e)(11).
[116] *Id.*
[117] 5 U.S.C. § 552a(a)(1).
[118] Obama January 2014 Remarks, *supra*.
[119] PPD-28.
[120] *Id.*

The basic pillars of data privacy impose comparable transparency obligations. For example, the Privacy Guidelines of the Organization for Economic Co-operation and Development call on data controllers—government or otherwise—to adopt a "general policy of openness about developments, practices and policies with respect to personal data." Similarly, the Fair Information Practices set forth by the Secretary's Advisory Committee on Automated Personal Data Systems prescribe (1) that "there must be a way for an individual to find out" how information collected about her is used, and (2) that there must be a way for an individual to prevent information "obtained for one purpose from being used or made available for other purposes" without her consent.[121] The data collected under EO 12333 should be held to these same standards.

In view of the above, the Board should ensure that the NSA, the CIA, and any other entity collecting data pursuant to EO 12333 publicly disclose detailed polices and procedures for retaining, minimizing, using, and disseminating that data. Though both the NSA and CIA have released bare-bones descriptions of their data handling policies and procedures,[122] these documents are much too brief and superficial to assess the strength of the agencies' privacy safeguards.[123] Greater transparency is required so that the public may "evaluate the degree to which its privacy is currently protected . . . ."[124]

---

[121] HEW Report, *supra*, at 40-41.
[122] *See generally* Nat'l Sec. Agency, PPD-28 Section 4 Procedures (2015), *available at* http://www.dni.gov/files/documents/ppd-28/NSA.pdf; Cent. Intelligence Agency, Signals Intelligence Activities (2015), *available at* http://www.dni.gov/files/documents/ppd-28/CIA.pdf.
[123] *See, e.g.*, Cent. Intelligence Agency, Signals Intelligence Activities (2015), *available at* http://www.dni.gov/files/documents/ppd-28/CIA.pdf (stating cursorily that "[t]he Agency shall establish policies and procedures reasonably designed to minimize the retention and dissemination of personal information acquired through SIGINT activities").
[124] *See* Letter from Media Freedom and Info. Access Practicum to Mary Ellen Callahan, Chief Privacy Officer, Dep't. of Homeland Sec. (Dec. 15, 2010), *available at* https://epic.org/privacy/fusion/MFIA_FusionCenters_CommentFinal.pdf.

2. Agencies should use robust privacy enhancing techniques to minimize the retention of personally identifiable information

There is a broad consensus on the need to minimize data collected under EO 12333, particularly when that data concerns USPs. Congress, legislating through the Privacy Act, has mandated that any agency that collects identifying records about USPs maintain "only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[125]

President Obama has specifically highlighted the importance of data minimization in an intelligence-gathering context. PPD 28 requires that agencies in the IC "establish policies and procedures reasonably designed to minimize the dissemination and retention of personal information," noting that "long-term storage of personal information unnecessary to protect our national security is inefficient, unnecessary, and raises legitimate privacy concerns."[126] The President's Review Group on Intelligence and Communications Technologies has similarly advised that if an intercepted communication "includes a United States person as a participant or reveals information about a United States person . . . any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others."[127]

Even the NSA has acknowledged the risks of failing to use minimization procedures. Overbroad retention of data means that the agency "may possibly fail to completely remove data [it] was not authorized to acquire" and "may potentially lose data because of 'spillage,' improper

[125] 5 U.S.C. § 552a(e)(1).
[126] PPD-28.
[127] President's Review Group Report, *supra*, at 145-46.

intentional disclosure, or malicious exfiltration."[128] The subsequent dissemination of improperly retained data means that the agency "could inappropriately share information that does not have a foreign intelligence purpose, or is based on data that is required to be removed" and "may possibly disseminate more information than is relevant to foreign intelligence."[129]

These concerns have long been reflected in the basic tenets of data privacy. In 1977, the Privacy Protection Study Commission—drawing on the Code of Fair Information Practices—urged that there be limits "on the internal uses of information about an individual within a record-keeping organization" and "on the external disclosures of information about an individual . . . ."[130] The National Strategy for Trusted Identities in Cyberspace echoed this in a 2011 report, announcing a "Data Minimization" principle: "Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s)."[131]

In view of the above, the Board should ensure that the NSA, the CIA, and any other entity collecting data pursuant to EO 12333 minimize the retention of PII by using robust privacy enhancing techniques. Such measures are necessary "to ensure that information belonging to both U.S. and non-U.S. persons is used, retained and disseminated only when necessary for the

[128] Nat'l Sec. Agency Dir. of Civil Liberties and Privacy Office, *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333* 14 (2014), *available at* https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf [hereinafter NSA CPLO Report].
[129] *Id*. at 16.
[130] Privacy Protection Study Comm'n, Protecting Privacy in an Information Society 501–02 (1977), *available at* https://epic.org/privacy/ppsc1977report/.
[131] Nat'l Strategy for Trusted Identities in Cyberspace, Enhancing Online Choice, Efficiency, Security, and Privacy 45 app. A (2011).

protection of specifically articulated U.S. national security interests and in a manner that produces the least intrusion on rights necessary to secure those interests."[132]

3. Data collected Under EO 12333 should only be retained as long as strictly necessary to serve the purpose of collection

In general, targeted data collection under EO 12333 that is unenciphered is retained for up to five years unless "there is a determination that continued retention is in the national security interest of the United States."[133] However, there are significant civil liberties and privacy risks inherent to storing sensitive PII, such as: 1) "retain[ing] data that is no longer authorized to retain;" (2) "fail[ing] to completely remove data the Agency was not authorized to acquire;" and (3) "potentially los[ing] data because of 'spillage,' improper intentional disclosure, or malicious exfiltration."[134] Therefore, EO 12333 collected data should be retained only as long as strictly necessary, protected against breaches, and promptly deleted when necessary.

Data collected through EO 12333 should only be retained strictly for length of time as required by law. PPD 28 acknowledges the importance of limiting the length of time that data is maintained:

> Personal information shall be retained only if the retention of comparable information concerning U.S. persons would be permitted under section 2.3 of EO 12333 and shall be subject to the same retention periods as applied to comparable information concerning U.S. persons. Information for which no such determination has been made shall not be retained for more than 5 years, unless the DNI expressly determines that continued retention is in the national security interests of the United States.[135]

---

[132] EPIC et al., *National Security Surveillance and Human Rights in a Digital Age* (2015), *available at* https://epic.org/privacy/intl/Joint-UPR-Submission-to-UN-HRC.pdf.
[133] NSA CLPO Report, *supra*.
[134] *Id*.
[135] PPD-28 Press Release, *supra*.

However, despite the call for strict retention requirements, the broad exception that allows data to be retained for longer than 5 years if the "DNI expressly determines that continued retention is in the interest of national security"[136] gives agencies a "broad based rationale" for maintaining records on individuals.[137] Additionally, encrypted communications may be retained for "any period of time during The NCTC even has the authority to permanently retain "United States person information that is reasonably believed to constitute terrorism information."[138] This indefinite retention has the potential to be misused and violate the Privacy Act's goal to "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, … and that adequate safeguards are provided to prevent misuse of such information . . ."[139]

Secondly, the agencies should take extreme measures to ensure that data collected under EO 12333 is secure, and that information is "stored under conditions that provide adequate protection and prevent access by unauthorized persons,"[140] intentional disclosures, or cyber security hacks.

This need for increased minimization and data security is especially acute in light of the federal government's inability to protect sensitive personal information. Just this month, the Office of Personnel Management announced a massive data breach in the federal government's employee database that resulted exposure of sensitive personal information for 4 million

[136] *Id.*
[137] Comments, EPIC, to Subcomm. on Oversight of Gov. Mgmt, the Fed. Workforce, and D.C., on "S. 1732, the Privacy Act Modernization for the Information Age Act of 2011" 3 (Mar. 27, 2012), *available at* https://epic.org/privacy/1974act/EPIC-on-S-1732-Privacy-Act-Modernization.pdf [hereinafter EPIC Comments on Privacy Act Modernization].
[138] Nat'l Counterterrorism Cen., *Guidelines for Access, Retention, Use, and Dissemination* 9 (2012), *available at* https://epic.org/foia/odni/nctc-guidelines.pdf.
[139] The Privacy Act of 1974, Pub. L. 93–579, § 2, 88 Stat. 1896 (Dec. 31, 1974).
[140] PPD-28 Press Release.

government employees.[141] Such failures in the protection of its own employees create serious concerns about the protection of US Persons information being retained under surveillance programs.

Finally, agencies should ensure the prompt deletion—once discovered—of any 12333-intercepted communication in which (a) a United States person is a participant, or (b) information is revealed about a United States person, unless it is directly relevant to a specific, authorized national security/terrorism investigation or is necessary to prevent serious harm to others.

The President's Review Group on Intelligence and Communication Technologies recommended that "if the communication either includes a United States person as a participant or reveals information about a United States person: (1) any information about that United States person should be purged upon detection unless it either has foreign intelligence value or is necessary to prevent serious harm to others."[142] Furthermore, "broad data retention requirements impose not only expensive technical compliance burdens, but also may jeopardize the speed and accuracy of investigations."[143]

These recommendations will ensure that agencies are protecting Americans data under EO 12333 from unnecessary retention and aligning the program with the requirements under the Privacy Act.

---

[141] Press Release, Office of Personal Management, *OPM to Notify Employees of Cybersecurity Incident* (June 4, 2015) http://www.opm.gov/news/releases/2015/06/opm-to-notify-employees-of-cybersecurity-incident/.
[142] President's Review Group Report, *supra*, at 145-46.
[143] *The Protecting Children from Internet Pornographers Act of 2011, Hearing on H.R. 1981 Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. at 5 (2011) (Testimony of Marc Rotenberg, Exec. Dir., EPIC, Adjunct Prof., Georgetown Univ. Law Ctr.), *available at* https://epic.org/privacy/testimony/EPIC_Data_Retention_Testimony_FINAL.pdf.

4. Dissemination of incidentally collected data on U.S. persons should be limited to necessary and lawful purposes

Given the global nature of communications, the indiscriminate mass surveillance the NSA conducts overseas under EO 12333 captures the information of millions of United States Persons.[144] The government can use and share this information without any order from a judge or oversight from Congress.[145] Furthermore, the huge amounts of data captured through EO 12333 mass surveillance is unrelated to the mission of national security.[146] The transfer of this USP data between government agencies disregards important Privacy Act principles, which harms the interests of innocent Americans.[147]

The Privacy Act of 1974 provides a sound framework for privacy protections in the U.S. With the Privacy Act, Congress sought to ensure that federal agencies "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information."[148] Similarly, the dissemination of data collected through EO 12333 should be protected from misuse. Specifically, data collected through EO 12333 should only be disseminated when there is a clear, legal purpose, and data should be protected from parallel construction and warrantless backdoor searches.

[144] EPIC 2014 PCLOB Statement, *supra*.
[145] *Id*.
[146] *Id*.
[147] *See* EPIC Comments on Privacy Act Modernization, *supra*.
[148] The Privacy Act of 1974, Pub. L. 93–579, § 2, 88 Stat. 1896 (Dec. 31, 1974).

PCLOB should ensure that any information derived from 12333 intercepts is not shared with other agencies, governments, or entities except in direct furtherance of a specific, authorized national security/terrorism investigation.

The Presidential Policy Directive 28 (PPD 28) discusses the need for the IC to create safeguards to minimize the dissemination of personal information collected from EO 12333.[149] PPD 28 prescribes that "Personal information shall be disseminated only if the dissemination of comparable information concerning U.S. persons would be permitted under 2.3 of Executive Order 12333."[150] Similar concerns of proper dissemination were highlighted in the NSA Director of Civil Liberties and Privacy Office (CLPO) Report in 2014, in which it described the risks associated with dissemination: "(1) NSA could inappropriately share information that does not have a foreign intelligence purpose, or is based on data that is required to be removed; or (2) NSA may possibly disseminate more information than is relevant to foreign intelligence."[151]

Indeed, the 2012 AG-DNI Guidelines permit the National Counterterrorism Center ("NCTC") to "*access* or *acquire* US Person information for the purpose of determining whether the information is *reasonably believed* to constitute terrorism information."[152] The NCTC has the ability to disseminate U.S. Person information if it "reasonably appears" to be terrorism information or "necessary to understand or access" terrorism information.[153] Further, the NCTC

[149] PPD-28 Press Release.
[150] *Id.*
[151] CLPO Report, *supra*, at 18.
[152] Nat'l Counterterrorism Ctr., NCTC Guidelines: Understanding Acquisition, Retention, and Dissemination of USP Information and Other Issues in EO 12333, *available at* https://epic.org/foia/odni/File-1-2.pdf.
[153] *Id.*

can disseminate non-TI "for a limited purpose (to access if TI)," which includes a dissemination of "a bulk dataset or significant portion" but only after consulting with ISPPO and Legal.[154] However, these loose standards have failed to provide meaningful privacy protection in the past. The PCLOB Report on the Telephone Records Program describes how calling detail records analyzed by the NSA were made available to the FBI without application of the legally mandated minimization rules.[155] Data collected under EO 12333 is susceptible to the same risks, and strict procedures should be enforced to ensure that data is only shared with other parties for a legal and authorized purpose.

PCLOB should ensure that information derived from 12333 intercepts is not used by any agency to bootstrap a non-national security/terrorism investigation (*i.e.,* parallel construction) and warrantless backdoor searches.

Further reforms should be implemented to provide Americans with greater safeguards against intrusion into their personal domain against unwarranted use access to incidentally collected data. As it stands, the government can use and share information obtained through EO 12333 without any order from a judge.[156] The threat to "public trust, personal privacy, and civil liberty" by warrantless searches and parallel construction has been noted by the President's Review Group on Intelligence and Communications Technologies.[157] Recommendation 12 of the report explicitly advocates for protections against these practices by stating that "any information

[154] *Id.*
[155] Privacy and Civil Liberties Oversight Bd., *Report of the Telephone Records Program Conducted under Section 215 of the USA Patriot Act of FISA Court* 87–91 (2014), *available at* https://www.emptywheel.net/wp-content/uploads/2014/01/140123-PCLOB.pdf.
[156] EPIC 2014 PCLOB Statement, *supra*, at 3.
[157] President's Review Group Report, *supra*, at 17-18.

about United States person *may not be used in evidence in any proceeding against that United States person* . . ." and:

> [T]he government may not search the contents of communications acquired . . . under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) *when the government obtains a warrant based on probable cause* to believe that the United States person is planning or is engaged in acts of international terrorism.[158]

The report explains that the "government cannot lawfully target the communications of a United States person, whether she is inside or outside the United States without satisfying the probable cause requirements of . . . the Fourth Amendment."[159] Furthermore it states, that the concern is exacerbated with "incidental interception" that occurs when the government engages in electronic surveillance.[160]

Use of USP data inadvertently collected under EO 12333 in criminal matters and without a warrant violates American's constitutional rights. EPIC Advisory Board member and national security law expert Laura Donohue analogously describes how under Section 702, "NSA's minimization procedures place a duty on the NSA to turn over any information regarding the commission of a crime to law enforcement agencies," and "used against them in a court of law, without law enforcement ever satisfying Title III requirements."[161] Professor Donohue cautions that, "query of databases using U.S. person identifiers may further implicate U.S. persons in criminal activity—even acts unrelated to national security. But no individualized judicial process

[158] *Id.* at 29 (emphasis added).
[159] *Id*. at 147.
[160] *Id.*
[161] Laura K. Donohue, Section 702 and the Collection of International Telephone and Internet Content, 38 Harv. J. L. & Pub. Pol'y 117, 202 (2015).

is required."[162] The broad dissemination procedure under EO 12333 similarly "falls outside of constitutional boundaries."[163]

As the Chief Justice recently explained, "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search of evidence of criminal activity."[164] Broad dissemination procedures that fail to follow strict rules violates American's constitutional rights, and broad goals set out by Congress in the Privacy Act.

B. Questions to Consider

- How do minimization procedures apply to encrypted data?
- How are the IC agencies implementing PPD-28, and what mechanisms are in place to ensure that PII is properly minimized?
- Are the same minimization rules applied to USP and foreign PII?
- Can data collected under EO 12333 be used in criminal proceedings?
- What percentage of data collected under EO 12333 is not related to any valid intelligence target?
- Are there any guidelines the DNI must consider when deciding to extend the retention period beyond 5 years?
- If data is retained beyond 5 years, what procedures are in place to ensure that data is purged when it is no longer needed?
- What auditing procedures are in place to ensure data security?

[162] *Id.*
[163] *Id.* at 206.
[164] *Riley v. California*, 134 S. Ct. 2473, 2494 (2014).

III. EO 12333 Surveillance Activities Warrant Improved Oversight and Increased Transparency

For over two hundred years, the American people have proudly and properly maintained a healthy skepticism of their government.[165] Correspondingly, an independent judiciary was established to ensure meaningful oversight of the law making and enforcement branches of our government.[166] However, EO 12333[167] effectively evades both public and judicial scrutiny.[168] While there are minimal reporting requirements for violations of the authority, the secrecy of activities conducted under EO 12333 makes evaluation of those activities—their legality, purpose, scope, and effectiveness—nearly impossible.

In 2009, President Barack Obama issued a memorandum to the heads of executive departments and agencies emphasizing the importance of transparency and open government in order to "strengthen our democracy," "promote efficiency and effectiveness in Government," and "ensure the public trust."[169] In 2014, President Obama issued Presidential Policy Directive 28,[170] laying out for the public the government's principles and doctrines of surveillance, an act in and of itself in favor of transparency. In February of this year, the President again lauded

[165] Technology and Privacy Advisory Comm., Safeguarding Privacy in the Fight Against Terrorism 54 (2004), *available at* https://epic.org/privacy/profiling/tia/tapac_report.pdf.
[166] Prepared Testimony and Statement for the Record of Marc Rotenberg, President, EPIC, Hearing on "Security and Liberty: Protecting Privacy, Preventing Terrorism," before the Nat'l Comm. on Terrorist Attacks Upon the U.S. 15 (Dec. 8, 2003), *available at* https://epic.org/privacy/terrorism/911commtest.pdf ("New surveillance authorities require corresponding means of public oversight and accountability. A strong and independent judiciary as well as extensive public reporting is critical for this purpose.").
[167] EO 12333.
[168] EPIC 2014 PCLOB Statement.
[169] Memorandum from Barack Obama, President, U.S., to the Heads of Executive Departments and Agencies, "Transparency and Open Government," 2009, *available at* https://www.whitehouse.gov/the_press_office/TransparencyandOpenGovernment/.
[170] Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive (PPD)-28, at § 4 (Jan. 17, 2014) [hereinafter PPD-28], *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

transparency when he stated, "technology so often outstrips whatever rules and structures and standards have been put in place, which means that government has to be constantly self-critical and we have to be able to have an open debate about it."[171] Yet, this very month, the Obama administration, without debate or public notice, expanded the National Security Agency's (NSA's) warrantless surveillance of Americans' international internet traffic to search for evidence of computer hacking.[172] It is precisely this type of "gradual and silent encroachment" that our the founders warned would lead to greater "abridgement of the freedom of the people" than by "violent and sudden usurpations."[173]

Potentially unlawful mass surveillance conducted under secret authority is not a phenomenon of the current presidency. In December 2005, the New York Times reported that President George W. Bush secretly issued an executive order in 2002 authorizing the NSA to conduct warrantless surveillance of international telephone and Internet communications on American soil.[174] EPIC submitted FOIA requests to the NSA just hours after the existence of the warrantless surveillance program was first reported.[175] However, not until September of 2014—after a disregarded court order and persistent delay—did the NSA turn over responsive

[171] President Barack Obama, Remarks at the Cybersecurity and Consumer Protection Summit (Feb. 13, 2015), *available at* https://www.whitehouse.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit.
[172] Charlie Savage et al., *Hunting for Hackers, N.S.A. Secretly Expands Internet Spying at U.S. Border*, N.Y. Times (June 4, 2015), http://www.nytimes.com/2015/06/05/us/hunting-for-hackers-nsa-secretly-expands-internet-spying-at-us-border.html.
[173] James Madison, Speech in the Virginia Ratifying Convention on the Control of the Military (June 16, 1788), in The History of the Virginia Federal Convention of 1788, with Some Account by Eminent Virginians of That Era Who Were Members of That Body 130 (Hugh Blair Grigsby et al. eds., 1890).
[174] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers without Courts*, N.Y. Times, (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html.
[175] *EPIC v. DOJ - Warrantless Wiretapping Program*, https://epic.org/privacy/nsa/foia/#foia (2015).

documents.[176] These documents offer the fullest justification of the program to date, but parts of the legal analysis, including possibly contrary authority, were still withheld.

U.S. District Judge Henry H. Kennedy echoed the need for transparency in his 2006 order to the NSA writing, "EPIC correctly argues, 'a meaningful and truly democratic debate on the legality and propriety of the warrantless surveillance program cannot be based solely upon information that the Administration voluntarily chooses to disseminate.'"[177] This argument again holds true where even less is known about EO 12333, stifling the dialogue about the order's legality and scope before it can begin.

For similar reasons, secret legal authorities inherently thwart proactive oversight mechanisms. In 2014, EPIC obtained documents that reveal that the FISA Court sharply criticized the NSA's internet metadata program, but the Court's criticism was kept secret.[178] One document in particular illustrates how oversight in secret is no oversight at all: FISA Court Judge John Bates' chastisement of the NSA for "long-standing and pervasive violations of the prior [court] orders in [the] matter."[179] While the FISA Court first authorized the metadata program in 2004, documents obtained by EPIC show that the program's legal justification was not provided

[176] Memorandum from Jack L. Goldsmith, Assistant Attorney General, U.S., to Attorney General, Review of the Legality of the STELLAR WIND Program (OLC54) (May 6, 2004), *available at* https://www.epic.org/foia/doj/olc/OLC54-09-05-14-Plaintiff-Release.pdf; Memorandum from Jack L. Goldsmith, Assistant Attorney General, U.S., to Attorney General, U.S., STELLAR WIND—Implications of Hamdi v. Rumsfeld (OLC85) (July 17, 2004), *available at* https://www.epic.org/foia/doj/olc/OLC85-09-05-14-Plaintiff-Release.pdf.
[177] *EPIC v DOJ*, Nos. 06-00096 & 06-00214 at 16 n.9 (D.D.C. 2007) (order granting preliminary injunction), *available at* https://epic.org/privacy/nsa/pi_order.pdf.
[178] *EPIC v. DOJ—Pen Register Reports*, https://www.epic.org/foia/doj/pen-reg-trap-trace/ (2015).
[179] Memorandum Opinion, U.S. Foreign Intelligence Surveillance Court, *available at* https://epic.org/foia/doj/pen-reg-trap-trace/EPIC-FISA-PEN-REGISTER-FOIA-RELEASE-08082014-17.pdf.

to Congress until 2009.[180] The documents also reveal that the DOJ withheld information about the program in testimony for the Senate Intelligence hearing prior to the reauthorization of the legal authority.[181] The program was shut down in 2011 after a detailed review.[182] What little oversight may be exercised over EO 12333 activities is severely hampered by a near total lack of transparency about which activities or programs are even conducted under its authority.

Many agencies, including the CIA and NSA, have yet to align their activities conducted under EO 12333 with the Principles of Intelligence Transparency.[183] Following PCLOB's recommendation,[184] the Office of the Director of National Intelligence issued the Principles of Intelligence Transparency for the Intelligence Community.[185] In 2014, the NSA released a privacy report on its surveillance activities under EO 12333. According to the agency, due to the nature of EO 12333 surveillance activities, the NSA is not under the same obligation as other agencies to release information.[186] Meaningful oversight requires a certain threshold of information that cannot be met when an agency determines for itself what disclosures are

[180] Application for Use of Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes, U.S. Foreign Intelligence Surveillance Court, *available at* https://www.epic.org/foia/doj/pen-reg-trap-trace/EPIC-FISA-PEN-REGISTER-FOIA-RELEASE-08082014-2.pdf.
[181] Testimony of Alberto R. Gonzales, Attorney General, U.S., and Robert S. Mueller, III, Dir., Fed. Bureau of Investigation, before the Select Comm. on Intelligence, U.S. Senate (Apr. 27, 2005) https://www.epic.org/foia/doj/pen-reg-trap-trace/EPIC-FISA-PEN-REGISTER-FOIA-RELEASE-08082014-3.pdf.
[182] Pen Register/Trap and Trace Team, Pen Register/Trap and Trace FISA NSA Review, https://www.epic.org/foia/doj/pen-reg-trap-trace/EPIC-FISA-PEN-REGISTER-FOIA-RELEASE-08082014-33.pdf.
[183] Office of the Dir. of Nat'l Intelligence, *Principles of Intelligence Transparency for the Intelligence Community*, *available at* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles?tmpl=component&format=pdf [hereinafter ODNI Transparency Principles].
[184] Privacy and Civil Liberties Oversight Bd., Recommendations Assessment Report 14 (2015), *available at* https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.
[185] ODNI Transparency Principles, *supra.*
[186] Nat'l Security Agency Civil Liberties and Privacy Office, NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities Under Executive Order 12333 16 (2014), *available at* https://www.nsa.gov/civil_liberties/_files/nsa_clpo_report_targeted_EO12333.pdf.

appropriate and compliant. In other words, "[w]here the government is given new authorities to conduct surveillance, there should be new means of oversight. Based on what we have learned, it is clear that the system of oversight for the collection of foreign intelligence information has collapsed. There is no meaningful review."[187]

EO 12333 requires the Intelligence Community to report to the President's Intelligence Oversight Board (IOB), in a manner consistent with EO 13462, intelligence activities that the Intelligence Community has reason to believe may be unlawful or contrary to an executive order or presidential directive.[188] Further, the National Security Act of 1947 requires that Congress be kept "fully and currently informed" about "significant" intelligence activities.[189] However, because EO 12333 activities receive little oversight, the intelligence agencies are left to determine for themselves what "fully and currently informed" means and thus what information it must share with Congress. So while there exists a mechanism for oversight, the level of deference given to agencies to determine if they are acting within the lawful bounds of their authority renders the oversight meaningless. "There's no clear definition," said House Intelligence Committee member Adam Schiff, D-Calif., who discussed whether the NSA had briefed the committee on its monitoring of German Chancellor Angela Merkel's cellphone. "We need to have a bigger discussion of what our mutual understanding is of what we want to be

[187] Prepared Statement for the Record of Marc Rotenberg, President, EPIC, Workshop on Domestic Surveillance Programs Operated Under the USA PATRIOT Act and the Foreign Intelligence Surveillance Act, before the Privacy and Civil Liberties Oversight Bd. (July 9, 2013), *available at* https://www.epic.org/privacy/oversight/EPIC-PCLOB-Statement.pdf.
[188] EO 12333. *See also* NSA Core Intelligence Oversight Training, published 2013-11-19 ("The NSA General Counsel and Inspector General shall: a. Conduct appropriate oversight to identify and prevent violations of Executive Order 12333").
[189] National Security Act of 1947, Pub. L. No. 80-235, 61 Stat. 495 (current version at 50 U.S.C. § 401 (2006)).

informed of."[190] Simply put, in order to determine whether civil liberties violations have in fact occurred under the authority of EO 12333, significantly more information is required.[191]

Even Senator Diane Feinstein, the Chairwoman of the Senate Select Committee on Intelligence who has traditionally defended the government's use of surveillance authorities, has said that her committee "has not been able to sufficiently oversee the programs run under EO 12333."[192] On a related issue, Reggie B. Walton, the FISA Court's presiding judge, recently wrote that he recognizes the "potential benefit of better informing the public" about secret surveillance activities.[193] And lastly, most saliently stated by President Obama, "for our intelligence community to be effective over the long haul, we must maintain the trust of the American people, and people around the world."[194]

In July of 2014, EPIC urged PCLOB to review the surveillance activities conducted under EO 12333.[195] EPIC explained how self-regulation has proven to be ineffective in limiting surveillance overreach.[196] While EO 12333 requires a court order to target a United States Person, mass surveillance the NSA conducts overseas inevitably captures United States Person

---

[190] Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, (Nov. 21, 2013), http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html.
[191] Comments, EPIC, to the Foreign Intelligence Surveillance Court on "Proposed Amended FISC Rules," 4 (Oct. 4, 2010), *available at* https://epic.org/privacy/terrorism/fisa/EPIC%20Comments_FISC%202010%20Proposed%20Rules.pdf.
[192] Freedom of Information Act Request from Alan Butler, Appellate Advocacy Counsel, EPIC, to Cindy S. Blacker, FOIA Contact, Nat'l Security Agency (July 31, 2014), *available at* https://epic.org/privacy/surveillance/12333/12333-NSA-FOIA.pdf (citing Ali Watins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, (Nov. 21, 2013), *available at* http://www.mcclatchydc.com/20 3/11/21/209167/most-of-nsas-data-collection-authorized.html).
[193] Letter from Reggie B. Walton, Presiding Judge, U.S. Foreign Intelligence Surveillance Court, to Senator Diane Feinstein, U.S. Senate, (Mar. 27, 2013), *available at* http://fas.org/irp/agency/doj/fisa/fisc-032713.pdf.
[194] President Barack Obama, Remarks on the Review of Signals Intelligence (Jan. 17, 2014), *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence.
[195] EPIC 2014 PCLOB Statement, *supra*.
[196] *Id*. at 3.

information.[197] And then once captured, all information can be used and shared without any order from a judge or oversight from Congress.[198] Because EO "12333 does not fall within the purview of the Foreign Intelligence Surveillance Court . . . no neutral arbiter reviews 12333 surveillance for compliance with the Fourth Amendment."[199] As EPIC previously explained, "[t]he minimal oversight in place does not even give the appearance of the checks and balances provided by judicial or congressional oversight. Congress has admitted to very little oversight of the activities under 12333.[200]

EPIC testified before Congress in 2012 on transparency and oversight concerns pertaining to the FISA Amendments. EPIC addressed both why increased transparency is necessary for adequate oversight, and the need for increased oversight authority.[201] A key component to both facets of EPIC's argument is the need for improved reporting on the activities conducted under FISA, or analogously, EO 12333. EPIC's President Marc Rotenberg stated in his testimony, "We might disagree over whether the federal government engages in too much or too little electronic surveillance, but the annual report of the Administrative Basis provides a basis to evaluate the effectiveness of wiretap authority, to measure its cost, to even determine the percentage of communications captured that are relevant to an investigation. These reporting requirements ensure that law enforcement resources are appropriately and efficiently used while safeguarding important constitutional privacy interests."[202]

---

[197] *Id.*
[198] *Id.*
[199] *Id.*
[200] *Id.*
[201] *See* The FISA Amendments Act of 2008, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (Statement of Marc Rotenberg, Exec. Dir., EPIC).
[202] *Id.* at 4.

Perhaps even more damaging is the potential impact the lack of transparency has on public speech. EPIC President Marc Rotenberg went on to state:

> "a lack of transparency or knowledge of the extent of government surveillance can have a severe chilling effect on protected speech and public activity. Individuals who are not reasonably certain that their communications will be private and confidential could be forced to censor themselves to protect sources and clients. Given the lack of transparency and [] reporting, it seems eminently reasonable for these individuals to fear unlawful interception of their private communications. In the absence of public reporting, similar to the annual reports provided for Title III Wiretaps, Americans are understandably concerned about the scope of surveillance [conducted]."[203]

In our *amicus* brief in *The New York Times Co. v. U.S. Dep't of Justice*[204] EPIC stressed the importance of disclosing legal authority in government actions in promoting transparency and public confidence. In that case, pursuant to the Authorization for the Use of Military Force, the federal government initiated a covert "targeted killing" program as part of its global war on terror.[205] Some of these individuals targeted and killed by missile strikes from combat drones in Afghanistan, Pakistan, Yemen, and Somalia were American citizens. In 2010, *The New York Times* filed FOIA requests and specifically requested DOJ Office of Legal Counsel (OLC) memoranda containing the legal justification for the Administration's conclusion that it is lawful to target for killing persons, including United States citizens, who are suspected of ties to terrorist groups.[206] Later *The New York Times* instituted a suit against the DOJ for non-compliance.

---

[203] *Id*. at 6.
[204] *New York Times Co. v. DOJ*, 752 F.3d 123 (2d Cir. 2014).
[205] EPIC, *New York Times v. DOJ, Concerning the Department of Justice's Obligation to Disclose OLC Legal Opinions Under the FOIA*, https://epic.org/amicus/foia/new-york-times/#background (2015).
[206] *New York Times Co.*, 752 F.3d at 127–28.

EPIC's argument for better transparency and more public oversight in *The New York Times* case properly transfers to the context of E.O. 12333, where the government's data collection and legal decision-making processes are largely unknown. EPIC's *amicus* brief in the previous case traced the history and legal authority of the Office of Legal Counsel ("OLC") to show how the OLC's legal opinions establish binding law for the Executive Branch.[207] EPIC showed that OLC's current policies and past directors all agree that the Office is the authoritative legal arbiter of the Executive Branch, that its opinions are binding law, and that its formal written opinions should be disclosed to the public.[208] Timely disclosures of the legal basis for government actions is in the public's interest, as well as in the government's own interest. These disclosures further Executive Branch transparency "thereby contributing to accountability and effective government, and promoting public confidence in the legality of government action."[209] Similarly, for transparency and accountability purposes, it is crucial that American are informed about the legal authority and circumstances under which their information and communication records might be collected and accessed by the Intelligence Community.

A. Recommendations to Increase Transparency and Improve Oversight

1. No secret laws; the Intelligence Community should make available legal justifications for EO 12333 surveillance programs

By collecting personal data and undermining people's privacy interest without explaining the legal basis, the Executive Branch is engaging in secret law making, which has no place in our democratic society. EPIC's amicus brief in *The New York Times* explained that the classification

[207] Brief for EPIC *et al*. as *Amici Curiae* Supporting Appellants, *New York Times Co. v. DOJ*, 752 F.3d 123 (2d Cir. 2014) (No. 13-0422), *available at* https://epic.org/amicus/foia/new-york-times/EPIC-et-al-Amici-Brief.pdf.
[208] *Id*.
[209] *Id*. at 11.

and withholding of OLC legal analysis established "secret law" within the Executive Branch that undermines oversight and accountability, violates the requirements of the FOIA, and is antithetical to democracy.[210] In a suit by EPIC against the DOJ for its failure to produce documents relating to the legal justification for the President's surveillance program in 2005 under FOIA[211], the court stated that "an agency will not be permitted to develop a body of 'secret law,' used by it in the discharge of its regulatory duties and in its dealings with the public, but hidden behind a veil of privilege, because it is not designated as 'formal,' 'binding,' or 'final.'"[212] Concerning massive data collection and electronic surveillance programs under EO 12333, American citizens have a right to know that the elected government has made sound decisions and struck the right balance between protecting national security and protecting individual privacy. Because past instances of withholding of legal memoranda has stifled public debate of important issues[213], given our democratic heritage, constitutional values, and statutory rights, the government should not be permitted to issue law in the shadows. EPIC recommends that, for current and future IC programs under EO 12333, agencies should proactively disclose final legal opinions and legal justifications, and should make readily available legal memoranda upon FOIA requests. This would promote public discourse, foster government oversight, and lead to well-informed policy decisions.

[210] *Id*.
[211] *EPIC v. DOJ*, 511 F. Supp. 2d 56 (D.D.C. 2007).
[212] *Id.* at 68 (citing *Coastal States Gas Corp. v. DOE*, 617 F.2d 854, 867 (D.C. Cir. 1980)).
[213] Brief for EPIC et al., *New York Times Co.*, 752 F.3d 123 (No. 13-0422).

2. The PCLOB should ensure that the Intelligence Community Comply with the Privacy Act and the Principles of Intelligence Transparency for the Intelligence Community

The PCLOB should also prioritize Privacy Act compliance within the Intelligence Community. Congress enacted the Privacy Act with the understanding that secret databases threatened individual liberties and freedom.[214] Government agencies within the Board's purview, such as the CIA and NSA, routinely collect personal records without granting individuals basic Privacy Act protections, like access, amendment, and notification rights.[215] The Privacy Act defines the right to privacy with regard to the collection and use of personal information by federal agencies,[216] and it is the Board's responsibility to see that the Act is enforced.

Additionally, the PCLOB must ensure that the Principles of Intelligence Transparency for the Intelligence Community[217] be faithfully implemented. The Principles of Intelligence Transparency for the Intelligence Community are intended to facilitate IC decisions on making information publicly available in a manner that enhances public understanding of intelligence activities, while continuing to protect information when disclosure would harm national security. The Principles suggest that agencies should "classify only that information which, if disclosed without authorization, could be expected to cause identifiable or describable damage to the national security."[218] Therefore, EPIC's "no secret law" recommendation is consistent with the Principles, requiring the agencies to de-classify documents such as final legal memoranda that otherwise do not qualify as client-attorney or deliberative works. At the same time, while making information publicly accessible, PCLOB should see to that the disclosure be made in an

[214] Letter from EPIC to PCLOB 3 (Nov. 11, 2014).
[215] *Id*. at 4.
[216] *Id*.
[217] ODNI Transparency Principles, *supra*.
[218] *Id*.

understandable fashion providing clarity and context[219], which would contribute to meaningful public dialogue and oversight rather than create public confusion and discouragement.

3. Agencies conducting EO 12333 surveillance activities must publically issue regular statistical reports that include all relevant, non-classified information

After Congress passed the USA PATRIOT Act, the American Bar Association made recommendations to ensure effective privacy safeguards, including an annual statistical report on investigations comparable to the annual Wiretap Report published by the Administrative Office of the United States Courts. As was similarly the case with surveillance authorized by the FAA, the broad scope of surveillance conducted under EO 12333 necessitates a comprehensive report releasing information, "to the greatest extent possible, consistent with the need to protect classified information. With respect to authorities and programs whose existence is unclassified, there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves." [220]

Aggregate statistical reporting would improve both executive and public oversight on the information gathering activities conducted under EO 12333. This type of reporting protects privacy, encourages oversight and accountability, and continues to provide law enforcement with the tools to conduct necessary investigations.[221] These reports allow Congress and interested groups to evaluate the effectiveness of Government programs and to ensure that important civil rights are protected.[222] For example, each year EPIC closely reviews the wiretap report and in

---

[219] *Id.*
[220] President's Review Group Report, *supra*, at 219–20.
[221] The FISA Amendments Act of 2008, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. at 6 (May 31, 2012) (Statement of Marc Rotenberg, Exec. Dir., EPIC).
[222] *Id.*

2013, wiretaps were up 5%.[223] Moreover, law enforcement encountered encryption during 41 investigations, but were unable to decipher encrypted messages in only 9 cases.[224] As EPIC previously reported, this statistic contradicts claims that law enforcement agencies are "going dark" as new technologies emerge. [225]

Both PCLOB and the President's Review Group on Intelligence and Communications Technologies have also called for aggregate statistical reporting about electronic surveillance activities.[226] In a recent report on the government's collection of telephone records, PCLOB stated, "One way to understand and assess any government program is numerically. . . . Periodic public reporting on surveillance programs is a valuable tool in promoting accountability and public understanding."[227] The President's Review Group specifically identified the reporting of aggregate statistics as a priority: "the government should, to the greatest extent possible, report publically on the total number of requests made and the number of individuals whose records have been requested. These totals inform Congress and the public about the overall size and trends in a program, and are especially informative when there are major changes in the

[223] Admin. Office of the U.S. Courts, *Wiretap Report 2013*, http://www.uscourts.gov/statistics-reports/wiretap-report-2013#sa5.
[224] *Id*.
[225] *See also In re Nat'l Security Letter*, No. 13-16732 (9th Cir. 2013) (citing EPIC, *Federal and State Wiretaps Up 24%, Primary Target Mobile Devices According to 2012 Report* (June 28, 2013), https://epic.org/2013/06/federal-and-state-wiretaps-up.html)).
[226] Brief of EPIC as *Amici Curiae* Supporting Respondents, In re Nat'l Security Letter, No. 13-16732 (9th Cir. 2013) (citing Privacy and Civil Liberties 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 201 (2014)).
[227] Privacy and Civil Liberties 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 201 (2014).

program."[228] Courts also agree that aggregate statistical reporting provides "remarkably useful data for evaluating surveillance methods without compromising any particular investigations."[229]

A statistical report on activities conducted under EO 12333 is critical to evaluating both the effectiveness and the need for various types of Government surveillance activities.

4. PCLOB Should Require Audit Trails for EO 12333 Surveillance Activities to Ensure Accountability

EPIC has long espoused the use of audit trails to establish individual accountability in mass data collection situations. In 2000, EPIC submitted its comments to the Independent Technical Review of the "Carnivore" (an Internet monitoring system then used by the FBI),[230] raising concerns of the lack of accountability inherent in the system.[231] EPIC stated that the over-collection flaw of the Carnivore system was exacerbated by the system's lack of an effective accountability mechanism, which did not provide adequate provisions (*e.g.* audit trails) for establishing individual accountability for actions taken during use of Carnivore.[232] Since auditing is crucial in security and NSA's programs under EO 12333 run the risk of over collecting data, it is urgent to institute audit trails to determine who, among a group of agents, may have accessed or disclosed information without authorization. Tracing the actions to specific individuals is the means by which users are held accountable for their actions.[233]

---

[228] President's Review Group Report, *supra*, at 128.
[229] *In re Nat'l Security Letter*, No. 13-16732 (9th Cir. 2013) (citing Admin. Office of the U.S. Courts, Wiretap Report 2012, http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2012.aspx (last updated Dec. 31, 2012)).
[230] EPIC, *Carnivore*, https://www.epic.org/privacy/carnivore/ (2005).
[231] Email from David L. Sobel, EPIC, to Carnivore Review Panel, U.S. Dep't. of Justice (Dec. 1, 2000) (https://epic.org/privacy/carnivore/review_comments.html).
[232] *Id*.
[233] *Id*.

Automated audit trails should be used to improve training efficiency and effective supervision, since incidents attributable to human errors constitute the majority of legal rules and privacy violations under NSA's SIGINT program. According to a leaked internal audit, there were 2,776 incidents[234] of unauthorized collection, storage, access to or distribution of legally protected communications in the preceding 12 months, and the number of EO 12333 (as well as under other authorities) incidents increased compared to the previous year. [235] The majority of incidents in all authorities were database query incidents due to human error, which encompassed typographical error, query technique understood but not applied, not familiar enough with the tool used for query, lack of due diligence (i.e., failure to follow standard operating procedure), training and guidance issues and inaccurate or insufficient research information and/or workload issues.[236] Audit trails will associate individuals with these incidents, and as a result will inform program directors of who are or are not best positioned for this task. The trails will also tell whether additional trainings are necessary in a specific area for certain group of agents.

By establishing individual accountability, automated audit trails will reduce willful rule violations and facilitate the Board's effective oversight of NSA's data collection programs. In 2013, NSA confessed that analysts have willfully violated internal agency protocols to collect info on love interests.[237] In response to the alleged rule violations by NSA agents, NSA Chief

[234] Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, Wash. Post (Aug. 15, 2013), http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html.
[235] Memorandum from SID Oversight & Compliance to SIGINT Director (May 3, 2012), available at https://s3.amazonaws.com/s3.documentcloud.org/documents/758651/1qcy12-violations.pdf.
[236] *Id*. at 6-7.
[237] Siobhan Gorman, *NSA Officers Spy on Love Interests*, Wall St. J. (Aug. 23, 2013), http://blogs.wsj.com/washwire/2013/08/23/nsa-officers-sometimes-spy-on-love-interests/.

Compliance Officer John DeLong emphasized in a conference call with reporters that those errors were unintentional. He conceded that there have been "a couple" of willful violations in the past decade.[238] Audit trails will effectively deter such willful, albeit infrequent, violations, since any access to the database will be recorded with the agent's information. Furthermore, an internal NSA guidance instructs agents to give minimal information to FAA overseers as to why the agent requests targeting.[239] The instruction asks agents to give only one-short-sentence rationale and must not include additional information such as proof of analytical judgment.[240] Audit trails would likely render such oversight-evading tactic futile because the Board will be able to see which information the agent has collected and accessed and request additional explanation from the agent if the vague rationale is called in doubt. In this way, the adoption of audit trails will make the Board's oversight more efficient.

Furthermore, audit trails are necessary to comply with the Privacy Act. The Privacy Act of 1974 Subsection (c) states that an agency must also keep accurate accounts of when and to whom it has disclosed personal records. [241] This includes contact information for the person or agency that requested the personal records. These accounts should be kept for five years, or the lifetime of the record, whichever is longer. Unless the records were shared for law enforcement purposes, the accounts of the disclosures should be available to the data subject upon request. Moreover, the National Research Council also recommends a "permanent, tamper-resistant record of when data have been accessed and by whom to create a non-human, automatic audit"

[238] *Id*.
[239] Nat'l Sec. Agency, *Targeting Rationale (TAR)*, available at http://s3.documentcloud.org/documents/750577/target-analyst-rationale-instructions-final.pdf.
[240] *Id*.
[241] 5 U.S.C. § 552a(c).

to intelligence agencies. [242] For the aforementioned reasons, audit trails foster legal compliance, minimize access to sensitive data, and provide meaningful oversight.

Accordingly, the Board should ensure that audits are implemented among agencies conducted EO 12333 surveillance activities.

5. The PCLOB should maintain independence from the Intelligence Community in the Executive Branch

It is imperative for the Board to remain an independent reviewing body, given that the IC currently only receives oversight from within the executive branch for operations under EO 12333.[243] Although Alexander W. Joel, the civil liberties protection officer for the Office of the Director of National Intelligence, describes the oversight IC receives as extensive and multi-layered under EO 12333,[244] this type of self-regulation has proven to be ineffective at best in limiting surveillance overreach."[245] Such an internal check is weak and lacks transparency. In its comments to the Foreign Intelligence Surveillance Court ("FISC") on "Proposed Amended FISC Rules," EPIC advocated for the independence of the FISC from the Executive Branch in order to duly exercise its role in ensuring "that the FISA does not become a tool that allows the government to create a dragnet through electronic surveillance."[246] EPIC maintains this recommendation for an independent review body – the PCLOB – for programs conducted under

[242] Nat'l Research Council, *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment* 62 (Nat'l Acads. Press 2008), *available at* http://www.nap.edu/catalog/12452.html.
[243] Alexander W. Joel, *The Truth About Executive Order 12333*, Politico Magazine (Aug. 18, 2014), http://icontherecord.tumblr.com/tagged/speeches-and-interviews.
[244] *Id*.
[245] EPIC 2014 PCLOB Statement, *supra*.
[246] EPIC, Comments of the Electronic Privacy Information Center to the Foreign Intelligence Surveillance Court "Proposed Amended FISC Rules" 4 (Oct. 4, 2010), *available at* https://epic.org/privacy/terrorism/fisa/EPIC%20Comments_FISC%202010%20Proposed%20Rules.pdf.

EO 12333. The Board should also report annually to Congress on its compliance oversight work.[247]

Additionally, the Board should apply rigorous scrutiny to reviewing the agencies' compliance with existing civil liberties requirements. Recently, the Board endorsed the mass communications collection of foreign emails, texts, and Americans' international calls under Section 702 of FISA,[248] even though the huge amount of data implicated serious privacy concerns.[249] The Board was also willing to endorse the NSA's collection of information that merely referenced a surveillance target ("about" collection).[250] One of the board members described NSA's digital surveillance as effective, valuable, and legal, and said that the PCLOB only made minor recommendations at the margins of the program.[251] The Board's report spurred much criticism among privacy advocates and called into question whether such leniency would open door to more outrageous government surveillance.[252] Although EO 12333 and FISA are separate, given the two systems' similar nature (in particular the incidental collection of U.S. persons' information[253] is akin to the "about" collection under Section 702), the public might question the Board's ability to exercise effective oversight or place meaningful limitation on the agencies' overreaching operations. Consequently, the Board must review EO 12333 programs rigorously and publish the standards and guidelines it uses in reviewing these programs.

---

[247] *Id*.
[248] Privacy and Civil Liberties Oversight Bd., *Report on the Surveillance Program Operated Pursuant to Sec 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report.pdf.
[249] Spencer Ackerman, *NSA Reformers Dismayed after Privacy Board Vindicates Surveillance Dragnet*, The Guardian (July 2, 2014), http://www.theguardian.com/world/2014/jul/02/nsa-surveillance-government-privacy-board-report?CMP=ema_565.
[250] *Id*.
[251] *Id*.
[252] *Id*.
[253] EO 12333 § 2.3 (i).

6. The PCLOB should develop its enforcement authority to compel agency cooperation and supervise the implementation of internal recommendations

The Board should strengthen its enforcement authority to bring about effective oversight. The Intelligence Reform and Terrorism Prevention Act that established the Board charged with "[d]etermin[ing], with leadership from the President, guidelines for gathering and sharing information in the new security systems that are needed, guidelines that integrate safeguards for privacy and other essential liberties."[254] The enumerated functions of the Board limit this ability by restricting the Board's activities to review and advise, while providing no method of enforcement or rectification of privacy or civil liberty violations.[255] The Board is further limited by the fact that the Attorney General and the Director of National Intelligence can withhold information in the interest of national security and counterterrorism and law enforcement efforts.[256] Because PCLOB relies on the cooperation of the agencies and agency personnel, the Board should take measures to establish authority within the Intelligence Community, which might include reporting to Congress of agency non-compliance in its annual reports and petitioning to Congress for granting it enforcement power within the Intelligence Community.

Additionally, the Board should have increased supervision power to ensure that internal recommendations are timely implemented. For example, the President's Review Group issued Recommendation 12 in its December 2013 report suggesting reform of Section 702 of the FISA Amendments Act and any other authority "that justifies the interception of a communication on the ground that it is directed at a non-United States person who is located outside the United

---

[254] Marc Rotenberg, Exec. Dir., EPIC, *The Sui Generis Privacy Agency: How the United States Institutionalized Privacy Oversight After 9-11*, 35–44 (Sept. 2006), https://epic.org/epic/ssrn-id933690.pdf.
[255] *Id.*
[256] *Id.*

States . . ."[257] which is understood to encompass EO 12333. Recommendation 12 calls for purging of US-person's information upon detection and not using the information in any proceeding against the US person.[258] There is no evidence that the NSA plans to adopt such a recommendation or is undertaking to bring its actions more in line with the report's general spirit. In its Recommendations Assessment Report,[259] the Board has identified many important compliance and transparency recommendations made by the Board that have not been adopted by the agencies. Given that these recommendations provide valuable protection for civil liberties and facilitate transparency and public oversight, it is crucial that the Board play a supervision role in their adoptions rather than just make reports on the progress.

Finally, the Board should encourage the agencies to make disclosures pursuant to a consistent level of transparency and understanding. For instance, after the President issued PPD-28, the Intelligence Community has revised their policies and adopted new rules regarding the retention and minimization of signals intelligence. However, the published policies vary in length and substance. The Board should uphold the highest possible standard of transparency, to which the agencies should be encouraged to conform their policy disclosures. Furthermore, the Board should ensure that the interpretations of key words in EO 12333 are consistent among agencies. A term as broad as "foreign intelligence"[260] might be interpreted differently in different agencies, and therefore the Board is tasked with ensuring that disclosed agency documents are clear and consistent when they reach the general public.

---

[257] President's Review Group Report, *supra*, at 145-150.
[258] *Id*.
[259] Privacy and Civil Liberties Oversight Bd., *Recommendations Assessment Report* (Jan. 29, 2015), *available at* https://www.pclob.gov/library/Recommendations_Assessment-Report.pdf.
[260] EO 12333 § 3.5 (e) (defining "foreign intelligence" as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists").

Before giving the Executive Branch enormous authority in conducting mass electronic surveillance, there needs to be meaningful oversight, accountability, and transparency governing EO 12333.[261] There is significant chilling effect on free speech and public activity due to the lack of transparency regarding the government's surveillance activities; there is a legitimate fear of "future injury" in the society at large. EPIC recommends publishing assessment reports regarding the Intelligence Community's compliance with PCLOB's guidelines and recommendations under EO 12333, statistics for rule violations, and a provision for an increased web presence. It is also important that the Board maintain independent from the rest of the Executive Branch and review the agencies' compliance with high degree of rigor. These measures would promote government transparency and oversight, and re-establish public confidence in agency operations.

IV. Conclusion

For the aforementioned reasons, the Board should work with the Intelligence Community to implement the recommended oversight, transparency, and accountability mechanisms.

[261] The FISA Amendments Act of 2008, Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary, 112th Cong. (May 31, 2012) (Statement of Marc Rotenberg, Exec. Dir., EPIC).

Respectfully submitted,

Marc Rotenberg, EPIC President and Executive Director
Khaliah Barnes, EPIC Associate Director
Alan Butler, EPIC Senior Counsel
Jeramie D. Scott, EPIC National Security Counsel

John Davisson, EPIC IPIOP Law Clerk
Britney Littles, EPIC IPIOP Law Clerk
Ximeng Tang, EPIC IPIOP Law Clerk
Michele Trichler, EPIC IPIOP Law Clerk
Kasey Wang, EPIC IPIOP Law Clerk
Jennifer Weekley, EPIC IPIOP Law Clerk

Electronic Privacy Information Center
1718 Connecticut Avenue, Suite 200
Washington, DC 20009
(202) 483-1140