WASHINGTON
LEGISLATIVE OFFICE

January 13, 2016

Privacy and Civil Liberties Oversight Board
2100 K Street NW, Suite 500
Washington, DC 20427

Dear Privacy and Civil Liberties Oversight Board Members:

On behalf of the ACLU, a non-partisan organization with over a million members, activists, and supporters, and affiliates nationwide, we write to offer comments regarding the Privacy and Civil Liberties Oversight Board's (PCLOB) examination of surveillance activities governed by Executive Order (EO) 12333.[1]

EO 12333 is the primary authority under which the NSA gathers foreign intelligence.[2] It provides broad latitude for the government to conduct surveillance on U.S. and non-U.S. persons—without judicial review and other protections that would apply to surveillance conducted under statutory authorities.[3] Despite its breadth, EO 12333 has not been subject to meaningful oversight. The Chairwoman of the Senate Intelligence Committee, Senator Dianne Feinstein, has candidly acknowledged that Congress has been unable to "sufficiently" oversee EO 12333 surveillance.[4]

On April 8, 2015, the PCLOB announced that it would examine counterterrorism-related activities governed by EO 12333. The examination would focus on activities of the CIA and NSA that involved 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.[5]

The ACLU urges the PCLOB to do the following as part of its examination of surveillance activities carried out under EO 12333:

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

KARIN JOHANSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] This submission reflects substantial contributions from ACLU staff including Alex Abdo, Ashley Gorski, Neema Guliani, Jameel Jaffer, Brett Max Kaufman, and Patrick Toomey.
[2] OVERVIEW OF SIGNALS INTELLIGENCE AUTHORITIES PRESENTATION 4 (Jan. 8, 2007), *available at* https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf [hereinafter OVERVIEW OF SIGNALS INTELLIGENCE].
[3] John Napier Tye, *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.
[4] Ali Watkins, *Most of NSA's Data Collection Authorized by Order Ronald Reagan Issued*, MCCLATCHY (Nov. 21, 2013), http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html.
[5] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, PCLOB EXAMINATION OF EO 12333 ACTIVITIES IN 2015, *available at* https://www.pclob.gov/library/20150408-EO12333_Project_Description.pdf (last visited Dec. 17, 2015).

- Issue a public report summarizing the scope of electronic surveillance conducted under the EO 12333 programs examined, including relevant policies and procedures related to collection, retention, use, and dissemination of information.

- Urge Congress to pass legislation, consistent with the recommendations in Section III, that appropriately circumscribes electronic surveillance currently conducted under EO 12333 and ensures it is consistent with the Constitution and international law. Briefly, the recommendations in Section III would:
    - Prohibit the mass surveillance of the communications of U.S. and non-U.S. persons;
    - Strengthen EO 12333's minimization procedures, including by eliminating the backdoor-search loophole for U.S. persons and by limiting retention of U.S. and non-U.S. persons information;
    - Limit the sharing of U.S and non-U.S. persons information with foreign governments;
    - Provide much-needed transparency into the operation of EO 12333 and its effect.

- Recommend that the Executive Branch adopt the recommendations in Section III until Congress passes legislation regulating EO 12333 activities.[6]

Section I of the comments below provides a summary of what is publicly known about EO 12333, the policies and procedures that implement its authority, and the extent to which the order and its implementing regulations permit the expansive collection, retention, use, and dissemination of the communications of U.S. and non-U.S. persons. Section II explains that surveillance of U.S. persons under EO 12333 violates the Constitution, underscoring the need for reform. And Section III provides a list of the recommendations that we urge the PCLOB to recommend that Congress and the Executive Branch adopt to ensure that EO 12333 activities comply with U.S. and international law.

I. What Is Publicly Known about the Collection, Retention, Use, and Dissemination of Information under EO 12333

a. EO 12333 Policies and Procedures

EO 12333, originally issued in 1981 by President Ronald Reagan and subsequently revised, is the primary authority under which the NSA gathers foreign intelligence.[7] It is used to justify, among other things, undisclosed surveillance activities within the United States, human and electronic surveillance conducted overseas targeting non-U.S. persons, and surveillance targeting U.S. persons overseas in limited circumstances.[8] Collection, retention, and dissemination of EO 12333 information is governed by directives and regulations promulgated by federal agencies and approved by the Attorney General, including United States Signals Intelligence Directive 0018 (USSID 18). In addition, Presidential Policy Directive-28 (PPD-28) and associated agency policies further regulate EO 12333 activities, with the stated goal of creating parity between the treatment of U.S. and non-U.S. person information.

EO 12333's stated goal is to provide authority for the intelligence community to gather the information necessary to protect U.S. interests from "foreign security threats," with particular emphasis on countering

[6] For an analysis of international law applicable to surveillance conducted under EO 12333, *see generally*, ACLU, INFORMATION PRIVACY IN THE DIGITAL AGE (Feb., 2015), *available at* https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf.

[7] OVERVIEW OF SIGNALS INTELLIGENCE, *supra* note 2.

[8] *See* Exec. Order No. 12333 § 2.4, *available at* http://www.dni.gov/index.php/about/organization/ic-legal-reference-book-2012/ref-book-eo-12333 [hereinafter EO 12333].

terrorism, espionage, and weapons of mass destruction.[9] Despite this stated goal, EO 12333 is used to justify surveillance for a broad range of purposes, resulting in the collection, retention, and use of information from large numbers of U.S and non-U.S. persons who have no nexus to foreign security threats.

i. Collection

EO 12333 and its accompanying regulations place few restrictions on the overseas collection of U.S. or non-U.S. person information. The order authorizes the government to conduct electronic surveillance abroad, targeted at non-U.S. persons, for the purpose of collecting "foreign intelligence"[10]—a term defined so broadly that it likely permits surveillance of any foreign person, including their communications with U.S. persons.[11] Neither this definition nor other policies under EO 12333 restrict the surveillance of journalists, healthcare providers, or attorneys—whose information is often subject to enhanced legal protections.

In addition, the order and its implementing regulations permit two forms of bulk surveillance.[12] First, they permit the government to engage in what is sometimes termed "bulk collection"—that is, the indiscriminate collection of electronic communications or data.[13] Though existing policies state that the government will use data collected in bulk for only certain purposes, they permit collection of electronic communications in bulk even if doing so sweeps up U.S. person domestic communications, U.S. person international communications, or irrelevant non-U.S. person communications.

Second, the order and its implementing regulations allow what might be termed "dragnet surveillance," in which the government indiscriminately scans the content of international electronic communications for "selection terms." Existing policies only require that such bulk collection targeting non-U.S. persons be as "tailored as feasible," and that it use "selection terms" defining targets or topics when possible. However, unlike the approach taken by provisions of the Foreign Intelligence Surveillance Act (FISA), existing policies place no meaningful restrictions on the scope of permissible selection terms. As a result, the government can use selectors likely to return large amounts of information, such as the names of countries, cities, or service providers. In addition, unlike the selectors the government claims to use under the FISA Amendments Act's upstream program, EO 12333 procedures permit selectors that are not associated with particular targets (such as an email address or phone number).[14] In other words, the government claims the

[9] *See* EO 12333 § 1.1 ("special emphasis should be placed on detecting and countering terrorism; the development, proliferation, or use of weapons of mass destruction; and espionage and other activities directed by foreign powers and intelligence services against the U.S.").
[10] Press Release, White House Office of the Press Secretary, Presidential Policy Directive—Signals Intelligence Activities: Presidential Policy Directive/PPD-28 §1 (Jan. 17, 2014), https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [hereinafter PPD-28].
[11] EO 12333 defines foreign intelligence as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists."
[12] *See, e.g.*, U.S. SIGNALS INTELLIGENCE DIRECTIVE SP0018 §4 [hereinafter USSID 18], *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf (all citations to USSID 18 are to the version dated January 25, 2011, unless noted otherwise); NATIONAL SECURITY AGENCY, PPD-28 SECTION 4 PROCEDURES § 5 (Jan. 12, 2015), *available at* https://www.nsa.gov/public_info/_files/nsacss_policies/PPD-28.pdf [hereinafter PPD-28 SECTION 4 PROCEDURES].
[13] For the purposes of this comment, "electronic communications" refers not only to information in transit, but also to stored communications and other data that U.S. persons entrust to companies offering communications services or remote storage, such as cloud-computing providers.
[14] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 7 (July 2, 2014), *available at*

authority under EO 12333 to scan all information collected in bulk, including U.S. persons' communications and data, for *keywords*.

In addition to the targeting of non-U.S. persons, EO 12333 permits the targeted electronic surveillance of information to or from a U.S. person in various situations, including in emergencies and under the approval of the Attorney General under undisclosed circumstances.[15]

ii. Retention, Dissemination, and Use

EO 12333 permits the retention and dissemination of both U.S. and non-U.S. person information. Under the relevant policies, the government can generally retain data for up to five years. In addition, it can retain data permanently in numerous circumstances, including data that is (1) encrypted or in unintelligible form;[16] (2) related to a foreign-intelligence requirement; (3) indicative of a threat to the safety of a person or organization; or (4) related to a crime that has been, is being, or is about to be committed. The government may also retain data if it determines in writing that retention is in the "national security interest" of the United States. Information in categories (2), (3), and (4), including identifiers of a specific U.S. or non-U.S. person, may be disseminated for use throughout the government.

Notably, the EO 12333 implementing regulations appear to allow so-called "backdoor" searches—the querying of data collected under EO 12333 specifically for information related to U.S. persons. The government presumably relies on the fruits of these searches in administrative, civil, and criminal proceedings, regardless of whether the proceedings have a nexus to the original purpose of the surveillance. Moreover, EO 12333 and its implementing regulations do not appear to require that the government notify criminal defendants or others when it uses evidence against them obtained or derived from EO 12333 surveillance programs.

iii. Sharing of Information with Foreign Entities

The U.S. government shares data collected under EO 12333 with foreign governments based on both formal agreements and informal arrangements. For example, the U.S. has agreements with the United Kingdom (UK), Australia, Canada and New Zealand in a partnership known as the "Five Eyes," through which the five countries share raw data, intelligence reports, intelligence structures, and operations centers.[17] While these agreements are not public, they reportedly allow for the sharing of raw data without

---

https://www.pclob.gov/library/702-Report.pdf (describing the government's tasking of selectors "such as telephone numbers or email addresses" for FAA surveillance), [hereinafter PCLOB REPORT ON 702].

[15] *See* USSID18, *supra* note 12 at § 4 (redacting permissible targeting of U.S. persons). EO 12333 appears to permit the targeting of U.S. persons by human intelligence in a larger subset of circumstances. A released DOD presentation states that U.S. person information may be collected in situations involving international narcotics activities; commercial organizations believed to have some relationship with a foreign organizations; or organizations owned or controlled by a foreign power. DOD HUMINT LEGAL WORKSHOP, FUNDAMENTALS OF HUMINT TARGETING, ASSISTANT GENERAL COUNSEL DEFENSE INTELLIGENCE AGENCY 6, *available at* https://www.aclu.org/files/assets/eo12333/DIA/DoD%20HUMINT%20Legal%20Workshop%20Fundamentals%20of%20HUMINT%20Targeting.pdf.

[16] The default five-year age-off is triggered when this data is in intelligible form. *See* PPD-28 SECTION 4 PROCEDURES, *supra* note 12 at § 6.1.

[17] PRIVACY INTERNATIONAL, EYES WIDE OPEN 4-21 (Nov. 26, 2013), *available at* https://www.privacyinternational.org/sites/default/files/Eyes%20Wide%20Open%20v1.pdf.

appropriate protections.[18] For example, the UK reportedly searches through U.S. person data without a warrant or the equivalent.

The United States also shares U.S. and non-U.S. person information with countries other than the Five Eyes, including Germany, Israel, and Saudi Arabia.[19] We know little about the scope of U.S. information-sharing agreements, but there appear to be inadequate restrictions on the use and dissemination of information that is shared. For example, the U.S. reportedly shares intelligence with Israel to aid military operations targeted at the Palestinian territories.[20] The Memorandum of Understanding governing this intelligence-sharing arrangement permits sharing of U.S. person information, contains no prohibition on the use of information to commit human rights abuses, allows sharing of non-U.S. person data with third parties, and contains no requirement that Israel adhere to U.S. policies regarding the treatment of non-U.S. person data.[21]

b. EO 12333 Electronic Surveillance Programs

Recent disclosures indicate that the government operates a host of large-scale programs under EO 12333, many of which likely involve the collection of vast quantities of U.S. and non-U.S. person information. For example:

- **MUSCULAR**, in which the U.S. intercepted all data transmitted between certain data centers operated by Yahoo! and Google outside of U.S. territory;[22]

- **MYSTIC**, a program involving the collection of all telephone metadata in the Bahamas, Mexico, Kenya, the Philippines, and Afghanistan, as well as the full audio of all phone calls in the Bahamas and Afghanistan, reportedly to target drug traffickers;[23]

- **DISHFIRE**, through which the U.S. reportedly collects 200 million text messages from around the world every day, and provides access to this information to the UK intelligence services;[24]

---

[18] James Ball, *GCHQ Views Data Without a Warrant, Government Admits*, THE GUARDIAN, (Oct. 28, 2014), http://www.theguardian.com/uk-news/2014/oct/29/gchq-nsa-data-surveillance.

[19] *See* Mark Hosenball, Phil Stewart & Warren Strobel, *Exclusive: US Expands Intelligence Sharing with Saudis in Yemen Operation*, REUTERS (Apr. 10, 2015), http://www.reuters.com/article/2015/04/11/us-usa-saudi-yemen-exclusive-idUSKBN0N129W20150411; Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN (Sept. 11, 2013) http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

[20] Greenwald, Poitras & MacAskill, *supra* note 19.

[21] Memorandum of Understanding between the NSA/CIA and the Israeli SIGINT National Unit (Sept. 11, 2013), *available at* http://www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document.

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

[23] Ryan Devereaux, Glenn Greenwald & Laura Poitras, *Data Pirates of the Caribbean: The NSA is Recording Every Cell Phone Call in the Bahamas*, THE GUARDIAN (May 19, 2014), https://firstlook.org/theintercept/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/.

[24] James Ball, *NSA Collects Millions of Text Messages Daily in 'Untargeted' Global Sweep,* THE GUARDIAN (Jan. 16, 2014), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep.

- **CO-TRAVELER**, through which the U.S. captures billions of location updates daily from mobile phones around the world, likely including information relating to U.S. persons;[25]

- **QUANTUM**, a U.S. program that monitors Internet traffic and responds based on certain triggering information with active attacks, including the delivery of malicious software to a user's device;[26]

- **Targeting of popular cell phone applications,** such as Angry Birds, Facebook, and Twitter, to gather information regarding (among other things) the device, location, age, and sex of their users;[27]

- **Buddy list and address book collection** programs, involving the interception of email address books and buddy lists from instant messaging services as they move across global data links;[28]

- **WELLSPRING**, an initiative that involved collecting images from e-mails for analysis by facial recognition software;[29] and

- **TRACFIN**, a database for information collected about credit card transactions and credit card purchases overseas from prominent companies such as Visa. In 2011, Tracfin reportedly contained 180 million records, 84% of which were from credit card transactions.[30]

In addition to these programs, EO 12333 also appears to be have been used for surveillance targeting journalists, diplomats, world leaders, technology companies, and geographic areas where the U.S. is engaged in military operations. For example:

- **BULLRUN**, a joint program to crack encryption and introduce vulnerabilities into commercial products;[31]

- **Hacking into news organizations**, such as Al Jazeera, to obtain information regarding communications with potential targets;[32]

---

[25] Barton Gellman & Ashkan Soltani, *NSA tracking cellphone locations worldwide, Snowden documents show,* WASH. POST (Dec. 4, 2013), https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html.

[26] Nicholas Weaver, *A Sloce Look at the NSA's Most Powerful Internet Attack Tool,* WIRED (March 13, 2014), http://www.wired.com/2014/03/quantum/.

[27] Jeff Larson, James Glanz & Andrew W. Lehren, *Spy Agencies Probe Angry Birds and Other Apps for Personal Data*, PROPUBLICA (Jan. 7, 2014, 1:30 PM) http://www.propublica.org/article/spy-agencies-probe-angry-birds-and-other-apps-for-personal-data.

[28] Barton Gellman & Ashkan Soltani, *NSA Collected 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_print.html.

[29] James Risen & Laura Poitras, *N.S.A. Collecting Millions of Faces from Web Images*, N.Y. TIMES (May 31, 2014), http://www.nytimes.com/2014/06/01/us/nsa-collecting-millions-of-faces-from-web-images.html?_r=0.

[30] *Follow the Money: NSA Spies on International Payments,* SPIEGEL ONLINE INT'L (Sept. 15, 2013), http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html.

[31] BULLRUN Briefing Sheet from GCHQ (last accessed Dec. 17, 2015) *available at* http://www.propublica.org/documents/item/784284-bullrun-briefing-sheet-from-gchq.html.

[32] The surveillance could also have been potentially conducted under Section 702 through targeting of specific officials. *Snowden Document: NSA Spied on Al Jazeera Communications,* SPIEGEL ONLINE INT'L (Aug. 31, 2013),

- **WABASH, BRUNEAU, HEMLOCK, BLACKFOOT, and other programs** to conduct surveillance of 38 embassies and missions in New York and Washington D.C.,[33]

- **Surveillance of major worldwide summits**, including the G8, G20, and 2009 U.N. Climate Change Conference;[34]

- **SHOTGIANT**, an initiative to hack into Huawei, a Chinese telecommunications company, to obtain information about routers, digital switches, and other products that could be exploited to conduct surveillance;[35]

- **VICTORYDANCE**, which uses drones to map the WiFi fingerprint of nearly every town in Yemen;[36]

- **Surveillance of major world leaders**, including surveillance of Russian leadership and hacking into the cell phones of German leadership;[37] and

- **GILGAMESH**, a program to geolocate individuals' SIM cards using predator drones in select geographic areas.[38]

II. Surveillance of U.S. Persons Under EO 12333 Violates the Constitution

Based upon the legal analysis that follows, the ACLU urges the PCLOB to conclude that the warrantless surveillance of Americans permitted under EO 12333 violates the Fourth Amendment, and accordingly recommend adoption of the proposals in Section III to ensure that EO 12333 surveillance more closely aligns with the Constitution's requirements.

---

http://www.spiegel.de/international/world/nsa-spied-on-al-jazeera-communications-snowden-document-a-919681.html.

[33] Some of this surveillance could also have been potentially conducted pursuant to FISA, given the domestic nature. Ewan MacAskill & Julian Borger, *New NSA Leaks Show How US is Bugging its European Allies,* THE GUARDIAN (June 30, 2013), http://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies.

[34] Greg Weston, Glenn Greenwald,& Ryan Gallagher, *New Snowden Docs Show U.S. Spied During g20 in Toronto,* CBCNEWS, http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448; Kate Sheppard & Ryan Grim, *Snowden Docs: U.S. Spied on Negotiators at 2009 Climate Summit,* HUFFINGTON POST (Jan. 29, 2014), http://www.huffingtonpost.com/2014/01/29/snowden-nsa-surveillance-_n_4681362.html.

[35] The surveillance could also have been potentially conducted under Section 702 through targeting of executives. David E. Sanger & Nicole Perlroth, *N.S.A. Breached Chinese Servers as Security Threat,* N.Y. TIMES (Mar. 22, 2014), http://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

[36] Jeremy Scahill & Glenn Greenwald, *The NSA's Secret Role in the U.S. Assassination Program,* THE INTERCEPT (Feb. 10, 2014), https://firstlook.org/theintercept/2014/02/10/the-nsas-secret-role/.

[37] *Sweden Key Partner for U.S. Spying on Russia-TV*, REUTERS (Dec. 5, 2013), http://www.reuters.com/article/2013/12/05/sweden-spying-idUSL5N0JK3MV20131205; Laura Poitras, Marcel Rosenbach & Holger Stark, *'A' for Angela: GCHQ and NSA Targeted Private German Companies and Merkel,* SPIEGEL ONLINE INT'L (Mar. 29, 2014), http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html.

[38] Bruce Schneier, *Everything We Know About How the NSA Tracks People's Physical Locations*, THE ATLANTIC, (Feb. 11, 2014), http://www.theatlantic.com/technology/archive/2014/02/everything-we-know-about-how-the-nsa-tracks-peoples-physical-location/283745/.

a. Surveillance of U.S. Persons Under EO 12333 Violates the Fourth Amendment

EO 12333 is used to justify the unconstitutional warrantless surveillance of Americans' international communications—communications in which Americans have a reasonable expectation of privacy. This surveillance takes many different forms, nearly all of which the government currently conducts without any prior judicial authorization or court oversight. Although the government seeks to circumvent the warrant requirement on a number of grounds, none are availing. No court has recognized a foreign intelligence exception broad enough to justify the various forms of dragnet surveillance presently conducted under EO 12333. Moreover, the government is not exempted from the warrant requirement merely because its surveillance is conducted outside the United States, or because its surveillance is "targeted" at non-U.S. persons.

The Fourth Amendment does not require the government to obtain prior judicial authorization for surveillance of foreign targets merely because those foreign targets might at some point communicate with U.S. persons. But, compliance with the warrant clause requires, at the very least, that the government take reasonable measures to avoid the warrantless acquisition of Americans' international communications. If the government nonetheless acquires U.S. persons' communications in the course of warrantless surveillance, the Fourth Amendment generally forecloses it from retaining those communications. In the narrow circumstances in which the Fourth Amendment may permit the government to retain Americans' communications acquired without prior judicial approval, it generally forecloses the government from accessing or using those communications without first seeking a warrant based on probable cause.[39]

Many forms of EO 12333 surveillance would be unconstitutional even if the warrant clause did not apply. As discussed below, surveillance under EO 12333 that sweeps up Americans' communications lacks the traditional indicia of reasonableness. Indeed, it authorizes the kind of surveillance that led to the adoption of the Fourth Amendment in the first place—generalized surveillance based on general warrants. While the government plainly has a legitimate interest in collecting information about threats to the national security, the Fourth Amendment requires that the government pursue this interest with narrower means when the collection invades rights protected by the Constitution.

b. Surveillance of U.S. Persons Under EO 12333 Must Comply with the Warrant Requirement

As part of its examination, we urge the PCLOB to conclude that EO 12333 surveillance must comply with the warrant requirement. As explained below, the warrant requirement presumptively applies to the invasion of privacy of U.S. persons. It is not displaced by the government's broad invocation of its foreign-intelligence purpose in conducting EO 12333 surveillance. Nor is it rendered inapplicable by the foreign location of the government's surveillance or the fact that the government is invading U.S. persons' privacy in the course of "targeting" foreigners abroad. We urge the PCLOB to adopt the legal analysis below as part of its report on surveillance conducted under EO 12333.

i. Americans have a protected privacy interest in their international communications and metadata

[39] An amendment co-sponsored by then-Senator Obama corresponded to these principles, though it was directed at surveillance under Section 702 of FISA. The amendment would have prohibited the government from acquiring a communication without a warrant if it knew "before or at the time of acquisition that the communication [was] to or from a person reasonably believed to be located in the United States." *See* S. Amdt. 3979 to S. Amdt. 3911, 110th Cong. (2008). It would also have generally prohibited the government from accessing Americans' communications collected without a warrant based on probable cause. *Id*.

Americans have a constitutionally protected privacy interest in their telephone calls, emails, and other internet communications. As the Supreme Court observed in *Keith*, "broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[40]

Americans also have a constitutionally protected privacy interest in various types of metadata that may be associated with their electronic communications, accounts, or activities. The question for Fourth Amendment purposes is not whether a particular type of information is characterized as content or metadata, but whether it reveals information in which the individual has a reasonable expectation of privacy.[41] Metadata, especially when collected in bulk and aggregated across time, can reveal a wealth of detail about familial, political, professional, religious, and intimate relationships—the same kind of information that could traditionally be obtained only by examining the contents of communications. For that reason, the persistent or dragnet collection of metadata may invade a reasonable expectation of privacy and constitute a Fourth Amendment search.[42]

The expectation of privacy in both content and metadata extends not just to communications within the United States, but to information sent or stored internationally.[43] The mere fact that a U.S. person transmits information abroad—whether intentionally or inadvertently—does not extinguish his or her privacy interest in that information. Not even the government argues that a U.S. person forfeits all Fourth Amendment protection simply by communicating internationally or using technology that stores or transmits communications overseas.[44] Such a rule would be especially unsupportable given the global architecture of the Internet, where communications may traverse borders without the parties to those communications even knowing.[45] By the same token, the existence of a privacy interest does not depend on *where* the government

---

[40] United States v. U.S. Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 313 (1972) ("*Keith*"); United States v. Katz, 389 U.S. 347, 353 (1967); Alderman v. United States, 394 U.S. 165, 177 (1969); United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010).

[41] *See Katz*, 389 U.S. at 360–61 (Harlan, J., concurring);

[42] *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom.* United States v. Jones, 132 S. Ct. 945 (2012); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring).

[43] *See, e.g.*, United States v. Ramsey, 431 U.S. 606, 616–20 (1977) (holding that Fourth Amendment was implicated by statute that authorized customs officers to open envelopes and packages sent from outside the United States); Birnbaum v. United States, 588 F.2d 319, 325 (2d Cir. 1979); United States v. Doe, 472 F.2d 982, 984 (2d Cir. 1973); United States v. Bin Laden, 126 F. Supp. 2d 264, 281 (S.D.N.Y. 2000); *see also* United States v. Maturo, 982 F.2d 57, 61 (2d Cir. 1992) (holding that Fourth Amendment is engaged even by *foreign* governments' surveillance of Americans abroad if the U.S. government is sufficiently involved in the surveillance); United States v. Peterson, 812 F.2d 486 (9th Cir. 1987) (same); Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144 (D.D.C. 1976) (same).

[44] *See* In re Directives to Yahoo!, Inc. Pursuant to Section 105B, No. 105B(g): 07-01, at 55–56 & n.56 (FISC Apr. 25, 2008), http://bit.ly/1vE3Lgt (conceding that Americans have a privacy interest in international communications collected under the Protect America Act); Gov't Unclassified Resp. 26, United States v. Mohamud, No. 10-cr-00475 (D. Or. May 3, 2014) (ECF No. 509) (not contesting that the Fourth Amendment protects privacy of U.S. persons' international communications); Defs.' Mem. in Opp'n to Pls.' Mot. for Summ. J. 48, Amnesty Int'l USA v. McConnell, 646 F. Supp. 2d 633 (S.D.N.Y. 2009) (No. 08 Civ. 6259) (same).

[45] Even communications or data that Americans believe to be wholly domestic are frequently susceptible to interception abroad. For instance, major Internet service providers, such as Google and Yahoo!, store copies of their users' data in data centers around the world. To improve performance and balance traffic loads, these companies will periodically "synchronize" user data across data centers—which can result in the international transmission of U.S. person data for even purely domestic communications. *See* Barton Gellman, Todd Lindeman & Ashkan Soltani, *How the NSA Is Infiltrating Private Networks*, WASH. POST, (Oct. 30, 2013), https://www.washingtonpost.com/apps/g/page/world/how-the-nsa-is-infiltrating-private-networks/542/. Moreover, for

happens to acquire the communication, whether inside the United States or abroad.[46] The government cannot erase the legitimate privacy interests of U.S. persons simply by moving its surveillance of Americans' communications offshore.

ii. The warrant requirement presumptively applies to the interception of Americans' communications

Because Americans have a constitutionally protected privacy interest in their international communications, the government generally may not monitor these communications without first obtaining a warrant based on probable cause.[47] Warrantless searches are "per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."[48]

The Supreme Court has interpreted the warrant clause to require three things: (1) that any warrant be issued by a neutral, disinterested magistrate;[49] (2) that those seeking the warrant demonstrate to the magistrate "probable cause";[50] and (3) that any warrant particularly describe the things to be seized as well as the place to be searched.[51]

---

reasons associated with network topology, cost, and server availability, domestic Internet traffic of all kinds may naturally travel an international route.

In addition to these scenarios, Internet protocols can be deliberately manipulated by intelligence agencies to steer traffic abroad, where it can be intercepted with fewer restrictions. *See, e.g.*, Axel Arnback & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM. & TECH. L. REV. 317 (2015), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2460462. Indeed, a recently released document from the Government Communications Headquarters, a British intelligence organization, describes how the agency has "re-route[d] selective traffic across international links toward GCHQ's passive collection systems." Andrew Fishman & Glenn Greenwald, *Spied Hacked Computers Thanks to Sweeping Secret Warrants, Aggressively Stretching U.K. Law*, THE INTERCEPT (June 22, 2015), https://firstlook.org/theintercept/2015/06/22/gchq-reverse-engineering-warrants/ (quoting GCHQ memorandum).

[46] If it were true that Americans' communications lost all protection the moment they crossed the border, then the government could target those communications for surveillance directly. Indeed, it could dispense altogether with the doublespeak of "incidental collection" and simply collect and store all Americans' every international call and email, plus all those domestic communications that happen to be routed abroad. Accepting such a view would mean the government has absolutely unfettered discretion to scrutinize every word that crosses the country's borders.

[47] *See* Dalia v. United States, 441 U.S. 238, 256 n.18 (1979) ("electronic surveillance undeniably is a Fourth Amendment intrusion requiring a warrant"); *Keith*, 407 U.S. at 313; *Katz*, 389 U.S. at 356; United States v. Figueroa, 757 F.2d 466, 471 (2d Cir. 1985) ("even narrowly circumscribed electronic surveillance must have prior judicial sanction"); United States v. Tortorello, 480 F.2d 764, 773 (1973).

[48] United States v. Karo, 468 U.S. 705, 717 (1984); *see* Payton v. New York, 445 U.S. 573 (1980); Chimel v. California, 395 U.S. 752, 768 (1969); *Katz*, 389 U.S. at 357.

[49] *Katz*, 389 U.S. at 357; *see also* Shadwick v. City of Tampa, 407 U.S. 345, 350 (1972) (stating that a "neutral, disinterested magistrate" must be someone other than an executive officer "engaged in the often competitive enterprise of ferreting out crime"); *Keith*, 407 U.S. at 316–17 ("The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised."); McDonald v. United States, 335 U.S. 451, 455–56 (1948) ("The right of privacy was deemed too precious to entrust to the discretion of those whose job is the detection of crime and the arrest of criminals.").

[50] *Keith*, 407 U.S. at 316. Probable cause "is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness." Camara v. Municipal Court of S.F., 387 U.S. 523, 534 (1967).

[51] Maryland v. Garrison, 480 U.S. 79, 84 (1987); *see also* United States v. Silberman, 732 F. Supp. 1057, 1061–62 (1990) ("[T]he particularity clause requires that a statute authorizing a search or seizure must provide some means of limiting the place to be searched in a manner sufficient to protect a person's legitimate right to be free from unreasonable searches and seizures."); *see also* United States v. Bianco, 998 F.2d 1112, 1115 (2d Cir. 1993) (stating that the particularity requirement "prevents a general, exploratory rummaging in a person's belongings" (internal

The importance of the particularity requirement "is especially great in the case of eavesdropping," because eavesdropping inevitably leads to the interception of intimate conversations that are unrelated to the investigation.[52] In the context of electronic surveillance, the requirement of particularity generally demands that the government identify or describe the person to be surveilled, the facilities to be monitored, and the particular communications to be seized.[53]

EO 12333 authorizes the Executive Branch to conduct electronic surveillance of U.S. persons' communications without complying with the warrant clause. While the government may not typically *target* a U.S. person without first applying for an order from the Foreign Intelligence Surveillance Court (FISC),[54] it routinely engages in the warrantless acquisition of Americans' communications win the course of bulk surveillance and surveillance directed at non-U.S. persons abroad. EO 12333 and its implementing regulations expressly contemplate the warrantless acquisition of communications of U.S. persons.[55]

This surveillance violates all three prongs of the warrant requirement. Under EO 12333, the government may monitor U.S. persons' communications with foreigners without prior judicial review,[56] without any evidence of wrongdoing,[57] and without any meaningful limit on the scope of the surveillance conducted. The last failing bears particular emphasis. The government's surveillance under EO 12333 may be targeted, bulk, or anything in between. Unlike FISA, EO 12333 does not require the government's surveillance to be individualized.[58] It does not limit the government's surveillance to any particular facilities, telephone lines, email addresses, places, premises, or property.[59] It does not limit the kinds of communications the government can acquire, beyond requiring that a programmatic purpose of the surveillance be to gather foreign intelligence.[60] Nor, finally, does it require the government to identify in advance "the particular conversations to be seized."[61] To the contrary, the government may surveil entire populations, geographic regions, Internet backbone chokepoints, or electronic communications service providers—in each case, implicating the communications of millions.[62]

---

quotation marks omitted)). The particularity requirement is designed to leave nothing "to the discretion of the officer executing the warrant." Andresen v. Maryland, 427 U.S. 463, 480 (1976).

[52] *Berger*, 388 U.S. at 65 (Douglas, J., concurring) ("The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations."); *see also Tortorello*, 480 F.2d at 779.

[53] *See* United States v. Donovan, 429 U.S. 413, 427 n.15, 428 (1977).

[54] 50 U.S.C. § 1881c.

[55] *See, e.g.*, United States Signals Intelligence Directive SP0018 ("USSID 18") §§ 4.3, 5.1, 5.4(d), 6.1, 7.2, 7.4.

[56] *Katz*, 389 U.S. at 357.

[57] *Cf.* 18 U.S.C. § 2518(3) (permitting government to conduct surveillance under Title III only after court makes probable cause determination); 50 U.S.C. § 1805(a)(2) (corresponding provision for FISA).

[58] *Cf.* 18 U.S.C. § 2518(1)(b)(iv) (requiring Title III application to include "the identity of the person, if known, committing the offense and whose communications are to be intercepted"); 50 U.S.C. § 1804(a)(2) (requiring FISA application to describe "the identity, if known, or a description of the target of the electronic surveillance").

[59] *Cf.* 18 U.S.C. § 2518(1)(b)(ii); 50 U.S.C. § 1804(a)(3)(b).

[60] *Cf.* 50 U.S.C. § 1804(a)(6) (allowing issuance of FISA order only upon certification that a significant purpose of the specific intercept is to obtain foreign intelligence information).

[61] *Donovan*, 429 U.S. at 427 n.15; *cf.* 18 U.S.C. § 2518(1)(b)(iii); 50 U.S.C. § 1804(a)(6).

[62] *See, e.g.*, Ryan Devereaux et al., *supra* note 23 (describing comprehensive NSA monitoring of phone calls in the Bahamas); Barton Gellman et al., *How We Know the NSA Had Access to Internal Google and Yahoo Cloud Data*, WASH. POST, (Nov. 4, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/04/how-we-know-the-nsa-had-access-to-internal-google-and-yahoo-cloud-data/; Barton Gellman & Matt DeLong, *One Month, Hundreds of Millions of Records Collected*, WASH. POST, (Nov. 4, 2013), http://apps.washingtonpost.com/g/page/world/one-month-hundreds-of-millions-of-records-collected/554/.

iii. The warrant clause is not rendered inapplicable by the fact that the government's surveillance is conducted for foreign intelligence purposes

The government has contended that the warrant requirement does not apply to surveillance undertaken for foreign intelligence purposes because such surveillance falls within the "special needs" doctrine.[63] This is incorrect. Courts recognize an exception to the warrant requirement only "in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable."[64]

The mere fact that the government's surveillance is conducted for foreign intelligence purposes does not render the warrant and probable cause requirements unworkable. In *Keith*, the Supreme Court expressly rejected the government's argument that intelligence needs justified dispensing with the warrant requirement in domestic surveillance cases.[65] The Court's logic applies with equal force to surveillance conducted for foreign intelligence purposes—at least when that surveillance sweeps up U.S. persons' communications, as many forms of EO 12333 surveillance do.[66] History shows that the courts are capable of overseeing foreign intelligence surveillance of U.S. persons' communications: since 1978, the FISC has granted more than 33,000 applications relating to foreign intelligence surveillance.[67] Even in the context of surveillance conducted abroad, there is nothing impracticable about interposing a judge between the government and access to Americans' private information. Indeed, since the passage of the FISA Amendments Act in 2008, the FISC has overseen certain types of surveillance conducted on foreign soil.[68]

Even if there is a foreign intelligence exception to the warrant requirement, that exception is not broad enough to render EO 12333 surveillance of U.S. persons' communications constitutional. Prior to the passage of FISA, some courts permitted warrantless surveillance of foreign powers and their agents in certain limited circumstances.[69] But the country's experience with FISA profoundly undermines the rationale of those cases.[70] Moreover, the courts that recognized a foreign intelligence exception to the warrant requirement defined the exception very narrowly. They excused the government from the warrant requirement only where the surveillance in question was directed at foreign powers or their agents and

[63] *Cf., e.g.*, Gov't Unclassified Resp. 32–34, United States v. Mohamud, No. 10-cr-00475 (D. Or. May 3, 2014) (ECF No. 509) (arguing that Section 702 surveillance of Americans' international communications falls within the special needs doctrine).
[64] New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).
[65] 407 U.S. at 316–21.
[66] *See* Zweibon v. Mitchell, 516 F.2d 594, 613–14 (D.C. Cir. 1975); S. Rep. No. 95-701 at 15 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3984 (stating that the arguments in favor of prior judicial review "apply with even greater force to foreign counterintelligence surveillance"); United States v. Bin Laden, 126 F. Supp. 2d 264, 272, 274 n.9 (S.D.N.Y. 2000).
[67] *See, e.g.*, *Foreign Intelligence Surveillance Act Orders 1979–2014*, ELEC. PRIVACY INFO CTR., https://epic.org/privacy/wiretap/stats/fisa_stats.html (last visited Aug. 8, 2015); *FISA Annual Reports to Congress 1979–2014*, *Foreign Intelligence Surveillance Act*, FED'N OF AM. SCIS.,http://fas.org/irp/agency/doj/fisa/#rept (last visited Dec. 17, 2015).
[68] *See* 50 U.S.C. § 1881c.
[69] *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 912–15 (4th Cir. 1980); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 604–05 (3d Cir. 1974); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973).
[70] *See* United States v. Bin Laden, 126 F. Supp. 2d 264, 272 n.8 (S.D.N.Y. 2000).

predicated on an individualized finding of suspicion.[71] They also required that the surveillance be personally approved by the president or attorney general.[72]

The Foreign Intelligence Surveillance Court of Review's (FISCR) decision in *In re Directives* underscores these crucial limitations.[73] That case addressed the constitutionality of surveillance conducted under the Protect America Act, EO 12333, and Department of Defense regulations. In its analysis, the FISCR emphasized that, "[c]ollectively, these procedures require a showing of particularity, a meaningful probable cause determination, and a showing of necessity."[74] Thus, while the FISCR recognized a foreign intelligence exception, that exception was a narrow one:

> [W]e hold that a foreign intelligence exception to the Fourth Amendment's warrant requirement exists when surveillance is conducted to obtain foreign intelligence for national security purposes and *is directed against foreign powers or agents of foreign powers* reasonably believed to be located outside the United States.[75]

In addition, the exception was premised on a probable-cause determination certified by the attorney general himself. And, finally, the FISCR's conclusion that the surveillance was lawful rested on the government's assurance "that it does not maintain a database of incidentally collected information from non-targeted United States persons."[76]

EO 12333 authorizes the seizure and searching of U.S. persons' communications on far more permissive terms. Surveillance under EO 12333 is not directed only at foreign powers or agents of foreign powers reasonably believed to be located outside the United States, but may be directed at *any* non-citizen outside the United States. Surveillance under EO 12333 is not limited to "national security purposes," but can be used to acquire virtually any information relating to foreign powers, organizations, or persons.[77] Surveillance under EO 12333 entails no probable-cause determination whatsoever. Further, the targets of EO 12333 surveillance need not be personally approved by the president or the attorney general; that responsibility belongs to an unknown number of lower-level intelligence analysts. In short, as this Board itself has noted, no court has ever recognized a foreign intelligence exception sweeping enough to render constitutional the surveillance at issue here.[78]

iv. The warrant clause is not rendered inapplicable by the fact that the surveillance is conducted abroad

The warrant clause protects Americans' communications against government intrusion even when those seizures and searches are effected abroad. The Constitution does not cease to restrain the government's

[71] *See, e.g.*, United States v. Duka, 671 F.3d 329, 338 (3d Cir. 2011); *In re Sealed Case*, 310 F.3d 717, 720 (FISCR 2002); *Bin Laden*, 126 F. Supp. 2d at 277 (S.D.N.Y.).
[72] *See, e.g.*, *id.*; *Buck*, 548 F.2d at 875.
[73] 551 F.3d 1004 (FISCR 2008).
[74] *Id.* at 1016; *see id.* at 1007, 1013–14.
[75] *Id*. at 1012 (emphasis added).
[76] *Id*. at 1015.
[77] *See, e.g.*, USSID 18, *supra* note 12 at § 9.9.
[78] *See* PCLOB REPORT ON 702, *supra* note 14 at 90, n.411 ("It is not necessarily clear that the Section 702 program would fall within the *scope* of the foreign intelligence exception recognized by these decisions, which were limited to surveillance directly authorized by the Attorney General, targeting foreign powers or their agents, and/or pursuing foreign intelligence as the primary or sole purpose of the surveillance.").

conduct against its own citizens at the nation's borders, as the Supreme Court has made clear.[79] Adherence to the warrant requirement remains mandatory—even abroad—except in those circumstances where compliance would be "impracticable and anomalous."[80] In most scenarios, application of the warrant requirement to the overseas surveillance of Americans' communications is neither impracticable nor anomalous.

The Supreme Court's decision in *Verdugo-Urquidez* does not excuse the government from complying with the warrant requirement when it surveils U.S. persons overseas, because that decision focused exclusively on the Fourth Amendment protections available to foreign nationals. In *Verdugo-Urquidez*, a Mexican national was arrested in Mexico and extradited to the United States in connection with various narcotics offenses.[81] Following the defendant's arrest, American Drug Enforcement Administration ("DEA") agents—acting with the cooperation of Mexican authorities—conducted a warrantless search of his properties in Mexico and seized certain documents. The district court granted the defendant's motion to suppress the seized evidence, the Ninth Circuit affirmed, but the Supreme Court reversed. It held that, "[u]nder these circumstances," the Fourth Amendment had no application.[82] The majority opinion focused on several relevant factors, including; (a) Verdugo-Urquidez's status as a citizen and resident of Mexico, (b) his lack of voluntary attachment to the United States, and (c) the location of the place searched.[83] Nowhere did the Court's analysis suggest that U.S. government searches of American citizens or their communications abroad are exempt from the Fourth Amendment's warrant requirement.[84]

Justice Kennedy joined the Court's opinion but also wrote separately, stating that the relevant question is whether adherence to the warrant clause under the circumstances would be "impracticable and anomalous."[85] Nearly twenty years later, in *Boumediene*, a majority of the Court endorsed this functional approach to the extraterritorial application of constitutional rights.[86] Under either the majority's reasoning in *Verdugo-Urquidez* or the "impracticable and anomalous" test, the warrant requirement applies to overseas surveillance of Americans' communications.

---

[79] *See* Reid v. Covert, 354 U. S. 1, 5 (1957) (plurality) (rejecting "the idea that when the United States acts against citizens abroad it can do so free of the Bill of Rights"); *see also United States v. Verdugo-Urquidez*, 494 U.S. 259, 283 n.7 (1990) (Brennan, J., dissenting) (recognizing "the rule, accepted by every Court of Appeals to have considered the question, that the Fourth Amendment applies to searches conducted by the United States Government against United States citizens abroad"); *United States v. Toscanino*, 500 F.2d 267, 280–81 (2d Cir. 1974) (observing that it is "well settled" that "the Bill of Rights has extraterritorial application to the conduct abroad of federal agents directed against United States citizens").

[80] United States v. Verdugo-Urquidez, 494 U.S. 259, 277–78 (1990) (Kennedy, J., concurring); *see also* Boumediene v. Bush, 553 U.S. 723, 759–60 (2008) (adopting functional test for application of constitutional rights abroad).

[81] *See Verdugo-Urquidez*, 494 U.S. at 262.

[82] *Id.* at 275.

[83] *See id.* at 274–75.

[84] *See, e.g.*, *id.* at 274 (describing costs associated with "the application of the Fourth Amendment abroad to aliens").

[85] *See id.* at 278. In dissent, Justice Brennan incorrectly characterized Justice Kennedy's rejection of the warrant requirement as based solely on "the location of the search." *See id.* at 294 n.13 (Brennan, J., dissenting). Although Justice Kennedy asserted that the warrant requirement "should not apply in Mexico as it does in the United States," the animating principle of his concurrence is that several factors—not only geography—are relevant to the extraterritorial application of the warrant requirement. Indeed, Justice Kennedy emphasized that "[i]n cases involving the extraterritorial application of the Constitution, we have taken care to state whether the person claiming its protection is a citizen," and that "[t]he rights of a citizen, *as to whom the United States has continuing obligations*, are not presented by this case." *Id.* at 278 (emphasis added).

[86] *See Boumediene*, 553 U.S. at 759–60 (citing Justice Kennedy's concurrence in *Verdugo-Urquidez*); *see also id.* at 764, 766 (explaining that "at least three factors" are relevant in determining the reach of the Suspension Clause, including the citizenship and status of the claimant).

In truth, it is the government's effort to dispense with the warrant requirement overseas that is anomalous. Such a rule introduces an unjustifiable and arbitrary distinction in the legal standards that protect U.S. persons' communications, based on factors Americans cannot control or account for, including: (1) the unpredictable route that any given communication, even a wholly domestic one, travels; and (2) the location of the government's surveillance. In a world where communications increasingly disregard national borders—generally without the knowledge of or notice to those communicating—U.S. persons should not lose the core protection of the Fourth Amendment simply because the government chooses to move its surveillance offshore.[87] Introducing such a distinction creates perverse incentives: it encourages the government to engage in sweeping bulk and "incidental" surveillance of U.S. persons from points abroad, where the rules are far more permissive. In short, it promotes a collect-it-all approach, where no one is "targeted" but everyone may be surveilled.

Furthermore, it is not impracticable to require the government to take reasonable measures when engaged in spying abroad to avoid the warrantless surveillance of Americans. Congress already requires prior judicial review and probable cause when the government seeks to *target* U.S. persons abroad,[88] offering clear evidence that the mere location of EO 12333 surveillance cannot justify dispensing with the core requirements of the warrant clause.[89] In the absence of exigent circumstances, the government must take reasonable measures to avoid warrantless acquisition of U.S. persons' communications. Yet apart from the prohibition on targeting U.S. persons, neither EO 12333 nor its implementing regulations require that the government take sufficient steps to minimize its warrantless acquisition of Americans' communications in the first instance.[90]

---

[87] Notably, the government itself has insisted that the applicable legal standards should not turn on where its surveillance occurs, agreeing that such a distinction is arbitrary and anomalous. *See* Gov't Unclassified Resp. 14, United States v. Mohamud, No. 10-cr-00475 (D. Or. May 3, 2014) (ECF No. 509) ("In [today's] environment, regulating communications differently based on the location of collection arbitrarily limits the government's intelligence-gathering capabilities."); *FISA for the 21st Century: Hearing before the S. Comm. On the Judiciary*, 109th Cong., 2d Sess. (Jul. 26, 2006) (statement of then-NSA Director General Michael V. Hayden) ("As long as a communication is otherwise lawfully targeted, we should be indifferent to where the intercept is achieved."); *Modernizing the Foreign Intelligence Surveillance Act: Hearing before the S. Select Comm. on Intel.*, 110th Cong., 1st Sess. (May 1, 2007) (statement of then-DNI J. Michael McConnell) (criticizing FISA for placing "a premium on the location of the collection").

[88] *See* 50 U.S.C. § 1881c.

[89] Congress's adoption of Section 704 of FISA, 50 U.S.C. § 1881c, undercuts several court decisions that have found the warrant clause inapplicable to surveillance of U.S. persons abroad based, in part, upon the conclusion that such a requirement would be impractical. *See* United States v. Barona, 56 F.3d 1087, 1092 n.1 (9th Cir. 1995); In re Terrorist Bombings, 552 F.3d 157, 170 (2d Cir. 2008) (quoting *Barona*).

[90] In a variation on this theory, the government has also suggested that the border-search doctrine permits the warrantless acquisition of Americans' international communications, wherever they might be found. *See, e.g.*, Gov't Unclassified Resp. 32–33, 49–50, United States v. Mohamud, No. 10-cr-00475 (D. Or. May 3, 2014) (ECF No. 509). But the border-search doctrine does not permit the surveillance of Americans' communications absent individualized suspicion, let alone far removed from any border crossing. Indeed, the doctrine does not even apply outside the context of individuals or property physically at a border. Even if it did, it does not permit the suspicionless review of private communications. The Supreme Court has made clear that the doctrine exists to serve the government's interest in "stopping and examining persons and property crossing into this country." United States v. Ramsey, 431 U.S. 606, 616 (1977) (emphasis added); *accord* United States v. Flores-Montano, 541 U.S. 149, 152 (2004). In its seminal case on the matter, moreover, the Court noted that, under the regulations at issue, "envelopes are opened at the border only when the customs officers have reason to believe they contain other than correspondence, while the reading of any correspondence inside the envelopes is forbidden." *Ramsey*, 431 U.S. at 624. It is not surprising, therefore, that "[e]ven at the border, [courts have] rejected an 'anything goes' approach." United States v. Cotterman, 709 F.3d 952, 957 (9th Cir. 2013) (requiring reasonable suspicion before a thorough review of a laptop at the border), *cert. denied*, 134 S. Ct. 899 (2014); *see also* Lamont v. Postmaster Gen. of the United States, 381 U.S. 301 (1965) (invalidating registration requirement for recipients of certain foreign mail).

v. The warrant clause is not rendered inapplicable by the fact that the government is not "targeting" U.S. persons

The government has argued that the warrant clause is not engaged when the government collects U.S. persons' communications "incidentally" in the course of surveillance targeting non-U.S. persons abroad. But the rule the government relies upon—sometimes called the "incidental overhear" rule—has no application here.

First, the surveillance of Americans' communications under EO 12333 is not merely "incidental." Although the government frequently uses this label, the acquisition of Americans' communications under EO 12333 surveillance is foreseeable and significant.[91] Far from requiring the government to diligently avoid and purge Americans' communications as one might expect, the rules governing EO 12333 surveillance explicitly permit the government wide latitude to acquire and exploit Americans' information. They allow the government to surveil Americans' communications even when that surveillance is entirely foreseeable—as it is in the course of bulk collection—and preventable.[92] They allow the government to retain those communications for at least five years by default—even if they contain nothing of interest—and indefinitely in many circumstances.[93] They also allow the government to review, query, and disseminate those communications for a variety of intelligence and law-enforcement purposes, including in investigations of Americans.[94] In short, under the guise of surveilling foreigners, the government has granted itself sweeping permission to warrantlessly acquire and access the communications of those who enjoy the full protection of the Fourth Amendment.

Second, the "incidental overhear" cases involve surveillance predicated on warrants—that is, they involved circumstances in which courts had found probable cause regarding the government's targets and had defined with particularity the facilities to be monitored.[95] In other words, the "incidental overhear" rule has been applied only where a court has carefully circumscribed the government's surveillance and limited its intrusion into the privacy of third parties.[96] The same cannot be said of *warrantless* surveillance under EO 12333 directed at foreigners abroad.[97]

---

[91] *Cf.* PCLOB REPORT ON 702 *supra* note 14 at 82 ("The collection of communications to and from a target inevitably returns communications in which non-targets are on the other end, some of whom will be U.S. persons. Such "incidental" collection of communications is not accidental, nor is it inadvertent.) (footnotes omitted).

[92] Outside of a narrow prohibition on the "targeting" of specific U.S. person communications (which is itself subject to a number of exceptions), these rules allow the government to knowingly and intentionally acquire Americans' communications. *See, e.g.*, USSID 18, *supra* note 12 at § 4.1; Dep't of Defense Reg. 5240.1-R §§ C5.2.2.1, C5.3.1.1, C5.3.3.1–2 (1982), http://bit.ly/1ffjRaR; PPD 28, *supra* note 28 at § 2 (Jan. 17, 2014) (authorizing bulk collection). They do not require it to take any steps to avoid or minimize the acquisition of those communications.

[93] USSID 18, *supra* note 12 at § 6.1.

[94] *See, e.g.*, USSID 18 §§ 5.1, 5.4, 7.2, 7.4; Dep't of Defense, Supplemental Procedures Governing Communications Metadata Analysis (attached to Memorandum for the Attorney General from Kenneth Wainstein, Nov. 20, 2007, http://bit.ly/1ews8pL).

[95] *See, e.g.*, United States v. Kahn, 415 U.S. 143 (1974); United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985).

[96] *See Donovan*, 429 U.S. at 436 n.24 (holding that while a warrant is not made unconstitutional by "failure to identify every individual who could be expected to be overheard," the "complete absence of prior judicial authorization would make an intercept unlawful"); United States v. Yannotti, 399 F. Supp. 2d 268, 274 (S.D.N.Y. 2005); PCLOB REPORT ON 702, *supra* note 14 at 95.

[97] Notably, the FISCR's reasoning on this point in *In re Directives* is little more than a tautology—expressing the view that "constitutionally permissible" surveillance is not "unlawful," without analyzing the legal question further. 551 F. 3d at 1015 ("It is settled beyond peradventure that incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."). More important to the FISCR's analysis, it seems, was the government's assurance that "it does not maintain a database of incidentally collected information

Applying the incidental-overhear doctrine in this context would have dramatic implications. The volume of communications that appears to be intercepted "incidentally" under EO 12333 dwarfs that of communications intercepted incidentally under original FISA, Title III, and likely Section 702 as well. The scale of incidental collection is a direct consequence of the fact that EO 12333 permits suspicionless targeting and bulk collection and retention.[98] Under the government's theory, EO 12333 even allows the NSA to review the contents of millions of Americans' communications for information "about" the government's targets using an even more extreme form of upstream surveillance.[99] The government's use of the term "incidental" is meant to convey the impression that its collection of Americans' communications under EO 12333 is a *de minimis* byproduct common to all forms of surveillance. But whereas surveillance under Title III or the original FISA might lead to the incidental collection of a handful of people's communications, surveillance under EO 12333 invades the privacy of countless Americans whose communications happen to transit networks abroad.

The government's effort to stretch the incidental overhear doctrine to cover its dragnet surveillance of Americans' international communications reflects a view that constitutional rules designed for an era of individualized surveillance can be applied blindly to broad programs of suspicionless or warrantless surveillance. This view is wrong. The Supreme Court has made clear that existing rules must be evaluated anew when it comes to novel forms of electronic searches, especially those that expose private information to government surveillance on a scale never before possible.[100]

vi. If the government acquires Americans' communications without a warrant, it must obtain one before accessing, using, or searching for those communications

Based on the analysis above, we urge the PCLOB to conclude that the Executive Branch must obtain a warrant before accessing, using, or searching the communications of Americans acquired through EO 12333 surveillance programs.

If the government acquires Americans' communications without a warrant in the course of EO 12333 surveillance, it must obtain a warrant when it seeks to exploit those communications. This requirement flows from the differences between the purpose of the initial acquisition and the later exploitation. At the outset, the government avoids complying with the warrant clause only because it claims its surveillance is directed at the communications of foreigners. But when the government later seeks to deliberately retain, use, or search for the communications of Americans, the scope and purpose of the surveillance has changed—and, at that point, the government must adhere to the Fourth Amendment rules that protect U.S. persons. As the Supreme Court said in *Terry v. Ohio*, "[t]he scope of [a] search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible."[101] A corollary to this requirement

---

from non-targeted United States persons"—an assurance that is not true now even if it was then. *Id.*; *see, e.g.*, USSID 18, *supra* note 12 at §§ 4.1, 4.3, 5.1 (permitting the NSA to retain, review, and query incidentally acquired communications of U.S. persons).

[98] *Cf.* PCLOB REPORT ON 702, *supra* note 14 at 116, ("[T]he expansiveness of the governing rules, combined with the technological capacity to acquire and store great quantities of data, permit the government to target large numbers of people around the world and acquire a vast number of communications.").

[99] USSID 18, *supra* note 12 at § 5.1.

[100] *See* Riley v. California, 134 S. Ct. 2473, 2488 (2014) (refusing to extend rules for physical searches to digital contents of cell phones); United States v. Jones, 132 S. Ct. 945, 954 & n.6 (2012) (recognizing that persistent collection of data raises different constitutional questions).

[101] 392 U.S. 1, 19 (1968) (quoting Warden v. Hayden, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)); *see also* Mincey v. Arizona, 437 U.S. 385, 393 (1978) ("[A] warrantless search must be "strictly circumscribed by the exigencies which justify its initiation") (quoting *Terry*, 392 U.S. at 25–26).

is the rule that an expanded search—one seeking different information or implicating different legal interests—requires an expanded legal justification.[102] This is especially crucial in the case of electronic searches or surveillance, where the government often over-collects data to facilitate its initial search.[103] When the government later seeks to exploit that data in the service of a new or broader investigative purpose, it must obtain legal authority corresponding to that new purpose.[104] The government apparently agrees with this basic proposition.[105] Yet the government does not seek judicial authorization before exploiting communications obtained under EO 12333 in investigations of U.S. persons.[106]

c. Even if the Warrant Requirement Does Not Apply, Surveillance of U.S. Persons Under EO 12333 is Unreasonable

Much of the surveillance of U.S. persons that the government is conducting under EO 12333 and its implementing regulations would be unconstitutional even if the warrant clause were inapplicable, because that surveillance is unreasonable. It is unreasonable because it entails sweeping surveillance of Americans' international communications with few, if any, meaningful restrictions on the acquisition, use, and dissemination of those communications. We urge the PCLOB to conclude as much and to recommend that the government adopt the proposals in Section III to more closely conform surveillance under EO 12333 to the Constitution's requirements.

"The ultimate touchstone of the Fourth Amendment is reasonableness," [107] and the reasonableness requirement applies even where the warrant requirement does not.[108] Reasonableness is determined by examining the "totality of circumstances" to "assess[], on the one hand, the degree to which [government

[102] *See* Rodriguez v. United States, 135 S. Ct. 1609, 1614–15 (2015) (prolonged detention for new investigative purpose required independent Fourth Amendment justification); Arizona v. Hicks, 480 U.S. 321, 326–29 (1987) (emergency justification for entry of home did not permit examination of stereo equipment for evidence of theft beyond what was in plain view); United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("Even when government agents may lawfully seize [] a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package.").

[103] *See, e.g.*, United States v. Comprehensive Drug Testing, *Inc.*, 621 F. 3d 1162, 1168, 1176 (9th Cir. 2010) (en banc) ("The government sought the authority to seize considerably more data than that for which it had probable cause, including various computers or computer hard drives and related storage media . . . ."); United States v. Ganias, 755 F.3d 125, 135 (2d Cir. 2014) (en banc review pending).

[104] *See, e.g.*, United States v. Sedaghaty, 728 F.3d 885, 910–13 (9th Cir. 2013) ("[T]he government should not be able to comb through [the defendant's] computers plucking out new forms of evidence that the investigating agents have decided may be useful, at least not without obtaining a new warrant."); United States v. Crist, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2012) (warrant required to expand electronic search of computer hard-drive); *Ganias*, 755 F.3d at 139–40 (prohibiting government from indefinitely retaining copied data outside the scope of the original warrant); *Comprehensive Drug Testing, Inc.*, 621 F. 3d at 1171 (prohibiting government from exploiting commingled data to search for information outside the scope of the original warrant); *cf.* United States v. Heldt, 668 F.2d 1238, 1266 (D.C. Cir. 1981) ("[T]he particularity requirement of the fourth amendment prevents the seizure of one thing under a warrant describing another.") (internal quotation marks and citation omitted).

[105] *See Ganias*, 755 F.3d at 129–30 (describing government agents' decision to obtain second warrant authorizing expanded search of previously seized computer data).

[106] As noted above, this scenario is fundamentally different from cases where individuals are overheard in the course of a Title III or traditional FISA wiretap—because in those cases the government has made a showing of probable cause to a neutral judicial officer before undertaking the surveillance. *See* Section II(B)(5), *supra*.

[107] *See* Brigham City v. Stuart, 547 U.S. 398, 403 (2006) (quotation marks omitted).

[108] United States v. Montoya de Hernandez, 473 U.S. 531, 539 (1985); *see In re Sealed Case*, 310 F.3d at 737 (assessing reasonableness of FISA); *Figueroa*, 757 F.2d at 471–73 (Title III); United States v. Duggan, 743 F.2d 59, 73–74 (2d Cir. 1984) (assessing reasonableness of FISA); United States v. Tortorello, 480 F.2d 764, 772–73 (2d Cir. 1973) (Title III).

conduct] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests."[109] In the context of electronic surveillance, reasonableness demands that government eavesdropping be "precise and discriminate" and "carefully circumscribed so as to prevent unauthorized invasions of privacy."[110] Courts that have assessed the lawfulness of electronic surveillance have often looked to Title III as one measure of reasonableness.[111] While constitutional limitations on foreign intelligence surveillance may differ in some respects from those applicable to law enforcement surveillance,[112] "the closer [the challenged] procedures are to Title III procedures, the lesser are [the] constitutional concerns."[113]

i. Surveillance of U.S. persons under EO 12333 lacks the traditional indicia of reasonableness

Surveillance of U.S. persons under EO 12333 and its implementing regulations lacks the indicia of reasonableness that courts have cited in upholding surveillance under Title III and traditional FISA.[114] Whereas both FISA and Title III require the government to identify to a court its targets and the facilities it intends to monitor, EO 12333 and its implementing regulation do not. Whereas both traditional FISA and Title III require the government to demonstrate individualized suspicion to a court, EO 12333 and its implementing regulations do not. (Indeed, neither EO 12333 nor its implementing regulations, so far as we know, require even an administrative finding of individualized suspicion.) And, whereas both FISA and Title III impose strict limitations on the nature of the communications that the government may monitor and the duration of its surveillance, EO 12333 and its implementing regulations do not.

In other words, whereas Title III and FISA permit monitoring of suspected criminals and agents of foreign powers in narrow circumstances, EO 12333 and its implementing regulations permit the warrantless and suspicionless monitoring of virtually any foreigner outside the United States, even if and when those people are communicating with U.S. persons.

For Americans whose communications are swept up under EO 12333 surveillance, the principal protection is the requirement—which, for the NSA, comes from USSID 18—that the government "minimize" the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting U.S. persons.[115] The protection provided by the minimization rules, however, is largely illusory.

---

[109] Samson v. California, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also* Virginia v. Moore, 553 U.S. 164, 169–70 (2008).

[110] *Berger*, 388 U.S. at 58 (quotation marks omitted); *see* United States v. Bobo, 477 F.2d 974, 980 (4th Cir. 1973) ("[W]e must look . . . to the totality of the circumstances and the overall impact of the statute to see if it authorizes indiscriminate and irresponsible use of electronic surveillance or if it authorizes a reasonable search under the Fourth Amendment.").

[111] *See, e.g.*, United States v. Mesa-Rincon, 911 F.2d 1433, 1438 (10th Cir. 1990) (evaluating reasonableness of video surveillance); United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986) (same); United States v. Torres, 751 F.2d 875, 884 (7th Cir. 1984) (same).

[112] *See Keith*, 407 U.S. at 323–24.

[113] *In re Sealed Case*, 310 F.3d at 737

[114] *See, e.g.*, *Duggan*, 743 F.2d at 73 (FISA); United States v. Pelton, 835 F.2d 1067, 1075 (4th Cir. 1987) (FISA); United States v. Cavanagh, 807 F.2d 787, 790 (9th Cir. 1987) (FISA); *In re Sealed Case*, 310 F.3d at 739–40 (FISA); *In re Kevork*, 634 F. Supp. 1002, 1013 (C.D. Cal. 1985) (FISA), *aff'd*, 788 F.2d 566 (9th Cir. 1986); United States v. Falvey, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (FISA); *Tortorello*, 480 F.2d at 773–74 (Title III); *Bobo*, 477 F.2d at 982 (Title III); United States v. Cafero, 473 F.2d 489, 498 (3d Cir. 1973) (Title III).

[115] *See generally* USSID 18, *supra* note 12 §§ 4–7.

First, as explained further below, the rules do not impose any meaningful obligation to avoid the acquisition of U.S. persons' communications; nor do they require the government to promptly purge those communications once acquired.[116] To the contrary, the government may retain U.S. persons' communications for a minimum of five years, or indefinitely if they contain "foreign intelligence" information.[117] That phrase is defined under USSID 18 so broadly as to encompass not just information relating to terrorism, but any information relating to "the capabilities, intentions, and activities of foreign powers, organizations, or persons."[118] Notably, that definition is significantly broader than the definition of "foreign intelligence information" under FISA.[119]

Second, unlike Title III and FISA, EO 12333 does not require that minimization be particularized with respect to individual targets, and it does not subject the government's implementation of minimization requirements to judicial oversight. Title III requires the government to conduct surveillance "in such a way as to minimize the interception of" innocent and irrelevant conversations.[120] It strictly limits the use and dissemination of material obtained under the statute.[121] It also authorizes courts to oversee the government's compliance with minimization requirements.[122] FISA similarly requires that each order authorizing surveillance of a particular target contain specific minimization procedures governing that particular surveillance.[123] It also provides the FISC with authority to oversee the government's minimization on an individualized basis during the course of the surveillance.[124]

Under EO 12333, minimization is not individualized but programmatic, with default rules that favor long-term retention. Moreover, no court has authority to supervise the government's compliance with the minimization requirements at any point—there is no requirement that the government seek judicial approval before it analyzes, retains, or disseminates U.S. communications.[125] This defect is particularly significant because EO 12333 does not provide for individualized judicial review at the acquisition stage. Under FISA and Title III, minimization operates as a second-level protection against the acquisition, retention, and dissemination of information relating to U.S. persons. The first level of protection comes from the requirement of individualized judicial authorization for each specific surveillance target.[126] Under

---

[116] *See* NSA/CSS POLICY 1-23: PROCEDURES GOVERNING ACTIVITIES OF NSA/CSS THAT AFFECT U.S. PERSONS § 4 (May 29, 2009) ("The United States Signals Intelligence System may collect, process, retain and disseminate foreign communications that are also communications of, or concerning, United States persons.").

[117] The NSA's minimization procedures also permit the indefinite retention of U.S. persons' communications that are encrypted. USSID 18, *supra* note 12 § 6.1(a)(2).

[118] *See, e.g.*, USSID 18 *supra* note 12 §§ 6.1, 9.9.

[119] *See* 50 U.S.C. § 1801(e)(2)(B) (defining "foreign intelligence information" to include "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to the conduct of the foreign affairs of the United States").

[120] 18 U.S.C. § 2518(5); *see id.* (stating that "every order and extension thereof shall contain a provision" regarding the general minimization requirement).

[121] *See* 18 U.S.C. § 2517.

[122] 18 U.S.C. § 2518(6).

[123] *See* 50 U.S.C. § 1804(a)(4); *id.* § 1805(a)(3); *id.* § 1805(c)(2)(A).

[124] *See id.* § 1805(d)(3).

[125] *Cf. id.* § 1805(d)(3); *id.* § 1801(h)(4) (requiring court order in order to "disclose[], disseminate[], use[] . . . or retain[] for longer than 72 hours" U.S. communications obtained in the course of warrantless surveillance of facilities used exclusively by foreign powers).

[126] *Cf.* Scott v. United States, 436 U.S. 128, 130–31 (1978) ("'The scheme of the Fourth Amendment becomes meaningful only when it is assured that at some point the conduct of those charged with enforcing the laws can be subjected to the more detached, neutral scrutiny of a judge who must evaluate the reasonableness of a particular search or seizure in light of the particular circumstances.'" (quoting *Terry*, 392 U.S. 1 (1968))); United States v. James, 494 F.2d 1007, 1021 (D.C. Cir. 1971) ("The most striking feature of Title III is its reliance upon a judicial officer to supervise wiretap operations. Close scrutiny by a federal or state judge during all phases of the intercept, from the

EO 12333, by contrast, there is no first-level protection, because the statute does not call for individualized judicial authorization of specific surveillance targets (or, for that matter, of specific facilities to be monitored or specific communications to be acquired).

Thus, the minimization requirements of EO 12333's implementing regulations do not prevent intrusion into the privacy of innocent U.S. persons. The requirements do not prohibit the government from acquiring Americans' communications en masse and mining them for foreign intelligence information.

ii. Neither EO 12333 nor its implementing regulations meaningfully restrict the acquisition of U.S. persons' communications

Although the government claims to minimize the warrantless acquisition of U.S. persons' communications, EO 12333 and its implementing regulations impose few meaningful restrictions. In effect, there is but one restriction: the prohibition on intentionally targeting specific U.S. person communications.[127] So long as the government claims to be pursuing the communications of foreigners, whether on an individual or programmatic basis, it is free to acquire U.S. persons' communications without meaningful limitation.[128] The regulations do not require the government to take any meaningful efforts to avoid the warrantless acquisition of Americans' communications in the first instance.[129] The absence of such a requirement facilitates the warrantless acquisition of U.S. persons' communications, often on a massive scale.

Most significantly, it permits the government to engage in bulk acquisition of foreigners' communications without regard for the communications of Americans that will inevitably be swept up in the process. For example, under the MYSTIC program, the government is reportedly recording the content of every phone call made in, into, or out of a number of countries, including the Bahamas, even though Americans' communications will be captured, predictably and in great quantity. Likewise, under other programs, the NSA is reportedly acquiring billions of cellphone location records, as well as hundreds of millions of email and instant-message contact lists. Though this bulk collection takes place abroad, it has significant consequences for the privacy of U.S. persons.

Relatedly, USSID 18 expressly authorizes the government to scan the content of every communication it is able to intercept—including U.S. persons' communications—for keywords.[130] Although this surveillance is nominally similar to "about" surveillance under Section 702 of FISA, it is in fact significantly more intrusive. Under Section 702, the government scans the content of international communications to determine whether the communications mention certain "hard selectors," such as email addresses or phone numbers, associated with the government's targets. But USSID 18 specifically permits the use of keywords "intended to intercept a communication on the basis of the *content* of the communication . . . rather than on the basis of . . . the fact that the communication mentions a particular individual."[131] This bulk content review takes place with minimal protections for U.S. persons.[132]

---

authorization through reporting and inventory, enhances the protection of individual rights." (quotation marks omitted)); *Cavanagh*, 807 F.2d at 790.

[127] *See, e.g.*, USSID 18, *supra* note 12 § 4.1; Dep't of Defense Reg. 5240.1-R §§ C5.2.2.1, C5.2.3.

[128] *See, e.g.*, USSID 18, *supra* note 12 § 4.3; Dep't of Defense Reg. 5240.1-R § C5.3.3.1.

[129] Notably, EO 12333's "least intrusive means" requirement applies only to surveillance directed at specific U.S. persons, but has no application even where surveillance ostensibly directed at foreigners involves severe and foreseeable intrusions on the privacy rights of U.S. persons. *See* EO 12333, *supra* note 8 § 2.4; Dep't of Defense Reg. 5240.1-R § C2.4.2.

[130] *See, e.g.*, USSID 18, *supra* note 12 § 5.1.

[131] *Id.* (emphasis added).

[132] "Selection terms" that are likely to result, or have resulted, in the "interception" of U.S. persons' communications may only be used if "there is a reason to believe that foreign intelligence will be obtained" and the terms are designed

Finally, it is not clear whether EO 12333 or its implementing procedures prohibit even so-called "reverse targeting," whereby the government targets a foreigner to acquire his or her communications with a particular U.S. person.[133] The government has repeatedly cited such a prohibition in defending the constitutionality of Section 702,[134] but nothing in EO 12333 or its implementing regulations obviously disallows such surveillance.

iii. EO 12333 imposes weak restrictions on the retention and use of U.S. persons' communications

The procedures regulating the retention and use of U.S. persons' communications under EO 12333 also fail to provide meaningful protection. Even if the acquisition of U.S. persons' communications were unavoidable in certain circumstances, for technical or other reasons, one would expect the government to employ strong back-end procedures to "minimize" warrantless intrusions on the privacy of Americans. But the existing procedures do the opposite: they give the government broad latitude to exploit the data it warrantlessly acquires.

Rather than requiring the government to segregate or destroy any U.S. person communications acquired without a warrant, EO 12333 and its implementing regulations explicitly permit the government to retain, query, and analyze all incidentally acquired U.S. person communications for as long as five years by default.[135] Moreover, there are numerous exceptions to the five-year rule. If, for example, the government concludes that a U.S. person's communications contain foreign intelligence information (defined expansively) or evidence of a crime, it can retain the communications indefinitely and disseminate them to various other agencies, including in aid of law-enforcement investigations.[136] These broad exceptions apply even to U.S. person communications otherwise protected by the attorney–client privilege.[137]

In some circumstances, EO 12333's implementing regulations permit the government to retain even communications solely between U.S. persons or communications acquired through the erroneous targeting of U.S. persons—such as when the government determines that the contents of the communication contain "significant foreign intelligence information" or "evidence of a crime."[138] In other words, even when analysts have violated the NSA's own rules, senior officials have wide latitude to approve the retention and use of protected communications by granting so-called "destruction waivers."[139] NSA compliance reports

---

"to defeat, to the greatest extent practicable under the circumstances, the interception of those communications which do not contain foreign intelligence." *Id.* § 5.1(a)–(c).

[133] *Cf.* 50 U.S.C. § 1881a(b)(2).

[134] *See, e.g.*, Gov't Unclassified Mem. at 55, United States v. Muhtorov, No.12-cr-00033 (D. Colo. May 9, 2014) (ECF No. 559), *available at* https://www.aclu.org/sites/default/files/field_document/muhtorov_-_govt_response_to_motion_to_suppress.pdf.

[135] *See, e.g.*, USSID 18, *supra* note 12 § 6.1(a).

[136] *See, e.g.*, *id.* § 6.1(b); *id.* § 7.2(c).

[137] *See id.* § 7.4.

[138] *See, e.g.*, *id.* § 5.4(a), (d).

[139] It is unclear, more generally, how diligently the NSA applies its own destructions rules. While the procedures ostensibly require the government to destroy inadvertently acquired U.S. person communications upon recognition, *see* USSID 18, *supra* note 12 § 5.4(a)–(b), disclosures suggest that such requirements often have little or no force in practice. *Cf.* PCLOB Report 153 (observing that, in the case of Section 702 surveillance, the government's practice is to err on the side of retaining any piece of private information "that might in the future conceivably take on value or that some other analyst in the intelligence community might find to be of value"); Barton Gellman *et al.*, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014),

show that such waivers have been sought and approved in cases where analysts targeted U.S. persons or improperly selected their communications from raw-traffic databases.[140]

Finally, EO 12333 and its implementing regulations appear to allow the government to conduct so-called "backdoor searches," in which the government searches its repositories of EO 12333–intercepted communications and data specifically for information about U.S. citizens and residents. The PCLOB has previously expressed concern about backdoor searches in the context of Section 702 surveillance, and the President's Review Group has recommended prohibiting them under both Section 702 and Executive Order, concluding that the practice violates the "full protection of [Americans'] privacy."[141]

Given the breadth of surveillance under EO 12333, the procedures in place to protect the privacy of U.S. persons should be at least as robust as the minimization procedures that govern *warrantless* surveillance under FISA of facilities used exclusively by foreign agents.[142] Those procedures forbid the government from "disclos[ing], disseminat[ing], or us[ing] for any purpose or retain[ing] for longer than 72 hours" communications to which a U.S. person is a party, absent a court order under Title I of FISA or a determination by the Attorney General that "the information indicates a threat of death or serious bodily harm to any person."[143] Instead, the current procedures are considerably weaker than even those the FISC has imposed for surveillance under Section 702 of the FISA Amendments Act.

iv. EO 12333 fails to provide adequate notice and disclosure of surveillance to U.S. persons and is therefore unreasonable

We urge the PCLOB to make clear that existing notice and disclosure requirements under EO 12333 are deficient and need to be strengthened to comport with the Fourth Amendment. Surveillance under EO 12333 runs afoul of the Fourth Amendment for yet another reason: the government does not provide adequate notice and disclosure of its surveillance to U.S. persons. The requirement that the government give notice of its searches has deep roots in Anglo–American law—and is an essential element of the Fourth Amendment reasonableness inquiry.[144] In all but exceptional circumstances, when the government invades an individual's zone of privacy, it has a constitutional duty to provide notice of the intrusion at the time of the search.[145] That obligation is triggered by the search itself; it does not depend on the

---

http://wapo.st/1xyyGZF (reporting that the NSA's "policy is to hold on to 'incidentally' collected U.S. content, even if it does not appear to contain foreign intelligence.").

[140] *See, e.g.*, Memorandum for the Chairman, Intelligence Oversight Board 2, 4 (March 4, 2013), http://bit.ly/1JDfaif (reporting request for destruction waiver where a U.S. person's telephone number was improperly tasked and approval of destruction waiver where analyst "performed a query in a raw traffic database on a selector associated with a U.S. person"); Report to the Intelligence Oversight Board on NSA Activities 2 (Feb. 11, 2008), http://bit.ly/1el9VLx.

[141] *See* PCLOB REPORT ON 702, 137–40, 151–60; PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 149, 145–50 (2013), https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[142] *See* 50 U.S.C. §§ 1802(a), 1801(h)(4) (requiring far stricter minimization procedures where surveillance is undertaken without prior judicial authorization).

[143] *Id.* § 1801(h)(4).

[144] *See, e.g.*, Berger v. New York, 388 U.S. 41, 60 (1967) (striking down New York's wiretapping statute in part because it allowed no-notice searches "without any showing of exigent circumstances"); United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986) (finding "sneak-and-peak warrant" constitutionally defective for its failure to provide explicitly for notice within a reasonable time frame); *Wilson v. Arkansas*, 514 U.S. 927, 931–37 (1995) (describing common-law origins of the "knock-and-announce" rule and incorporating notice requirement into Fourth Amendment reasonableness analysis).

[145] The notice requirement is grounded not only in the Fourth Amendment right to privacy, but also in the due process rights of the Fifth Amendment. A search or seizure is a deprivation of liberty within the meaning of due process—it deprives an individual of a protected privacy interest. *See, e.g.*, West Covina v. Perkins, 525 U.S. 234, 240–41 (1999);

government's decision to use the fruits of its search in a criminal prosecution. Indeed, failures to provide adequate and timely notice have proven constitutionally fatal to government searches.[146] Although courts have on occasion upheld the constitutionality of delayed notice schemes, these opinions reflect the bedrock assumption that notice will be given to the subject of a search after no more delay than is reasonably necessary.[147] That notice ensures that individuals subjected to government searches have an opportunity to seek judicial review.[148] Nonetheless, the government typically does not provide *any* notice—even after the fact—to those subjected to EO 12333 surveillance. This failure significantly undermines any claim that EO 12333 surveillance is reasonable.[149]

The government also fails to provide adequate notice of EO 12333 surveillance when individuals' liberty is at stake—*i.e.*, in criminal prosecutions. Without notice, it is nearly impossible for defendants to exercise their Fourth and Fifth Amendment rights to challenge the admissibility evidence that has been unlawfully acquired.[150] Yet recent reports indicate that the government holds an unjustifiably narrow view of its notice obligations with respect to EO 12333 surveillance, even in criminal cases. Officials have insisted to *The New York Times* that "defendants have no right to know if 12333 intercepts provided a tip from which investigators derived other evidence."[151] The withholding of notice in these circumstances conflicts directly with the "fruit of the poisonous tree"[152] doctrine and defendants' constitutional right to seek suppression of unlawfully acquired evidence.

III. Policy Recommendations

Existing procedures governing the collection, retention, dissemination, and use of EO 12333 information are inadequate to meet the government's constitutional and international obligations. Given the legal and policy concerns associated with EO 12333 policies, we urge the PCLOB to recommend that Congress pass legislation consistent with the recommendations below. In addition, we urge the PCLOB to recommend that the Executive Branch adopt the recommendations below, until such legislation is adopted. It is

---

United States v. Minor, 228 F.3d 352, 356 (4th Cir. 2000); Willis v. United States, 787 F.2d 1089, 1093 (7th Cir. 1986). Thus, government searches and seizures trigger the familiar due process requirement of notice. *See* Mathews v. Eldridge, 424 U.S. 319, 348 (1976).

The government's constitutional obligation to provide notice is also reflected in Federal Rule of Criminal Procedure 41(f); its predecessors, Rule 41(d) and 18 U.S.C. § 622 (1928), required much the same. *See Katz v. United States*, 389 U.S. 347, 355 n.16 (1967); *see also, e.g.*, 18 U.S.C. § 3103a (permitting delayed notice only "where the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result").

[146] *See* Berger v. New York, 388 U.S. 41, 60 (1967); United States v. Freitas, 800 F.2d 1451, 1456 (9th Cir. 1986).

[147] *See, e.g.*, Dalia v. United States, 441 U.S. 238, 248 (1979) (observing that Title III provided a "*constitutionally adequate substitute for advance notice* by requiring that once the surveillance operation is completed[,] the authorizing judge must cause notice to be served on those subjected to the surveillance" (emphasis added)); United States v. Chun, 503 F.2d 533, 537–38 (9th Cir. 1974) (discussing Title III notice requirements).

[148] Notice, of course, is a prerequisite for any post-deprivation hearing or challenge, such as a claim for civil damages, a motion for return of property, or a motion to suppress evidence.

[149] *See Berger*, 388 U.S. at 60; *cf.* Richards v. Wisconsin, 520 U.S. 385, 392–95 (1997) (rejecting the Wisconsin court's "blanket exception" to the knock-and-announce requirement for felony drug cases, which would "impermissibly insulate[]" many cases from judicial review).

[150] *See, e.g.*, United States v. U.S. District Court (Keith), 407 U.S. 297 (1972).

[151] Charlie Savage, *Reagan-Era Order on Surveillance Violates Rights, Says Departing Aide*, N.Y. TIMES (Aug. 13, 2014), http://www.nytimes.com/2014/08/14/us/politics/reagan-era-order-on-surveillance-violates-rights-says-departing-aide.html?_r=0; *see also* United States v. Muhtorov, Gov't Consolidated Resp., No. 12-cr-00033-JLK (D. Colo. Feb. 26, 2015) (ECF No. 711) (declining to address defendants' arguments concerning the constitutional bases for notice of EO 12333 surveillance).

[152] *See, e.g.*, Alderman v. United States, 394 U.S. 165 (1969).

important to note that we do not believe that adoption of the recommendations below would be sufficient to fully address the civil and human rights concerns associated with EO 12333 activities. Notwithstanding this, however, we believe that they would provide meaningful protections for the rights of Americans and individuals abroad.

a. Collection

Surveillance under EO 12333 involves the large-scale monitoring of U.S. and non-U.S. persons, in violation of the Constitution and international law. To address this core deficiency, we urge the PCLOB to examine electronic surveillance collection under EO 12333 programs and recommend that Congress and the President:

- **Prohibit acquisition that is not restricted by selectors associated with specific individuals (such as email addresses and phone numbers) or small groups of individuals**. If Congress does not categorically prohibit such acquisition, it should make clear that such acquisition is permissible only if it is limited to the transient acquisition of data necessary to allow for surveillance that relies on specific selectors.

- **Require that even surveillance that relies on specific selectors is permissible only to the extent the targets of the surveillance are agents of foreign powers**. If Congress does not impose this restriction, it should, at a minimum, narrow the definition of "foreign intelligence information" in EO 12333 to conform to 50 U.S.C. § 1801(e)(1).

- **Prohibit "about" surveillance and other forms of surveillance premised on the scanning of content**, such as the surveillance described in § 5.1 of USSID 18.

- **Require the government to adopt reasonable measures designed to prevent the warrantless collection of any communication to or from a U.S. person** except where one party to the communication is a foreign agent. Even with respect to a communication involving a foreign agent, the government should be required to obtain a warrant (i) before accessing or reviewing a communication to or from a U.S. person or (ii) if and when there is reason to believe that a communication is to or from a U.S. person.

- **Eliminate the presumption that communications or data collected outside the United States is non-U.S.-person information,** and instead require an assessment of whether it is reasonably likely that the information in question is U.S.-person information.

- **To the extent Congress provides for exceptions to the limitations proposed above, the exceptions should be narrowly cabined by time, geography, and purpose**. Any exception for situations of imminent or actual armed conflict, for example, should be limited to the duration and specific place of the armed conflict.

b. Retention, Use, and Dissemination of Information

Current policies governing the retention, use, and dissemination of information collected under EO 12333 fail to comply with the privacy protections required under domestic and international law. These policies permit large-scale retention of U.S. and non-U.S. person information, circumvent the warrant requirement by allowing the seizure, search, and use of U.S. person information, and fail to provide appropriate notification for impacted individuals and companies. Accordingly, we urge the PCLOB to consider the

adequacy of existing procedures governing the retention, use, and dissemination of information under EO 12333, and recommend that Congress and the President:

- **Change the default age-off for data acquired under EO 12333 from five years to a maximum of three years for targeted collection,** consistent with the PCLOB's recommendations for Section 215**.**[153] To the extent that large-scale, indiscriminate collection continues under EO 12333, the default age-off for data collected in such a fashion should be, at most, one year and, in any event, no longer than the exigency used to justify the collection.

- **Prohibit the retention, use, or dissemination of information associated with or reasonably likely to be associated with a U.S. person,** unless the government obtains an order from the FISC under Title I of FISA.

- **Prohibit the querying of information collected under EO 12333 using identifiers of U.S. persons or any other search term or terms** intended or reasonably likely to result in the return of U.S. person information, absent an order from the FISC under Title I of FISA.

- **Prohibit the use of data collected under EO 12333 against U.S. persons in criminal prosecutions, immigration proceedings, civil proceedings, or any other administrative proceedings**, except where the collection, querying, or use of that information has been authorized by the FISC under Title I of FISA**.** Such a policy is analogous to recommendations made by the President's Review Group with regards to U.S. person information collected under Section 702 of FISA and EO 12333. Moreover, to the extent information used in legal proceedings was obtained or derived from EO 12333 surveillance, Congress should require notice in those proceedings.

- **Prohibit the sharing of information with domestic law enforcement agencies for general law enforcement activities,** given that the collection is subject to no judicial oversight or process**.**

- **Only permit the retention of non-U.S. person information that constitutes foreign intelligence,** under the amended definition of foreign intelligence articulated above.

c. Sharing of Information with Foreign Entities

Despite the extensive nature of its intelligence sharing practices, the United States has failed to disclose what safeguards, if any, it has to ensure that shared information is not used to contribute to human rights abuses, circumvent legal obligations in the U.S., or evade privacy obligations under international law. The absence of such procedures are particularly concerning given that the U.S. appears to engage in large-scale sharing of U.S. and non-U.S. person data, permit use of data for a wide variety of purposes, and allow entities to use data in a manner that would not be permitted under U.S. law and policies. To address these concerns, we urge the PCLOB to consider the standards and procedures governing the sharing of information with foreign governments under the programs being examined, and to recommend that Congress and the President:

- **Extend current restrictions on the sharing of information concerning U.S. persons in intelligence reports to the sharing of U.S. person information contained in raw data.** Under

[153] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 17 (Jan. 23, 2015), *available at* https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf.

current guidelines, the U.S. government does not share with foreign governments any intelligence reports that contain unmasked U.S. person information. However, existing loopholes permit the sharing of identical U.S. person information in raw or unprocessed data, and there have been reports of such U.S. data being shared with intelligence partners who permit the querying of U.S. person information without a warrant or other safeguards. To close this loophole, current policies prohibiting the sharing of U.S. person information in intelligence reports should be extended to cases in which it is reasonably likely that unprocessed or raw data will contain U.S. person information.

- **Prohibit the sharing of non-U.S. person information unless there is a reasonable belief that the information is necessary to protect against** (a) an actual or potential attack or other grave hostile acts of a foreign power, (b) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or agent of a foreign power; or (c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

- **Prohibit information sharing, including raw or unprocessed data, with a foreign entity if there are reasonable grounds to believe that it could contribute to the violation of human rights.** To implement this policy, prior to entering into a new information sharing agreement, the U.S. government should conduct a human rights analysis analogous to the vetting procedure currently used by the State Department in determining if the provision of military aid is appropriate. As part of this assessment, the State Department in partnership with the Secretary of Defense and intelligence community, should consider the human rights record of the receiving entity and the safeguards in place to ensure that information is used appropriately. Such analysis should be updated on an annual basis.

- **Require written assurances from any foreign entity receiving intelligence information regarding the retention, use, and dissemination of information**. Specifically, any entity receiving information should be required to adhere to the analogous restrictions that would apply if the U.S held the information, and there should be appropriate compliance procedures in place to ensure that the assurances are followed.

- **Withhold or submit an error assessment in cases where** there are doubts about the reliability of outgoing intelligence.

- **Require that any information received by the U.S. from a foreign entity be governed by the same policies and restrictions** that apply to information collected by the U.S.

d. Transparency

Despite the breadth of EO 12333 activities, little information is publicly available regarding the scope of 12333 activities or applicable standards. Indeed, to date, EO 12333 surveillance has occurred absent sufficient judicial, congressional, or administrative oversight. Given the lack of information available about EO 12333 activities, we urge the PCLOB to make public the results of its inquiry into EO 12333 activities. Additionally, we urge the PCLOB to declassify and make public the following additional information regarding EO 12333 activities, and recommend that such information be updated annually and made publicly available:

- **Information regarding the number of individuals who have had information collected under EO 12333 surveillance**, including:

- The number of communications that have been acquired, collected, or retained under EO 12333, including a breakdown of the number of U.S. person communications and a breakdown of the number of communications collected using surveillance directed at non-targets;
- The number of individuals and accounts which have had their information collected under EO 12333 programs annually, including a breakdown of the number associated with U.S. persons;
- The number of individuals who have had digital network intelligence acquired under 12333, including a breakdown of the number of U.S. persons;
- The types of information that have been collected under EO 12333 surveillance; and
- The number of other types of information that have been collected under 12333 (such as geolocation information), including a breakdown of the proportion of this information likely associated with U.S. persons. If such information is not available, this information should be estimated based on a statistical sample of the collection.

- **Information regarding the policies and procedures that govern EO 12333 activities,** including**:**
  - All minimization procedures and related guidance for all IC components;
  - The policies in places to ensure that collection is as narrowly tailored as possible, as required under Presidential Policy Directive 28;
  - The policies governing if and when any entity of the U.S. government can query EO 12333 collected information;
  - The policies governing if and when any entity of the U.S. government can query EO 12333 collected information using U.S. person identifiers; and
  - The targeting procedures governing how the government determines appropriate targets or selection terms.

- **Information regarding the retention, use, and dissemination of information collected under EO 12333**, including:
  - The domestic agencies and foreign governments who have access to unprocessed or processed data acquired under EO 12333;
  - The numbers of times that information derived from EO 12333 data has been used in criminal investigations and prosecutions, or other legal or administrative government proceedings, and the requirements that exist for disclosing the use of this information;
  - The types of analysis, including facial recognition, biometrics, contact chaining, or pattern based data mining, used on EO 12333 data;
  - The number of times EO 12333 data is queried; and
  - The number of times EO 12333 data is queried using U.S. person identifiers.

- **Information regarding the sharing of information with foreign entities**, including:
  - Requirements or processes for determining with whom data is shared, including how equities are weighed when sharing intelligence with governments that have a history of committing human rights abuses;
  - Guidelines that foreign governments who receive EO 12333 data are required to follow;
  - Existing compliance procedures to ensure that EO 12333 is not used to commit human rights abuses;
  - The countries and entities with whom the U.S. government receives intelligence data; and
  - The protocols that govern the treatment of data that the U.S. receives from foreign partners.

For more information, please contact Legislative Counsel Neema Guliani at nguliani@aclu.org or 202-675-2322.

Sincerely,

Karin Johanson
National Political Director

Jameel Jaffer
Deputy Legal Director

Neema Singh Guliani
Legislative Counsel

Patrick C. Toomey
Staff Attorney, National Security Project