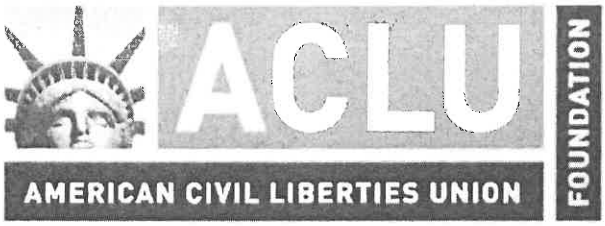

Testimony of

Ashley Gorski
Staff Attorney
National Security Project
American Civil Liberties Union Foundation

Before the
Deutscher Bundestag
1st Committee of Inquiry in the 18th Electoral Term

September 8, 2016

On behalf of the American Civil Liberties Union ("ACLU"), I would like to thank the Committee of Inquiry for holding this hearing, and for the opportunity to testify on electronic surveillance conducted by the U.S. National Security Agency ("NSA").

The ACLU is a U.S. nationwide, non-profit, nonpartisan organization with more than 500,000 members, dedicated to protecting the fundamental rights guaranteed by the U.S. Constitution, the laws of the U.S., and the international laws and treaties by which the U.S. is bound.

I understand that the goal of this hearing is for the Committee of Inquiry to assess the activities of the U.S.'s intelligence services, with a particular focus on changes to the laws regarding the collection, retention, and dissemination of Internet and telecommunications data. In light of that goal, I will seek to clarify the legal frameworks governing U.S. government surveillance, the scope of this surveillance, and some of the reforms that have taken place since the media first reported on Edward Snowden's disclosures in June 2013.

Introduction

Thanks to Edward Snowden and a group of particularly courageous reporters, over the past three years, the U.S. public and elected officials have engaged in a long-overdue debate about government surveillance and civil liberties. This debate is ongoing, and has been informed

by three fundamental lessons about the nature of U.S. surveillance and the legal and political structures in which it takes place.

First, through the Snowden disclosures and subsequent government revelations, the public is now aware that pervasive surveillance is not just theoretically possible, but it is in fact occurring. Since the summer of 2013, we have learned, among other facts, that the NSA was obtaining records of every domestic phone call every single day (and that the Director of National Intelligence lied about this when testifying before Congress); that the NSA hacked into links between Google's and Yahoo's data centers; that the NSA searches the content of substantially all text-based Internet communications that enter or exit the U.S.; and that the NSA collects data outside of the U.S.—including emails, text messages, internet chat transcripts, the full content of phone calls, cell phone location information, and contact lists—on a massive scale. For example, as reported in Der Spiegel, the NSA collects and retains data from approximately 500 million German phone and Internet communications each month.

Second, the U.S. lacks an adequate system of checks and balances to oversee and restrain executive-branch surveillance. When the government conducts surveillance that takes place on U.S. soil or targets Americans, a secret court, known as the Foreign Intelligence Surveillance Court ("FISC"), is supposed to serve as a check on the executive branch's surveillance activities. But it has become apparent that this secret court has failed to meaningfully constrain the executive branch. Even more problematically, when the U.S. conducts surveillance overseas, it is subject to virtually no congressional or judicial oversight—despite the fact that this surveillance sweeps countless Americans into its dragnet. And as a general matter, it is exceptionally difficult to challenge the government's surveillance programs in ordinary courts. Civil litigants are almost always stymied by the doctrine of "standing," which requires them to show with sufficient likelihood that they have been or will be subject to secret surveillance. In the context of criminal cases, the government relies on an unjustifiably narrow interpretation of its legal obligation to notify defendants when it intends to use evidence against them that was obtained or derived from secret surveillance. As a result, countless criminal defendants who have been subject to highly controversial surveillance programs are unable to challenge them in court.

Third, the U.S. government is not sufficiently transparent about its interpretations of surveillance law and the scope of its practices. Indeed, in many respects, the Snowden disclosures were the product of a culture of excessive secrecy. Had the government been more transparent about the extent and intrusiveness of its surveillance, these disclosures may have been unnecessary. Of course, no one suggests that U.S. should reveal every operational detail related to its surveillance activities. But in order to maintain democratic legitimacy, the government must be more forthcoming with the public about the general scope of its surveillance, as well as its understanding of the breadth of its legal authorities.

Informed by these three lessons, the domestic debate over privacy and surveillance has resulted in some reforms, the most significant of which relates to the NSA's domestic call-records program. For more than a decade, the NSA kept a record of substantially all phone calls made or received on major U.S. telephone networks. The ACLU challenged the legality of this surveillance in court, and a federal court of appeals ruled in May 2015 that the NSA's bulk collection of domestic call records was illegal. Not long thereafter, Congress passed the USA FREEDOM Act, which put an end to the NSA's bulk collection program and enacted other modest reforms to domestic intelligence-gathering.[1] While the passage of this act was a milestone, the legislation left many of the government's most intrusive and overbroad surveillance powers untouched, as discussed below.

The testimony below focuses on two of the most significant U.S. government surveillance authorities: Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), which authorizes surveillance that takes place on U.S. soil, and Executive Order ("EO") 12333, which authorizes electronic surveillance that largely takes place abroad. After describing Section 702 and EO 12333 surveillance, I discuss the post-Snowden reform most relevant to U.S. surveillance of Germans' communications and data, Presidential Policy Directive 28 ("PPD-28").

The NSA's Global Surveillance

I. Section 702 of the Foreign Intelligence Surveillance Act

A. Legal Background

1. Collection

In 2008, Congress enacted Section 702 of FISA, a statute that radically reduced judicial oversight of surveillance of international communications that either begin or terminate in the United States.[2] Since Section 702 was signed into law, the ACLU has opposed the statute on the grounds that it authorizes the warrantless surveillance of Americans' international communications. Over the past eight years, the defects in the Section 702 surveillance scheme—lack of judicial oversight, inadequate targeting and minimization procedures, and absence of redress mechanisms, among others—have become even more apparent. Perhaps most disturbingly, the public has also learned that the NSA relies on Section 702 to copy and search *substantially all* text-based Internet communications flowing into and out of the country.

[1] USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

[2] Section 702 was enacted as part of the FISA Amendments Act of 2008, often referred to as the "FAA." By statute, this authority will sunset on December 31, 2017, unless it is reauthorized by Congress.

Section 702 authorizes the government's large-scale, warrantless acquisition of the contents of communications from Internet and telecommunications providers inside the U.S. when two primary conditions are satisfied: first, the target of the NSA's surveillance must be a foreigner located abroad, and second, the purpose of the surveillance must be to gather "foreign intelligence information."[3]

Neither of these conditions imposes a meaningful restraint on the U.S. government's surveillance. Critically, Section 702 does not require the government to make any finding—let alone demonstrate probable cause to a court—that its surveillance targets are foreign agents, engaged in criminal activity, or even remotely associated with terrorism. Additionally, the phrase "foreign intelligence" is defined extraordinarily broadly to include information related to the U.S.'s "foreign affairs," which could encompass communications between international organizations and government whistleblowers, or even between journalists and sources.[4] Thus, the government's authority is *not* limited to the surveillance of suspected terrorists or criminals, but extends to the surveillance of individuals who are not suspected of any wrongdoing whatsoever.

Although the FISC, a secret court, annually reviews the general targeting and minimization procedures that the government proposes to use in carrying out its surveillance,[5] the FISC does not evaluate whether there is sufficient justification to surveil specific targets, or whether the government's collection and use of information concerning specific targets is lawful. In short, the effect of Section 702 is to give the government broad authority to warrantlessly monitor Americans' international communications, with virtually no judicial oversight.

2. Retention, Dissemination, and Use

Under Section 702, the government has broad authority to retain, analyze, and use the data it has collected. It can retain communications indefinitely if they are encrypted or are found to contain foreign intelligence information. Even for data that does not fall into either of these categories, the default retention period is five years for PRISM collection, and two years for Upstream collection—two distinct methods of collection discussed in greater detail below. In addition, data can be disseminated to other countries, and used for a wide variety of purposes, including criminal investigations and prosecutions.[6]

---

[3] *See* 50 U.S.C. § 1881(a).

[4] *Id.* § 1801(e).

[5] *See id.* § 1881a(i).

[6] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NSA IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED §§ 6–8 (July 15, 2015), *available at* https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf.

B. Section 702 Surveillance Programs

The Snowden revelations and subsequent government disclosures show that the government uses Section 702 to conduct at least two types of surveillance: Upstream and PRISM surveillance.[7]

Upstream surveillance, which the government claims is authorized by Section 702, involves the mass copying and searching of virtually all Internet communications flowing into and out of the U.S. With the help of companies like Verizon and AT&T, the NSA conducts this surveillance by tapping directly into the Internet backbone inside the U.S.—the physical infrastructure that carries the communications of hundreds of millions of Americans and others around the world. After copying nearly all of this traffic, the NSA searches the metadata and content for key terms, called "selectors," that are associated with its tens of thousands of foreign targets. Communications containing selectors—as well as those that happen to be bundled with them in transit—are retained on a longer-term basis for further analysis and dissemination, with few restrictions. Thus, through Upstream surveillance, the NSA indiscriminately accesses, copies, and searches through vast quantities of personal metadata and content.[8]

The second type of Section 702 surveillance is known as "PRISM." Through PRISM, the government obtains stored and real-time communications directly from U.S.-based electronic communications service providers, such as Google, Yahoo, Facebook, and Microsoft. The government identifies the user accounts it seeks to monitor—for example, particular Yahoo email addresses—and then collects from the provider all communications to or from those accounts.[9] As of April 2013, the NSA was monitoring at least 117,675 targeted accounts via PRISM.[10]

II. EO 12333

A. Legal Background

EO 12333, originally issued in 1981 by President Ronald Reagan and subsequently revised, is the primary authority under which the NSA gathers foreign intelligence. It provides broad latitude for the government to conduct surveillance on Americans and others alike—without judicial review or other protections that apply to surveillance conducted under Section

---

[7] *See, e.g.*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SEC. 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 33–41 (2014), *available at* https://www.pclob.gov/library/702-Report.pdf ("PCLOB Report").

[8] *See, e.g.*, *id.* at 35–39, 111 n.476; *[Redacted]*, 2011 WL 10945618, at *10–11 (FISC Oct. 3, 2011).

[9] *See, e.g.*, PCLOB Report 33–34.

[10] *See NSA Slides Explain the PRISM Data Collection Program*, WASH. POST, July 10, 2013, http://wapo.st/158arbO.

702 or other statutory authorities. As noted above, electronic surveillance under EO 12333 is largely conducted outside the U.S.[11]

Collection, retention, and dissemination of data gathered under EO 12333 is governed by directives and regulations promulgated by federal agencies and approved by the Attorney General, including U.S. Signals Intelligence Directive 0018 ("USSID 18") and other agency policies.[12] In addition, as discussed in greater detail below, PPD-28 and its associated agency policies further regulate EO 12333 activities.

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 terrorism, espionage, and weapons of mass destruction.[13] Yet 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.

Despite its breadth, EO 12333 has not been subject to meaningful oversight. Surveillance programs operated under EO 12,333 have never been reviewed by any court. Moreover, these programs are not governed by any statute, including FISA, and, as the former Chairman of the Senate Intelligence Committee has conceded, they are not overseen in any meaningful way by Congress.[14]

1. Collection

EO 12333 and its accompanying regulations place few restrictions on the collection of U.S. or non-U.S. person information. The order authorizes the government to conduct electronic surveillance abroad for the purpose of collecting "foreign intelligence"—a term defined so broadly that it likely permits surveillance of any foreign person, including surveillance of their

[11] *See* John Napier Tye, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, WASH. POST, July 18, 2014, http://wapo.st/2bnOU39; EO 12333, as amended, *available at* http://www.dni.gov/index.php/about/organization/ic-legal-referencebook-2012/ref-book-eo-12333.

[12] *See* National Security Agency, USSID 18 (Jan. 25, 2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf; *see also* Office of the Director of National Intelligence, *Status of Attorney General Approved U.S. Person Procedures Under E.O. 12333* (July 14, 2016), https://www.dni.gov/files/documents/Table_of_EO12333_AG_Guidelines%20for%20PCLOB_%20Updated%20July_2016.pdf (listing other agencies' EO 12333 guidelines).

[13] *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.").

[14] 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.

communications with U.S. persons.[15] The definitions and policies that apply to EO 12333 surveillance contain no protection for many categories of sensitive information subject to enhanced legal protection in other contexts—such as confidential information compiled by healthcare providers or journalists—and only minimal protections for a narrow class of attorney–client communications.

In addition, the order and its implementing regulations permit two forms of bulk surveillance.[16] First, they permit the government to engage in what is sometimes termed "bulk collection"—that is, the indiscriminate collection of electronic communications or data. 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 "bulk searching," in which the government indiscriminately searches the content of electronic communications for "selection terms," as it does with Upstream surveillance under Section 702 of FISA. In short, the NSA subjects the communications content (and metadata) of the general population to real-time surveillance, as it looks for specific information of interest. Under EO 12333, the selection terms the NSA uses to search communications in bulk may include a wide array of keywords. Indeed, unlike the selectors the government claims to use under Section 702's Upstream surveillance, EO 12333 procedures permit selectors that are not associated with particular targets (such as an email address or phone number).[17] As a result, the government can use selectors likely to return even larger amounts of information, such as the names of countries or political figures.

2. 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;[18] (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

[15] *See* EO 12333 § 3.5(e) (defining "foreign intelligence" as "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, foreign persons, or international terrorists").

[16] *See, e.g.*, USSID 18 § 4; 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.

[17] *See* PCLOB Report 7 (describing the government's tasking of selectors "such as telephone numbers or email addresses" for Section 702 surveillance).

[18] The default five-year age-off is triggered when this data is in intelligible form. *See* PPD-28 Section 4 Procedures § 6.1.

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 U.S. 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.

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, 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.[19] While these agreements are not public, they reportedly allow for the sharing of raw data without appropriate protections.[20] For example, the United Kingdom reportedly searches through U.S. person data without a warrant or the equivalent.

The U.S. also shares U.S. and non-U.S. person information with countries other than the Five Eyes, including Germany, Israel, and Saudi Arabia.[21] 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.[22] 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.[23]

B. EO 12333 Surveillance Programs

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

---

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

[20] 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.

[21] *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.

[22] Glenn Greenwald, Laura Poitras & Ewen MacAskill, *NSA Shares Raw Intelligence Including Americans' Data with Israel*, THE GUARDIAN, Sept. 11, 2013, https://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents.

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

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

- **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;[24]

- **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 United Kingdom intelligence services;[25]

- **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;[26]

- **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;

- **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]

---

[24] 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/.

[25] 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.

[26] 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.

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

[28] Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally,* WASH. POST, Oct. 14, 2013, http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_print.html.

- **International Transit Switch Collection under "Transit Authority**," in which the U.S. collects cable traffic that traverses U.S. territory but originates and terminates in foreign countries;[29]

- **WELLSPRING**, an initiative that involved collecting images from e-mails for analysis by facial recognition software;[30] 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.[31]

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;[32]

- **Hacking into news organizations**, such as Al Jazeera, to obtain information regarding communications with potential targets;[33]

- **WABASH, BRUNEAU, HEMLOCK, BLACKFOOT, and other programs** to conduct surveillance of 38 embassies and missions in New York and Washington D.C.;[34]

- **Surveillance of major worldwide summits**, including the G8, G20, and 2009 U.N. Climate Change Conference;[35]

---

[29] *See, e.g.*, Signals Intelligence Directorate, NSAW SID Intelligence Oversight Quarterly Report at 5 (May 3, 2012), *available at* https://www.aclu.org/sites/default/files/field_document/sid_oversight_and_compliance.pdf; Charlie Savage, Power Wars Document: Transit Authority and the 1990 Lawton Surveillance Memo, Nov. 18, 2015, http://www.charliesavage.com/?p=557.

[30] 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.

[31] *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.

[32] BULLRUN Briefing Sheet from GCHQ, *available at* http://www.propublica.org/documents/item/784284-bullrun-briefing-sheet-from-gchq.html.

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

[34] 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.

- **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;[36]

- **VICTORYDANCE**, which uses drones to map the WiFi fingerprint of nearly every town in Yemen;[37]

- **Surveillance of major world leaders**, including surveillance of Russian leadership and hacking into the cell phones of German leadership;[38] and

- **GILGAMESH**, a program to geolocate individuals' SIM cards using predator drones in select geographic areas.[39]

Post-Snowden Reform: PPD-28

In January 2014, President Barack Obama issued PPD-28, an executive-branch directive that articulates broad principles to govern the collection of signals intelligence, and that imposes certain constraints on (i) the use of electronic communications collected in "bulk" under EO 12333; (ii) the retention of communications containing personal information of non-U.S. persons; and (iii) the dissemination of communications containing personal information of non-U.S. persons.

While the ACLU applauds PPD-28's recognition of the privacy interests of non-U.S. persons, the directive includes few meaningful reforms—and these reforms can easily be modified or revoked by the next U.S. President. At bottom, PPD-28 is designed to accommodate the government's ongoing bulk surveillance of U.S. and non-U.S. persons under EO 12333.

---

[35] Greg Weston, Glenn Greenwald & Ryan Gallagher, *New Snowden Docs Show U.S. Spief During g20 in Toronto,* CBCNEWS, Nov. 27, 2013, 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.

[36] 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.

[37] 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/.

[38] *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.

[39] 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/.

I. PPD-28's Principles

The broad principles articulated in PPD-28 include the following:

- The U.S. shall not collect signals intelligence for the purpose of suppressing or burdening criticism or dissent, or for disadvantaging persons based on their ethnicity, race, gender, sexual orientation, or religion.[40]

- The collection of foreign private commercial information or trade secrets is authorized only to protect the national security of the U.S. or its partners and allies.[41]

- Signals intelligence activities shall be as tailored as feasible. In determining whether to collect signals intelligence, the U.S. shall consider the availability of other information, including from diplomatic and public sources.[42]

- All persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the national of the individual to whom the information pertains or where that individual resides.[43]

Although the executive branch's commitment to these principles in the abstract is encouraging, as discussed below, PPD-28 unfortunately includes few meaningful constraints on the government's surveillance practices.

II. Bulk Collection

PPD-28 provides that when the U.S. collects nonpublicly available signals intelligence in bulk, it shall use that data only for the purposes of detecting and countering six specified activities:

- espionage and other threats and activities directed by foreign powers or their intelligence services against the U.S. and its interests;

- threats to the U.S. and its interests from terrorism;

[40] PPD-28 § 1(b).

[41] *Id.* § 1(c).

[42] *Id.* § 1(d).

[43] *Id.* § 4.

- threats to the U.S. and its interests from the development, possession, proliferation, or use of weapons of mass destruction;

- cybersecurity threats;

- threats to U.S. or allied Armed Forces or other U.S. or allied personnel; and

- transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes above.

While these restrictions are a step in the right direction, they do not go nearly far enough to constrain the bulk collection of U.S. and non-U.S. person data. As an initial matter, the six categories, taken together, are extremely broad. They also effectively ratify the practice of bulk, indiscriminate surveillance—despite the fact that bulk surveillance is inherently unlawful and nearly always disproportionate, and as such it violates Article 17 of the International Covenant on Civil and Political Rights.[44]

Moreover, PPD-28's limitations on "bulk collection" do not extend to other problematic types of mass surveillance—including the "bulk searching" of Internet communications described above. PPD-28 defines bulk collection to include only: "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)."[45] This definition explicitly excludes data that is "temporarily acquired to facilitate targeted collection."[46] In other words, these restrictions on use do not apply to data that is acquired in bulk and held for a short period of time, such as data acquired in bulk through Upstream surveillance under Section 702.

Finally, PPD-28 in no way limits the *collection* of information in bulk. Rather, these limitations apply only to the *use* of data that has already been collected in bulk. Thus, under EO 12333, the government can still collect data in bulk simply for the purpose of gathering information relating to the capabilities, intentions, or activities of foreign persons, organizations, or governments—without any nexus to a threat to the U.S.[47]

---

[44] *See, e.g.*, ACLU, INFORMATIONAL PRIVACY IN THE DIGITAL AGE: A PROPOSAL TO UPDATE GENERAL COMMENT 16 TO THE INTERNATIONAL COVENANT ON CIVIL AND POLITICAL RIGHTS (Feb. 2015), *available at* https://www.aclu.org/sites/default/files/field_document/informational_privacy_in_the_digital_age_final.pdf.

[45] PPD-28 § 2 n.5.

[46] *Id.*

[47] EO 12333 §§ 2.3, 3.5(e).

III. Retention, Dissemination, and Use

PPD-28's most significant reforms are with respect to the retention and dissemination of communications containing "personal information" of non-U.S. persons. However, even these reforms do little to rein in the government's mass violations of the privacy rights of non-U.S. persons.

Under the directive, the government may retain the personal information of non-U.S. persons only if retention of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333.[48] Similarly, the government may disseminate the personal information of non-U.S. persons only if the dissemination of comparable information concerning U.S. persons would be permitted under Section 2.3 of EO 12333.[49]

Critically, however, Section 2.3 of EO 12333 imposes few restraints on the government: it authorizes the retention and dissemination of communications to, from, and about U.S. persons in a wide variety of circumstances, as discussed in Section II.A.2 above. Thus, while the executive branch's efforts to create new protections for non-U.S. persons are welcome—and long overdue—these protections are extremely weak.[50]

Conclusion

The Snowden disclosures and subsequent domestic debates over privacy have resulted in some surveillance reforms in the U.S.; however, two of the most significant surveillance authorities, Section 702 and EO 12333, remain largely intact. Although PPD-28 imposes new limitations on the government's retention and use of non-U.S. person communications, these protections are extremely weak. Moreover, the directive explicitly accommodates the government's ongoing bulk collection of Internet and telecommunications data.

Thank you again for the invitation to discuss the legal frameworks governing U.S. foreign intelligence surveillance. The ACLU appreciates the Committee of Inquiry's attention to these issues.

[48] PPD-28 § 4(a)(i). PPD-28 requires that departments and agencies apply the term "'personal information' in a manner that is consistent for U.S. persons and non-U.S. persons," and states that "'personal information' shall cover the same types of information covered by 'information concerning U.S. persons' under section 2.3 of Executive Order 12333." *Id.* § 4 n.7. Notably, however, EO 12333 does not define "information concerning U.S. persons."

[49] PPD-28 § 4(a)(i).

[50] *Id.*