



July 31, 2014

VIA FACSIMILE and eFOIA PORTAL

Carmen L. Mallon
 Chief of Staff, Office of Information Policy
 U.S. Department of Justice
 Suite 11050
 1425 New York Avenue, NW
 Washington, DC 20530-0001
 (202) 514-1009 (Fax)

1718 Connecticut Ave NW

Suite 200

Washington DC 20009

USA

+1 202 483 1140 [tel]

+1 202 483 1248 [fax]

www.epic.org

RE: Freedom of Information Act Request to Office of the Attorney General

Dear Ms. Mallon:

This letter constitutes as request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, and is submitted on behalf of the Electronic Privacy Information Center ("EPIC") to the Department of Justice ("DOJ") Office of the Attorney General ("OAG").

EPIC seeks records related to the government's surveillance and collection of electronic communications data outside the United States under Executive Order 12333 ("EO 12333"), and other related Executive Orders, including the collection and interception of messages, metadata, and other transactional and business records regarding e-mail, telephone, and Internet usage. The Attorney General coordinates all implementing procedures under EO 12333, and all Intelligence Community members must seek Attorney General approval of their implementing guidelines. Therefore, the OAG should have records responsive to this request.

Background

President Ronald Regan issued EO 12333 on December 4, 1981, in order to redefine the authorities of the Intelligence Community ("IC")¹ to "provide the President and the National Security Council with the necessary information on which to base decisions" regarding a broad range of topics, including "development of foreign, defense, and economic policy" and national security.² According to the Director of National Intelligence ("DNI"), this order "establishes the Executive Branch framework for the country's national intelligence efforts, and for protecting privacy and civil liberties in the conduct of

¹ The U.S. Intelligence Community is comprised of 17 different sub-agencies within 7 Executive Branch agencies: CIA, Department of Defense (DIA, NSA, NGA, NRO, AFISRA, MI, MCIA, and ONI), Department of Energy (OICI), Department of Homeland Security (I&A and CGI), Department of Justice (FBI and DEA), Department of State (INR), and Department of Treasury (TFI).

² Exec. Order No. 12333 § 1.1. *See* Member Agencies, <http://www.intelligence.gov/mission/member-agencies.html>.

intelligence activities,”³ and yet since its adoption, surveillance activities have been carried out under this order without adequate transparency or public oversight.

The Order has three distinct parts: Part 1 outlines the roles and responsibilities of “national security and intelligence elements of the Executive Branch,” Part 2 includes “[r]estrictions on the conduct of intelligence activities,” and Part 3 addresses “[d]efinitions and general terms.”⁴ The Attorney General, in particular, has a key role in coordinating the procedures adopted to implement the Order. Specifically, the Order requires that IC elements establish “implementing guidelines that must be approved by the AG.”⁵ The IC elements may “collect, retain, or disseminate information concerning United States persons” only “in accordance with procedures established by the head of the Intelligence Community element concerned or by the head of a department containing such element and approved by the Attorney General . . . after consultation with the Director of National Intelligence.”⁶ The Order mandates that these procedures allow for the “collection, retention, and dissemination” of a broad range of information of interest to the IC.⁷

Some of these procedures have, in the past, been publicly released, but most remain secret and many are decades out of date. For example, the Defense Department’s 1982 regulations implementing the Order are available at the Defense Technical Information Center.⁸ Similarly, the Army has published its intelligence procedures as of 2007.⁹ But most IC members have not published or addressed their guidelines and procedures for collection, retention, and dissemination of communications data under EO 12333. In response to one active FOIA suit, the DNI has released the National Security Agency’s procedures from January 2011.¹⁰ The NSA, CIA, DIA, FBI, and State Department have also agreed to search for and process three narrow categories of documents, including their “formal regulations or policies” regarding electronic surveillance under EO 12333.¹¹

But recent reports have highlighted the expansive use of EO 12333 authorities to acquire Internet and other electronic communications data from major service providers and other sources that frequently handle U.S. person communications, stored files, and

³ OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE, CIVIL LIBERTIES AND PRIVACY OFFICE, CIVIL LIBERTIES AND PRIVACY INFORMATION PAPER: DESCRIPTION OF CIVIL LIBERTIES AND PRIVACY PROTECTIONS INCORPORATED IN THE 2008 REVISION OF EXECUTIVE ORDER 12333, at 1 (2008), *available at*

http://www.dni.gov/files/documents/CLPO/CLPO_Information_Paper_on_2008_Revision_to_EO_12333.pdf (version reformatted in 2013 for posting on dni.gov).

⁴ *Id.* at 3.

⁵ *Id.*

⁶ Exec. Order No. 12333 § 2.3.

⁷ See KRIS & WILSON 1, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS 2D § 2:7 (2012).

⁸ DEP’T OF DEFENSE, DOD 5240 1-R, PROCEDURES GOVERNING THE ACTIVITIES OF DOD INTELLIGENCE COMPONENTS THAT AFFECT UNITED STATES PERSONS (Dec. 1982), *available at* <http://www.dtic.mil/whs/directives/corres/pdf/524001r.pdf>.

⁹ ARMY REGULATION 381-10, ARMY INTELLIGENCE PROCEDURES, § 2-2(L) (2007), *available at* http://armypubs.army.mil/epubs/pdf/r381_10.pdf.

¹⁰ NAT’L SEC. AGENCY, U.S. SIGNALS INTELLIGENCE DIRECTIVE 18 (Jan. 2011), *available at* <http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf>.

¹¹ See Stipulation and Order Regarding Document Searches, *ACLU v. NSA et al.*, No. 13-cv-9198, at 2-4 (S.D.N.Y. May 9, 2014).

other sensitive metadata.¹² As a result of the technical evolution of Internet services, the private data of U.S. persons is no longer stored and processed only within our borders. Cross-border data flows are routine, especially where large providers seek to back up data in redundant systems around the globe, or to serve customers who travel internationally.¹³ One former State Department official has stated publicly that he filed a complaint with the Department's Inspector General over activities that he says resulted in such broad collection of American's data that it violates the Fourth Amendment unreasonable search and seizure prohibition.¹⁴

The President spoke about the scope of foreign intelligence surveillance in January 2014, and issued a new directive regarding signals intelligence activities, Presidential Policy Directive 28 ("PPD 28").¹⁵ The PPD 28 requires that the "DNI, in consultation with the Attorney General, shall ensure that all elements of the IC establish policies and procedures that apply the following principles for safeguarding personal information collected from signals intelligence activities."¹⁶ In addition, the PPD 28 requires that the DNI and AG, in coordination with the heads of other IC members "shall prepare a report" by July 16, 2014 "evaluating possible additional dissemination and retention safeguards for personal information collected through signals intelligence, consistent with technical capabilities and operational needs."¹⁷ The PPD 28 also requires that President's

¹² See Ellen Nakashima & Ashkan Soltani, *Privacy Watchdog's Next Target: the Least-known But Biggest Aspect of NSA Surveillance*, WASH. POST (July 23, 2014), available at <http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/23/privacy-watchdogs-next-target-the-least-known-but-biggest-aspect-of-nsa-surveillance/>; John Napier Tye, Opinion, *Meet Executive Order 12333: The Reagan Rule That Lets the NSA Spy on Americans*, WASH. POST (July 18, 2014), available at http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html; Barton Gellman & Ashkan Soltani, *NSA Surveillance Program Reaches 'Into the Past' to Retrieve, Replay Phone Calls*, WASH. POST (Mar. 19, 2014), available at http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html; Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 4, 2014), available at http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html; Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST (Oct. 30, 2014), available at http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html.

¹³ See Nakashima & Soltani, *supra* note 12 ("Once upon a time, you could be fairly certain that overseas collection would pick up only foreigners' phone calls, and that Americans' communications would stay inside the United States. But today, e-mails, calls, and other communications cross U.S. borders and are often stored beyond them. Companies like Google and Yahoo have "mirror" servers around the world that hold customers' data.")

¹⁴ See Tye, *supra* note 12.

¹⁵ Directive on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 31 (Jan. 17, 2014), available at <http://www.gpo.gov/fdsys/pkg/DCPD-201400031/pdf/DCPD-201400031.pdf>.

¹⁶ *Id.* at 5.

¹⁷ *Id.*

Intelligence Advisory Board provide a report “identifying the options for assessing the distinction between metadata and other types of data” by May 17, 2014.¹⁸

Documents Requested

1. Any policies, regulations, white papers, final memoranda, guidelines, or training materials interpreting or addressing the collection, retention, dissemination, or sharing of electronic communications or metadata under EO 12333.
2. The most recent version of IC member agency procedures adopted under EO 12333, including DOD 5240 1-R, Army Regulation 381-10, and USSID-18.

Request for Expedited Processing

This request warrants expedited processing because it is made by “a person primarily engaged in disseminating information . . .” and it pertains to a matter about which there is an “urgency to inform the public about an actual or alleged federal government activity.”¹⁹ EPIC is “primarily engaged in disseminating information.”²⁰

There is clearly an urgency to inform the public about the government’s surveillance activities conducted under EO 12333, given the current efforts by the President to reform bulk collection programs²¹ and the ongoing public interest in increased intelligence transparency. EPIC recently called for an independent investigation into the government’s use of 12333 authorities.²² Even Senator Diane Feinstein, the Chairwoman of the Senate Select Committee on Intelligence who has traditionally defended the government’s use of surveillance authorities, has said that her committee “has not been able to ‘sufficiently’ oversee the programs run under” EO 12333.²³ NSA surveillance of communications data, and other related surveillance activities, have been the subjects of continual news coverage for the past fourteen months.²⁴ The government’s use of surveillance authority was also the

¹⁸ *Id.* at 7.

¹⁹ 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

²⁰ *American Civil Liberties Union v. Dep’t of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004).

²¹ See Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 30 (Jan. 17, 2014), available at <http://www.gpo.gov/fdsys/pkg/DCPD-201400030/pdf/DCPD-201400030.pdf>.

²² Statement of Jeramie D. Scott, National Security Counsel, Electronic Privacy Information Center, at the Public Meeting Before the Privacy and Civil Liberties Oversight Board (Jul. 23, 2014), available at http://epic.org/news/privacy/surveillance_1/EPIC-Statement-PCLOB-Review-12333.pdf.

²³ Ali Watkins, Most of NSA’s Data Collection Authorized by Order Ronald Reagan Issued, *MCCLATCHYDC* (Nov. 21, 2013), available at <http://www.mcclatchydc.com/2013/11/21/209167/most-of-nsas-data-collection-authorized.html>.

²⁴ See, e.g., Nakashima & Soltani, *supra* note 12; Tye, *supra* note 12; Ellen Nakashima, *Clapper Confirms Warrantless Searches by NSA*, WASH. POST, Apr. 2, 2014, at A3; Ellen Nakashima, *NSA Breached Chinese Tech Giant’s Servers*, WASH. POST, Mar. 23, 2014, at A11; Gellman & Soltani, *NSA Surveillance Program Reaches ‘Into the Past’*, *supra* note 12; Barton Gellman, *Restrictions Rely on Narrow Definition of ‘Spying’*, WASH. POST, Jan. 18, 2014, at A1; Craig Timberg & Ashkan Soltani, *NSA Cracked Popular Cellphone Encryption*, WASH. POST, Dec. 14, 2013, at A1; Ashkan Soltani, Andrea Peterson, & Barton Gellman, *NSA Using Internet ‘Cookies’ to Find Targets*, WASHINGTON POST, Dec. 11, 2013, at A1; Barton Gellman & Ashkan Soltani, *NSA Maps Targets by Their Phones*,

subject of an extensive report by the President's Review Group on Intelligence and Communications Technologies.²⁵ The Privacy and Civil Liberties Board is also set to review surveillance conducted under EO 12333.²⁶ But the public cannot debate these complicated issues without further disclosures from the Attorney General. In order to adequately evaluate the reform proposals, it is essential to understand the government policies and procedures that apply to these programs.

Request for "News Media" Fee Status

EPIC is a "representative of the news media" for fee waiver purposes.²⁷ As such, EPIC is entitled to receive the requested record for the cost of duplication only. Because disclosing this information will "contribute significantly to public understanding of the operations or activities of the government," any duplication fees should be waived.²⁸

Conclusion

Thank you for your consideration of this request. As provided in 5 U.S.C. § 552(6)(e)(2), I will anticipate your determination of our request for expedited processing within 10 business days. For questions regarding this request, I can be contacted at 202-483-1140 x103 or foia@epic.org.

WASH. POST, Dec. 5, 2013, at A1; Gellman & Soltani, *NSA Taps Yahoo, Google Links*, *supra* note 12; Michael Birnbaum & Ellen Nakashima, *U.S. Accused of Eavesdropping on German President*, WASH. POST, Oct. 24, 2013, at A10; Barton Gellman, Craig Timberg, & Rich Steven, *Files Show NSA Targeted Tor Encrypted Network*, WASH. POST, Oct. 5, 2013, at A1; Ellen Nakashima & Julie Tate, *NSA Broke Privacy Rules for 3 Years, Documents Say*, WASH. POST, Sept. 11, 2013, at A1; Ellen Nakashima, *NSA Has Cracked Encryption*, WASH. POST, Sept. 6, 2013, at A3; Barton Gellman & Craig Timberg, *NSA Pays Firms Large Sums for Network Access*, WASH. POST, Aug. 30, 2013, at A1; Carol Leonning, *Surveillance Judge Says Court Relies on Government to Report Its Own Actions*, WASH. POST, Aug. 16, 2013, at A1; Dana Priest, *At NSA, a Boom Fed by Post-9/11 Demands*, WASH. POST, Jul. 22, 2013, at A1; Craig Timberg, *Slide Shows NSA Surveillance of Data from Undersea Cables*, WASH. POST, Jul. 11, 2013, at A8; Barton Gellman, *U.S. Surveillance Architecture Includes Collection of Revealing Internet, Phone Metadata*, WASH. POST, June 16, 2013, at A1; Barton Gellman & Laura Poitras, *U.S. Mines Internet Firms' Data, Documents Show*, WASH. POST, June 7, 2013, at A1.

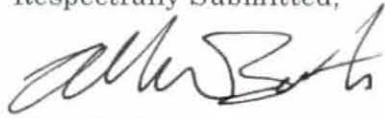
²⁵ RICHARD A. CLARKE, MICHAEL J. MORRELL, GEOFFREY R. STONE, CASS R. SUNSTEIN, & PETER SWIRE, *LIBERTY AND SECURITY IN A CHANGING WORLD* (2013), available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

²⁶ Nakashima & Soltani, *supra* note 12.

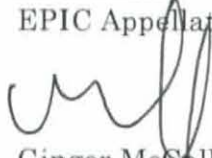
²⁷ *EPIC v. Dep't of Defense*, 241 F. Supp. 2d 5 (D.D.C. 2003).

²⁸ 5 U.S.C. § 552(a)(6)(E)(v)(II) (2008); *Al-Fayed v. CIA*, 254 F.3d 300, 306 (D.C. Cir. 2001).

Respectfully Submitted,



Alan Butler
EPIC Appellate Advocacy Counsel



Ginger McCall
Director, EPIC Open Government Project