April 7, 2016

Hon. James R. Clapper
Director, Office of the Director of National Intelligence
Washington, DC 20511

Admiral Michael S. Rogers
Director, National Security Agency
Fort Meade, MD 20755

Re: Changes to Executive Order 12333 Minimization Procedures

Dear Director Clapper and Admiral Rogers:

The undersigned organizations write to request that you halt the proposed changes to Executive Order 12333 policies that would share raw data collected by the National Security Agency with law enforcement agencies. As you know, EO 12333 sets forth a framework for the collection of foreign intelligence information overseas, but sweeps in massive amounts of Americans' data as well, including private messages, address books, and Internet metadata.[1] Considering the extent and scope of the information collected under EO 12333, the policy changes under consideration could allow agencies like the FBI to circumvent constitutional protections and will pose new threats to the privacy and civil liberties of ordinary Americans. At a minimum, when the administration seeks to ratchet back privacy protections for Americans, Congress and the American public should have the opportunity to weigh in.

The *New York Times* reported that the White House and the Director of National Intelligence are in the process of establishing procedures to expand intra-governmental access to raw data gathered by the NSA, including communications to, from, and about U.S. persons.[2] As a threshold matter, we were dismayed to learn about this development in the press instead of directly from your offices. News reports indicate the NSA has been developing these new procedures "for years"—since at least the start of the administration. The secrecy of this major undertaking undercuts Intelligence Community claims of increased transparency and engagement with civil society and the public and is inconsistent with the "Principles of Intelligence Transparency" adopted by ODNI in January of this year and reaffirmed through an implementation plan issued by ODNI in February.[3]

---

[1] Ellen Nakashima and Ashkan Soltani, "Privacy watchdog's next target: the least-known but biggest aspect of NSA surveillance," Washington Post (July 24, 2014), available at http://wapo.st/1SmuqEx.
[2] Charlie Savage, "Obama Administration Set to Expand Sharing of Data That N.S.A. Intercepts," N.Y. Times (Feb. 25, 2016), available at http://nyti.ms/21vgS0f; See also Amos Toh, Faiza Patel, and Elizabeth Goitein, "Overseas Surveillance in an Interconnected World," Brennan Center report, Part IV.B, available at http://bit.ly/1UfSdMW.
[3] Principle 2 states the IC will "[b]e proactive and clear in making information publicly available through authorized channels, including taking affirmative steps to…provide timely transparency on matters of public interest," and "engage with stakeholders to better explain information and to understand diverse perspectives…"

Moreover, the reported changes would fatally weaken existing restrictions on access to the phone calls, emails, and other data the NSA collects. Currently, under United States Signals Intelligence Directive 18 (USSID18), access to raw data containing U.S. persons' identities is limited.[4] Intelligence reports disseminated to other agencies may include U.S. persons' identities only if the U.S. person has consented, the information is publicly available, or the identity of the U.S. person is necessary to understand the foreign intelligence information or assess its importance.[5] The reported changes would jettison these longstanding restrictions and allow multiple other government agencies access to the NSA's raw take.

This change is particularly troubling because EO 12333 data collection is far broader than the controversial surveillance programs carried out under the auspices of other legal authorities, such as Section 702 of the Foreign Intelligence Surveillance Act (FISA). Data obtained under EO 12333 may be gathered through mass, even indiscriminate, surveillance. Given that even wholly domestic communications today may be routed or stored overseas, such broad surveillance inevitably captures the data of millions of Americans.[6] Sharing such information with U.S. law enforcement agencies would allow them to circumvent the strict, constitutionally mandated rules of evidence gathering that govern ordinary criminal investigations. The ongoing but largely obscured practice of parallel construction, whereby information gathered for national security purposes is laundered through domestic law enforcement while concealing its origins and manufacturing a new discovery history, undermines the important role that Courts play in policing the bounds of our Constitution and could become a more common occurrence under these new procedures.[7]

The secret shift in policy is particularly troubling at a time when Congress and government oversight bodies are calling for the NSA to move in the other direction—to provide more information to the general public about the legal authorities governing U.S. surveillance programs and to enact greater privacy protections for U.S. persons affected by these programs. Last year, Congress enacted the USA Freedom Act to prohibit the U.S. government's mass collection of Americans' phone records. Surely Congress did not intend for the government to evade this prohibition through new NSA procedures giving law enforcement agencies easy access to Americans' phone metadata swept in under EO 12333.

Similarly, the independent group of experts appointed by President Obama to review surveillance practices in 2013 recommended significantly *tightening* the limits on the retention and use of information about U.S. persons collected under Section 702 of FISA "or under any other authority that justifies the interception of a communication on the ground that it is directed at a non-United States

---

[4] USSID18 § 6.2.
[5] USSID18 § 7.2.
[6] See Toh, Patel, and Goitein, Brennan Center report, Part I.C, http://bit.ly/1UfSdMW.
[7] See Request to the United States Commission on Civil Rights to investigate disproportionate impacts of "Parallel Construction" on communities of color, prepared by Sean Vitka, X-Lab, http://bit.ly/1ZKEddd.

person who is located outside the United States."[8] In addition, recognizing the implications of EO 12333 surveillance, the congressionally created Privacy and Civil Liberties Oversight Board is currently examining several EO 12333 programs.

Congress has taken notice of the NSA's planned changes. Members of the House Oversight and Government Reform Committee recently wrote a letter to NSA Director Admiral Rogers asking for the NSA to confirm whether the Agency intends to routinely provide intelligence information—collected without a warrant—to domestic law enforcement agencies. If the NSA intends to go down this uncharted path, the letter states, "we request that you stop." The letter further emphasizes that the proposed shift in the relationship between our intelligence agencies and the American people should not be done in secret.[9]

We join Representatives Lieu and Farenthold in requesting that you halt efforts to modify EO 12333 information sharing procedures and any other related efforts that would expand the sharing of raw information gathered by NSA with agencies that have law enforcement functions. We also ask that you release the 21-page draft policy referenced in the *New York Times* article to enable the American public to weigh in on a planned policy change that would directly affect their rights and interests.

We would appreciate and request the opportunity to discuss this matter in greater detail. To reply to this letter, or to arrange a call or meeting, please contact any of the following representatives of our coalition:

Mark M. Jaycox
Civil Liberties Legislative Lead
Electronic Frontier Foundation
Jaycox@eff.org
415-436-9333

Patrice McDermott, Executive Director
OpenTheGovernment.org
pmcdermott@openthegovernment.org
202-332-6737

Daniel Schuman, Policy Director
Demand Progress
daniel@demandprogress.org
202-577-6100

Elizabeth Goitein, Co-Director
Liberty & National Security Program
Brennan Center for Justice
goiteine@mercury.law.nyu.edu
202.249.7192

Thank you for your prompt response.

Sincerely,

[8] Recommendation 12, Review Group on Intelligence and Communications Technologies.
[9] Letter to Admiral Michael S. Rogers, Director, National Security Agency, from Representatives Ted W. Lieu and Blake Farenthold, March 23, 2016: http://bit.ly/25whJke.

Advocacy for Principled Action in Government
American Civil Liberties Union
American-Arab Anti-Discrimination Committee
Arab American Institute
American Library Association
Bill of Rights Defense Committee
Brennan Center for Justice
Campaign for Liberty
Constitutional Alliance
Defending Dissent Foundation
Demand Progress
Electronic Privacy Information Center (EPIC)
Electronic Frontier Foundation
Free Speech Coalition
Fight for the Future
Government Accountability Project
The Niskanen Center
Media Freedom Foundation
National Security Counselors
National Association of Criminal Defense Lawyers
Liberty Coalition
New America's Open Technology Institute
OpenTheGovernment.org
Project Censored
Project On Government Oversight
Public Citizen
Restore The Fourth
RootsAction.org
R Street
Sunlight Foundation
TechFreedom
X-Lab

cc: Members of the United States Senate Committee on the Judiciary
Members of the United States House of Representatives Committee on the Judiciary