October 29, 2015

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

Dear Director Clapper:

The undersigned organizations, which are dedicated to preserving privacy and civil liberties, write to request that you provide certain basic information about how Section 702 of the Foreign Intelligence Surveillance Act (FISA) affects Americans and other U.S. residents. Disclosing this information is necessary, we believe, to enable informed public debate in advance of any legislative reauthorization efforts in 2017.

We acknowledge that you have publicly released a significant amount of information about Section 702, as well as declassifying information for inclusion in the report of the Privacy and Civil Liberties Oversight Board (PCLOB). These disclosures have been helpful, and we appreciate them. However, there remains a significant and conspicuous knowledge gap when it comes to the impact of Section 702 surveillance on Americans.

Information about that impact is critical in light of official representations that Section 702 is aimed at foreign threats and that collection of Americans' information is merely "incidental." The American public must have the data necessary to evaluate and weigh these official claims. Moreover, it is unacceptable that the government itself has no idea how many Americans are caught up in an intelligence program ostensibly targeted at foreigners. We therefore ask that you disclose the following information, as discussed further below:

- A public estimate of the number of communications or transactions involving American citizens and residents subject to Section 702 surveillance[1] on a yearly basis.

- The number of times each year that the FBI uses a U.S. person identifier to query databases that include Section 702 data, and the number of times the queries return such data.

- Policies governing agencies' notification of individuals that they intend to use information "derived from" Section 702 surveillance in judicial or administrative proceedings.

[1] This request seeks an estimate corresponding to each of the following categories:
(1) The number of communications or transactions involving U.S. residents whose contents or metadata are "screened" for selectors in the course of upstream surveillance;
(2) The number of communications or transactions involving U.S. residents that are retained after their contents or metadata have been screened for selectors in the course of upstream surveillance;
(3) The number of communications or transactions involving U.S. persons that are retained in the course of PRISM surveillance; and
(4) The number of U.S. residents whose information is examined or obtained using any other type of surveillance conducted pursuant to Section 702.

Estimate of How Many Communications Involving U.S. Residents Are Subject to Surveillance

As you know, Senators Wyden and Mark Udall repeatedly have requested that you provide an estimate of how many American communications are collected under Section 702. In 2012, the NSA Inspector General studied whether such an assessment would be feasible. As relayed in a letter from the Inspector General (IG) for the Intelligence Community, the NSA IG concluded that dedicating sufficient resources to such an assessment "would likely impede the NSA's mission." He also concluded that reviewing the NSA's intake to ascertain the effect on American citizens and residents "would itself violate the privacy of U.S. persons."

We disagree with these conclusions and believe that they are undermined by subsequent disclosures. With regard to the question of resources, an October 3, 2011 opinion of the Foreign Intelligence Surveillance Court (FISC) reveals that the NSA, in an effort to address the court's concerns about how many wholly domestic communications were acquired through upstream collection, "conducted a manual review of a random sample consisting of 50,440 Internet transactions taken from the more than 13.25 million Internet transactions acquired through NSA's upstream collection during a six month period." There is no evidence that this undertaking impeded any NSA operations.

Moreover, the NSA's mission is broader than the IG's letter implies. "[P]rotection of privacy and civil liberties" is an express component of the NSA's stated mission. *See* https://www.nsa.gov/about/mission/. Yet the NSA apparently does not know, even at the level of an estimate, how many U.S. person communications it screens or retains under Section 702. The government's lack of information on this critical aspect of its own intelligence activities is remarkable. Ascertaining this information would assist the NSA in pursuing its mission, not impede it.

We understand that the NSA's privacy concerns stem from the possibility that assessing whether communications involve U.S. persons could require a manual review of communications that otherwise would not be accessed or examined. This concern should not arise when ascertaining the impact on U.S. persons of "upstream" surveillance (the term used for obtaining Internet and telephone communications in transit over the telecommunications backbone). These communications contain routing information – the IP address for Internet communications and the country code for telephone communications – that provide a rough, albeit imperfect, indication of the communicants' U.S.-person status. While not an appropriate basis for other extrapolations, this data should be sufficient to provide a broad estimate without any need for manual review. Indeed, the PCLOB has recommended that the NSA count and disclose the number of telephone communications acquired in which one caller is located in the United States, as well as the number of Internet communications acquired through upstream surveillance that originate or terminate in the United States.

About 90 percent of the communications retained under Section 702, however, are stored communications obtained from companies under the PRISM program, which may not contain the same routing information that accompanies communications in transit. In light of the overriding need for Americans to know how this massive surveillance program affects them, the undersigned groups, including many organizations whose missions are centrally focused on

protecting privacy, believe that a one-time, limited sampling of these communications would be a net gain for privacy *if* conducted under appropriate safeguards and conditions.

Many of the undersigned groups possess or have access to significant technical expertise, and are happy to work with the Intelligence Community to devise a minimally intrusive way of ascertaining the U.S.-person status of those whose information is acquired under PRISM. If, after all other alternatives are thoroughly explored, it appears that manual review is required in some instances, measures to mitigate the privacy intrusion would be critical. For instance, the review should be conducted by an independent office; it should use a sample that is about to reach the "age-off" date (*i.e.*, is reaching the end of the applicable retention limit) and is representative of current collection practices; and the communications should be destroyed immediately after review. The review could be used to gauge the percentage of data obtained under PRISM that involves U.S. persons, which then could be applied to the current total number of communications or transactions obtained under PRISM in order to estimate the number of U.S. persons affected.

FBI's Use of U.S. Person Identifiers to Query Section 702 Data

As you know, so-called "back door searches" of Section 702 data are highly controversial. These searches use U.S. person identifiers to query data, even though the data was obtained pursuant to a certification that no U.S. persons were targets. In order to have an informed debate on how Congress should address this issue in 2017, the public needs and deserves better information.

You have disclosed the yearly number of U.S.-person queries that the CIA and NSA perform on Section 702-derived data. You have not disclosed this same figure for the FBI, however, and the USA FREEDOM Act conspicuously exempts the FBI from such a requirement. Given the PCLOB's description of how the FBI uses this information, there is every reason to believe the number of FBI queries far exceeds those of the CIA and NSA. To present a fair overview of how foreign intelligence surveillance is used, it is essential that you work with the Attorney General to release statistics on the FBI's use of U.S. person queries.

There is no practical reason why this information cannot be reported. According to the PCLOB, the FBI does not track U.S. person queries because its minimization rules do not require officials to record whether search terms relate to U.S. persons. However, as evidenced by the NSA and CIA statistics, it is clearly *possible* to record and track that information. Moreover, to the extent the FBI maintains databases in which Section 702 and non-Section 702 data are commingled, that should not be an obstacle. The law requires Section 702 data to be clearly marked as such. For commingled databases, the FBI could simply report the total number of U.S.-person queries, as well as the number of these queries that returned Section 702-derived data.

Notification of Use of Information "Derived From" Section 702

The law requires the government to notify individuals if it intends to use information "obtained or derived" from Section 702 against them in legal or administrative proceedings. Until recently, however, this requirement was honored in the breach. Although the Administration began notifying criminal defendants of the use of Section 702-derived information in October 2013, it

did so in only five cases, and there has not been a single notification in seventeen months. In addition, the Treasury Department's Office of Foreign Assets Control reportedly relies on Section 702-derived information but has never notified those affected by its proceedings. Reports also indicate that some agencies engage in "parallel construction": they reconstruct Section 702-derived information using less controversial methods in order to avoid disclosing the use of Section 702, on the dubious ground that the reconstructed evidence is not "derived from" Section 702 surveillance.

Individuals should know whether they are being given a fair opportunity to challenge Section 702 surveillance when the fruit of such surveillance is used against them. We ask that you disclose how the Department of Justice and other agencies interpret the statutory notification requirement, including the legal interpretations that control when those agencies consider evidence to be "derived from" Section 702 surveillance. These disclosures also should make clear whether evidence collected based on a "tip" arising from Section 702 surveillance is considered "derived" evidence, and the circumstances in which agencies permit investigators to reconstruct evidence originally obtained under Section 702 in order to avoid notification. Keeping these key legal interpretations secret prevents the public from understanding how Section 702 is used in practice, and perpetuates the anti-democratic practice of secret law.

***

The Principles of Intelligence Transparency, adopted by your office in January and reaffirmed through an implementation plan issued by your office two days ago, state that the Intelligence Community 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." This is exactly such a case. The FISA Amendments Act is set to expire on December 31, 2017. Knowing the impact of the law on Americans is not only important to an informed public debate, it is essential. Disclosing the information requested above will remove three of the most significant barriers to that debate.

Sincerely,

Advocacy for Principled Action in Government
American-Arab Anti-Discrimination Committee
American Civil Liberties Union
American Library Association
Bill of Rights Defense Committee
Brennan Center for Justice
Center for Democracy & Technology
The Constitution Project
Constitutional Alliance
Cyber Privacy Project
Defending Dissent Foundation
Demand Progress
DownsizeDC.org, Inc.

Electronic Frontier Foundation
Electronic Privacy Information Center (EPIC)
Fight for the Future
Free Press
Government Accountability Project
Liberty Coalition
National Association of Criminal Defense Lawyers
National Security Counselors
New America's Open Technology Institute
Niskanen Center
OpenTheGovernment.org
PEN American Center
Project On Government Oversight
R Street
Restore the Fourth
The Sunlight Foundation
TechFreedom
World Privacy Forum
X-Lab