January 18, 2017

The Honorable Richard Burr
Chairman
Senate Select Committee on Intelligence
217 Russell Senate Office Building
Washington, D.C. 20510

The Honorable Mark Warner
Vice Chairman
Senate Select Committee on Intelligence
475 Russell Senate Office Building
Washington, D.C. 20510

Chairman Burr, Vice Chairman Warner, and Members of the Committee,

Title VII of the FISA Amendments Act (FAA) will expire on December 31, 2017 unless Congress acts to extend the law. Section 702 of the FAA is used to authorize electronic surveillance targeting non-U.S. Persons where the collection takes place within the United States. This authority is very broad and the programs operated under its purview harm private business and the global internet economy. They also violate international human rights standards.

Without significant reform, Section 702 will continue to threaten the free flow of information overseas, and negatively impact global data privacy and U.S. economic interests internationally. Section 702 programs undoubtedly impact the human rights of U.S. persons. Surveillance under Section 702 was at the heart of the Court of Justice of the European Union's decision to strike down the "Safe Harbor" data transfer arrangement between the United States and the European Union. Safe Harbor was subsequently replaced by the Privacy Shield, which is up for review in the EU this summer as well as being reviewed in two court cases. Unless Section 702 undergoes significant reform to address the issues raised by the CJEU, Privacy Shield will likely also be invalidated, leaving companies and the people who use their services in a state of perpetual uncertainty.

This letter suggests several proposals to amend Section 702 of the FAA. Generally we split these proposals into categories based on whether they are codifying current and former safeguards or seeking new safeguards. There are also proposals in each of these categories that will increase future transparency and accountability of the programs conducted pursuant to Section 702. Several of these proposals are derived from reports of oversight bodies like the Privacy and Civil Liberties Oversight Board (PCLOB) and the President's Review Group. The below list isn't intended to be an exhaustive list of all possible reforms, but to represent ways that Section 702 and the FISA Amendments Act can be narrowed to better respect human rights considerations.

***Current and Former Safeguards***

*Include definitions to ensure proper understanding of the law* - As the PCLOB noted, keys words in the FISA like "targeting" and "reasonable belief" are not defined by law.[1] In addition, while the

[1] https://www.pclob.gov/library/702-Report.pdf

PCLOB sought to reassure the public that the term “selectors” (which is not actually used in the statute but guides the implementation of the programs) no longer is being stretched to include servers or gateways as it was previously, there is no mandatory public reporting that can provide on-going reassurance of this. As we learned in the effort to reform the USA PATRIOT Act from 2013-2015, the ability of the intelligence community to re-define the scope of key terms can have huge impacts on the scale of surveillance. Key definitions and limitations must be written into the public law to protect against this result.

*Codification (and expansion) of Presidential Policy Directive 28* - President Obama took a positive step when he implemented Presidential Policy Directive (PPD) 28, which, among other things, recognized that non-U.S. persons have a legitimate privacy interest.[2] The protections in PPD should be codified into law in order to preserve them against future administrations. In addition, the language should be expanded not to only recognize the interests of these persons, but also that they have rights to privacy and freedom of expression. The other sections in PPD 28, like the prohibition against using surveillance to obtain a competitive advantage, are also important to codify.

*Minimize the data that is retained in massive surveillance databases* - The internal practice at some agencies to mask identifiers of innocent people within surveillance information should be normalized and applied evenly to both U.S. persons and non-U.S. persons. Congress should also codify the requirement that all queries of Section 702 surveillance be documented and included in regular audits.

*Limit surveillance targets to foreign powers or agents of foreign powers* - To limit the number of innocent people included in Section 702 surveillance, targets should be limited, at a minimum, to foreign powers or agents of foreign powers. This was a limitation that was accepted in the original version of the President’s Surveillance Program, which was already considered far too overbroad, but is in fact far narrower than the mass surveillance program that operates today. This requirement, however, could come with additional improvements in process and procedure to help provide the flexibility and fast response time that the government may need.

***New Safeguards***

*Recognize human rights standards* - The International human rights standards generally accepted under treaties ratified by countries around the world, including the United States, require that all surveillance must be both necessary and proportionate. Unfortunately the U.S. has never recognized those rights for non-citizens outside the country. In order for Section 702 to satisfy the United States’ international obligations, not only should surveillance be limited to foreign powers as described above, but operations should be limited to those that are necessary and proportionate to achieve a legitimate and identified aim.

[2]https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

*Strengthen the standards for collection* - The scope of what can be collected under Section 702 is very broad. This should be narrowed. One way would be to limit the definition of "foreign intelligence information," for example by striking the part of the definition that includes "the conduct of the foreign affairs of the United States." Alternatively, the law can be amended to expressly limit the valid foreign intelligence purposes of Section 702, such as to only counter-terrorism or proliferation. In addition, language in Section 702 that presumes to authorize surveillance if the collection of foreign intelligence information is only a "significant" purpose, and not even the primary purpose, must be stricken to remedy a huge loophole to get around the authority's already limited protections for human rights.

*Strike the encryption exception for data retention* - Current policy is that information that is encrypted (or carries "secret meaning") can be retained by the government indefinitely. As expert Laura Donohue has pointed out, it is an exception that threatens to swallow the rule limiting data retention, particularly as the amount of encrypted information on the internet continues to increase (a positive step that protects the digital integrity of users at risk).[3] The current limits on retention should apply regardless of if there is any encryption applied to the information.

*Prohibit acquisition of communications from non-targets* - As part of the Upstream program, the NSA intentionally collects all internet transactions to, from, or "about" a target, and specifically anticipates acquiring communications from people who are not themselves targeted by a program. The government has claimed, and the PCLOB has reiterated, that distinguishing content from metadata in the upstream scan is not possible at this time.[4] But just because unlawful surveillance is necessary to conduct lawful surveillance does not mean it should be condoned. In one case, the NSA had to limit data it was getting under a surveillance program because the technology at the time was unable to comply with statutory limitations - only after the technology was developed to properly limit collection was the collection allowed.[5] Additionally, the ACLU has cast doubt on the overall assertion that there are no technical means to eliminate the acquisition of communications from non-targets.[6]

*Limit the dissemination of data to other agencies and international partners* - Several U.S. government agencies and international partners or allies are authorized to access or receive surveillance data collected under Section 702.[7] Limitations on sharing and dissemination should be codified in order to ensure against secret mission creep and protect the sensitive information of people around the world.

---

[3] http://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=2364&context=facpub
[4] https://www.pclob.gov/library/702-Report.pdf
[5] See Power Wars by Charlie Savage, Chapter 5, Section 4.
[6] https://www.justsecurity.org/33044/unprecedented-unlawful-nsas-upstream-surveillance/?source=techstories.org
[7] https://www.privacyinternational.org/node/51

***Transparency and Accountability***

*Increased transparency at the FISA Court* - The USA FREEDOM Act took a step forward on transparency of FISA Court activities, including by providing for the publication of major FISA Court opinions. To ensure that the public maintains a level of transparency into the operation of these surveillance programs, there should be a requirement that the FISA Court both writes and makes publicly available an opinion on each question of law that it confronts. Additionally, the current USA FREEDOM provisions on publishing court opinions should be given explicit retroactive application to make sure there are no other secret interpretations of law.

*Increased public reporting* - Section 702 has provisions built in for internal oversight in the executive branch, by certain, limited Congressional committees, as well in the FISA Court. The current administration has supported transparency in its policy in favor of publication of certain documents (though not all documents that are necessary to review the programs), though there is no guarantee that it will continue, specifically in the instance of major changes or expansions to the current programs.[8] However, there are few provisions that allow for public transparency into any of the workings of the program. A public eye into the operation of Section 702, as consistent with national security, must be codified to ensure the preservation of current levels of transparency. A start would be to require that reports about Section 702 surveillance, as well as targeting and minimization procedures, be made public to the extent possible.

---

Thank you for your consideration. We look forward to working with you on security and human rights throughout the year.

Sincerely,

Amie Stepanovich
U.S. Policy Manager

Nathan White
Senior Legislative Manager

[8]https://theintercept.com/2015/10/29/privacy-groups-challenge-director-of-national-intelligence-to-uphold-transparency-promise/