Statement for the Record of

Gregory T. Nojeim
Director, Project on Freedom, Security & Technology
Center for Democracy & Technology

Senate Judiciary Committee

May 10, 2016 Hearing on
Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties
May 17, 2016

Chairman Grassley, Ranking Member Leahy, and Members of the Senate Judiciary Committee:

The Center for Democracy & Technology (CDT)[1] submits the following statement for the record summarizing the privacy and civil liberties concerns presented by surveillance under Section 702 of the Foreign Intelligence Surveillance Act (FISA), along with policy recommendations for addressing those concerns. Section 702 is scheduled to sunset on December 31, 2017, and the reauthorization process presents an opportunity to consider reforms. Unlike the independent reviews of bulk collection of telephone call records conducted under Section 215 of the Patriot Act, independent reviews of Section 702 surveillance confirm that 702 surveillance has been useful in thwarting terrorist attacks. Accordingly, our recommendations are calibrated to focus the warrantless surveillance program onto its appropriate purpose: intelligence gathering for the detection and prevention of national security threats to the United States, including terrorism.

The 2008 FISA Amendments Act, which added Section 702 to FISA, made a fundamental change in FISA for surveillance conducted in the US of non-US persons: it did away with the requirement that the target of surveillance be a terrorist, a spy, or another agent of a foreign power. The only meaningful limitation on the scope of Section 702 surveillance of non-U.S. persons abroad is the limitation that "a significant purpose" of surveillance must be to collect "foreign intelligence information."[2] The primary purpose can be something else entirely, including investigation of crime or tax evasion. Moreover, "foreign intelligence" is broadly defined to include information that merely relates to U.S. foreign

[1] The Center for Democracy & Technology is a nonprofit public interest organization dedicated to keeping the internet open, innovative and free. Among our priorities is preserving the balance between security and freedom for U.S. and non-U.S. persons alike.
[2] 50 U.S.C. § 1881a(g)(2)(A)(v).

policy and national security.[3] When protesters gather in Istanbul, Brasília, Cairo, or Paris to protest government policies, the reasons for their protests "relate" to U.S. foreign policy. Section 702 gives the NSA statutory authority to compel U.S. communications service providers to disclose the protesters' stored email or to assist with wiretapping them. This is far too broad an authority, and it goes well beyond fighting terrorism.

Reports resulting from disclosures by Edward Snowden and subsequent declassifications by the federal government confirm that Section 702 surveillance sweeps broadly, and compromises the privacy rights of non-targets of the surveillance. In 2014, the *Washington Post* examined a large sample of e-mails and instant messenger conversations collected under Section 702 between 2009 and 2012, and found that 90 percent of the communications the government had captured and retained were from online accounts not belonging to foreign surveillance targets.[4] A surveillance program purportedly geared towards foreign intelligence has instead swept up a huge amount of communications content belonging to innocent, untargeted people,[5] and the fruits of those warrantless searches have been used to conduct criminal investigations against Americans – investigations that are unrelated to national security and terrorist activity.[6]

Overall, the Section 702 program has strayed too far from the world envisaged by the authors of the U.S. Constitution – a world where an American need not worry about general "writs of assistance" because his government may only intrude upon his sensitive papers and effects when a judicial authority finds there is strong evidence that he is up to no good. Moreover, the overbroad collection, retention, and querying of data for a myriad of purposes unrelated to national security has violated the privacy obligations of the United States under the International Covenant on Civil and Political Rights[7] and the American Declaration of the Rights and Duties of Man.[8]

This broad surveillance program threatens not just privacy rights in the U.S. and abroad, but the flow of data for commercial reasons between the U.S. and Europe. In *Schrems v. Data Protection*

---

[3] 50 U.S.C. § 1801(e).

[4] Barton Gellman, Julie Tate & Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," WASH. POST (Aug. 8, 2013), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

[5] *Id.*

[6] *See* Privacy and Civil Liberties Oversight Board (PCLOB), "Report on the Surveillance Programs Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 64 (July 2, 2014) [hereinafter "PCLOB Report"]; *see also* John Shiffman and Kristina Cooke, "Exclusive: U.S. directs agents to cover up program used to investigate Americans," REUTERS (Aug. 5, 2013), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805.

[7] International Covenant of Civil and Political Rights (ICCPR), G.A. res. 2200A (XXI), 21 U.N. GAOR Supp. (No. 16) at 52, U.N. Doc. A/6316 (1966), 999 U.N.T.S. 171 (Mar. 23, 1976), http://www1.umn.edu/humanrts/instree/b3ccpr.htm.

[8] American Declaration of the Rights and Duties of Man (1948), http://www.cidh.oas.org/Basicos/English/Basic2.american%20Declaration.htm.

Commissioner,[9] the Court of Justice of the European Union (CJEU) struck down the U.S.-E.U. Safe Harbor agreement, an agreement vital to transatlantic trade on which over 4,000 U.S. companies had relied for fifteen years. The CJEU found that the European Commission, in approving the Safe Harbor, had not adequately accounted for the extent to which Europeans' data transferred to the United States by U.S. companies was accessible for surveillance purposes. In addition, a 2014 analysis found that U.S. technology companies, particularly in the cloud-computing sector, are likely to lose billions of dollars in revenue due to U.S. warrantless surveillance.[10]

As the Section 702 sunset date approaches, CDT encourages Congress to embrace the reforms below not just because they would facilitate commercial trade, but because they would advance the human rights of people on a global basis, strengthen the tenuous constitutional foundation on which the surveillance program now rests, and better focus the surveillance on terrorism and other national security threats the United now faces.

I. Use and Retention of Data Collected Under Section 702

The amount of data the Intelligence Community already has on hand as a result of Section 702 is staggering. The government has estimated that in 2015, it had 94,368 targets under the program.[11] In addition, a mere three years after the program's inception, the NSA was acquiring approximately 26.5 million internet transactions per year through Upstream collection.[12] Therefore, this Statement begins with proposals for limiting the further retention and use of data that already has been collected, and will be collected under Section 702 in the future.

A. Problem: *The Backdoor Search Loophole*

Although Section 702 was authorized for purposes of collecting foreign intelligence information about non-U.S. persons abroad, the government is using the program to access information about U.S. persons located in the United States without judicial oversight. This practice is commonly referred to as the "backdoor search loophole" because if the NSA wanted to conduct the surveillance of U.S. persons

[9] Case C-362/14, *Maximillian Schrems v. Data Protection Comm'r* (Oct. 6, 2015), *available at*: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

[10] Danielle Kehl et al., *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE 7-13 (2014), https://www.newamerica.org/downloads/Surveilance_Costs_Final.pdf.

[11] ODNI, "Statistical Transparency Report Regarding Use of National Security Authorities," 5 (April 30, 2016) [Hereinafter "ODNI Statistical Report"], *available at* https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf.

[12] PCLOB Report at 37. An internet "transaction" refers to "any set of data that travels across the Internet together such that it might be understood by a device on the internet." Such transactions may involve a single communication (such as an email sent from one server to another) – referred to as Single Communication Transactions (SCT's) – or it may involve multiple communication transactions – referred to as Multiple Communication Transactions (MCT's). *See* PCLOB Report at 39.

directly, it would have to obtain a full FISA Court (FISC) order based on a finding that the U.S. person is a terrorist, spy, or other agent of a foreign power.[13] Similarly, if the FBI wanted to search a U.S. person's communications content for criminal purposes, its procedures would require it to obtain a warrant based on probable cause. A 2016 report released by the Office of the Director of National Intelligence shows that the backdoor search loophole is being used by the NSA and the CIA more than ever before: last year, there were 4,672 acknowledged backdoor searches of U.S.-person content in the agencies' Section 702 databases, representing over a 223% increase since 2013.[14,15] That number does not include the number of FBI queries, because the FBI is excluded from this reporting requirement established by the USA FREEDOM Act.

In 2015, the Administration announced a new policy to limit the backdoor search capability, but, as evidenced by the ODNI's statistical reporting, these changes did little to nothing to close the door. Under the new policy, the NSA and the CIA can query their 702 databases with U.S. person identifiers only after developing a "written statement of facts showing that a query is reasonably likely to return foreign intelligence information."[16] This change, although welcome, is still a far cry from requiring a judicial finding of probable cause that the person whose communications are sought is an agent of a foreign power, as Senator Ron Wyden has previously recommended.[17] Moreover, a recently released FISC opinion from November 2015 confirms that the FBI is not limited to this same restriction, and that the FBI may even query 702 data with U.S. person information in order to *initiate* an investigation of any federal crime.[18] Although the FBI has claimed that only FBI personnel with specialized training can view 702 data, there is an easy workaround to this limitation: if authorized personnel determine that the 702 information that the non-authorized personnel wishes to view contains evidence of a crime, then the non-authorized personnel may view that 702 information.[19] As a result, this "limitation" is a very mild one – it is tantamount to asking someone else to search a home, retrieve any evidence of any crime that they find, and then hand over that information to law enforcement officials who did not obtain a warrant to search that home themselves.

i. Recommendation: *Congress should amend Section 702 to require the government to obtain a search warrant based on a finding of probable cause to search for communications content of particular U.S. persons in information obtained through Section 702 surveillance.*

[13] 50 U.S.C. § 1805.
[14] ODNI Statistical Report at 5.
[15] PCLOB Report at 57-58.
[16] "New Privacy Protections for Information Collected Under Section 702," IC ON THE RECORD (Feb. 3, 2015), https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.
[17] The Intelligence Oversight and Surveillance Reform Act (S.1551) (Introduced Sept. 25, 2013), https://www.govtrack.us/congress/bills/113/s1551/text.
[18] [Redacted], Docket [Redacted], at *27–28 and n. 27 (FISC Nov. 6, 2015) [hereinafter "Hogan Opinion"], *available at*: https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[19] *Id.* at 35.

Congress explicitly barred use of Section 702's broad authority to intentionally target U.S. persons for surveillance. To prohibit targeting of U.S. persons, but then permit the NSA, CIA, and FBI to search for U.S. persons' communications that are incidentally swept into the database violates the spirit of the law and undermines protections that were included by Congress. To prevent this abuse, Section 702 should be amended to state that, absent an imminent emergency, a search of the database with a U.S. person identifier is prohibited unless the FISC has determined that there is probable cause to believe that the U.S. person is a terrorist, spy, or other agent of a foreign power – the same legal standard required to authorize direct surveillance of that U.S. person under 50 U.S.C. section 1805.

B. Problem: *702 Data Is Being Used in Criminal Investigations Against U.S. Persons*

Under the NSA's old Section 702 Minimization Guidelines, the NSA was permitted to retain, share, and use communications about U.S. persons that may constitute evidence of any crime.[20] Under the Administration's new policy announced in 2015, such information "will not be introduced as evidence against that [U.S.] person in any criminal proceeding except 1) with the approval of the Attorney General, and 2) in criminal cases with national security implications or certain other serious crimes."[21] Director of National Intelligence General Counsel Robert Litt clarified that "serious crimes" would be limited to crimes involving: 1) death, 2) kidnapping, 3) substantial bodily harm, 4) conduct that constitutes a criminal offense that is a specified offense against a minor as defined under 42 U.S.C. § 16911, 5) incapacitation or destruction of critical infrastructure as defined in 42 U.S.C. § 5195c(e), 6) cybersecurity, 7) transnational crimes, and 8) human trafficking.[22]

Although these changes are a positive step in the right direction, there is still a lot of room for improvement. Terms such as "criminal cases with national security implications" and "crimes involving cybersecurity" are undefined, and capable of being applied too broadly. Moreover, the limitations were not officially adopted into the NSA, CIA, or FBI's minimization procedures, [23] which means they can be changed at any time, without FISC or Attorney General approval.[24] Finally, even if 702-acquired data cannot be introduced as *evidence* in a criminal case, law enforcement agents can still *use* such information to obtain other evidence that they *can* use in their investigations. This is especially

[20] *See, e.g.*, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2014) [Hereinafter "Minimization Procedures"], *available at*: https://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf.

[21] IC ON THE RECORD, *supra* n.16.

[22] "ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute," IC ON THE RECORD (Feb. 4, 2015), *available at*: https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on.

[23] Hogan opinion at n.18.

[24] If included in the minimization procedures, the limitations could not be changed without the approval of the Attorney General and the FISC. *See* 50 U.S.C. § 1881a(e).

troubling, given the U.S. Drug Enforcement Administration's use of parallel construction to rely on information obtained through intelligence surveillance throughout their criminal investigations, then obscure the source of that intelligence information from the defendant and his attorney.[25]

i. Recommendation: *Congress should codify the use restrictions announced by the Administration in 2015, and make such restrictions apply to all uses of the information to conduct criminal investigations – not only to evidence used in court.*

The retention and dissemination of U.S. persons' communications for law enforcement purposes permits an end-run around the Fourth Amendment, which would bar the collection and use of those communications without a probable cause finding by a court. Congress should codify the use restrictions announced by the Administration and apply those restrictions to all uses of 702-derived information in criminal cases. The law should also be amended to require that the use limitations be included in the Intelligence Community's minimization procedures.

C. Problem: *FISA's Retention Limitations Contain a Cryptanalysis Exception*

In general, data acquired under Section 702 may only be retained on FBI, CIA, and NSA systems for no more than five years.[26] In addition, domestic communications must be promptly destroyed upon recognition.[27] However, the NSA's Minimization Procedures permit unlimited retention and dissemination of communications – including those of U.S. persons – that are "enciphered or reasonably believed to contain secret meaning," as well as communications that could otherwise aid cryptanalysis.[28] This is a significant loophole to the retention and purging requirements, because the services that average individuals use are increasingly encrypting communications by default.[29] In addition, encrypting communication in no way implies that it includes information that is relevant to a national security threat.

i. Recommendation: *Congress should prohibit exempting communications from Section 702 data retention limits solely because they are encrypted*

The move toward universal encryption could, over time, make a five-year retention limit for Section 702 data the exception, rather than the rule. Closing the cryptanalysis loophole would not allow malicious use of encryption to override legitimate foreign intelligence needs. The government would

[25] Shiffman and Cooke, *supra* n. 6.
[26] PCLOB Report at 60.
[27] Minimization Procedures at Sec. 5.
[28] *Id.* at Sec. 5(3).
[29] *See, e.g.*, Cade Metz, "Forget Apple vs. the FBI: WhatsApp Just Switched On Encryption for a Billion People," WIRED (April 5, 2016), http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

still be permitted to retain encrypted communications when they are reasonably believed to contain foreign intelligence,[30] but encryption should no longer be the sole basis for retaining a communication.

II. Collection and Targeting Under Section 702

A. Problem: *Purposes for Which 702 Surveillance May Be Conducted Are Too Broad*

Despite claims that 702 surveillance is "targeted," the program can be accurately characterized as a "bulk-ish" collection program because the purpose for which the surveillance may be conducted is overly broad, which has resulted in hundreds of millions of communications with little to no foreign intelligence value being swept up by the program.[31] Under Section 702 of FISA, the government is authorized to collect "foreign intelligence information," which, for information pertaining to non-U.S. persons, is broadly defined as 1) information that *relates to* the ability of the U.S. to protect against a hostile attack, espionage, sabotage, international terrorism, or proliferation of weapons of mass destruction; or 2) information with respect to a foreign territory or foreign power (which includes a foreign government, political party, or entity controlled by a foreign government, or a foreign terrorist organization) that *relates to* the security of the U.S. or to the conduct of U.S. foreign affairs.[32]

Moreover, it is the NSA, not the FISC, that determines whether tasking a selector (such as an email address) belonging to a target will likely result in one of the approved categories of foreign intelligence information. The NSA's Targeting Procedures, which were leaked by Edward Snowden, contain a non-exhaustive list of factors that the NSA considers when making this determination, and these factors demonstrate just how easily a non-U.S. person located abroad can have their communications acquired by the foreign intelligence program. The assessment of whether or not a target may possess foreign intelligence information includes, for example, determining whether or not there is "reason to believe" the target is or has communicated with an individual "associated with" a foreign power or territory.[33] What it takes to be considered "associated with" a foreign power or territory is unclear.

The alarmingly lax standards used for determining whether the purpose of Section 702 is being fulfilled in practice has prompted concern globally that surveillance under Section 702 is broadly directed at individuals not suspected of wrongdoing. This over breadth was, we believe, in large part what led the CJEU to strike down the Safe Harbor agreement. The *Schrems* judgment indicated that E.U.-U.S. data

[30] Such belief may be formed based on metadata analysis and other circumstances under which the communication was made, without accessing the encrypted contents of the communication.
[31] *See* Gellman et al., *supra* n. 4.
[32] *See* 50 U.S.C. § 1801(e) (emphasis added). For information concerning U.S. persons, the information must be "necessary to," rather than "relate to." *Id*.
[33] *See* PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (current as of July 2009) [Hereinafter "Targeting Procedures"], *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716665/exhibit-a.pdf.

transfers should not take place unless the U.S. government can only gain access to (and use) the data "for purposes which are specific, strictly restricted and capable of justifying" the privacy intrusion involved.[34] Although a Presidential Policy Directive, PPD-28, limits the *use* of data collected *in bulk* to five broadly-defined national security purposes,[35] it includes no meaningful limitations on the initial collection. Without meaningful reform to the scope of Section 702 surveillance, the Privacy Shield[36] – which the U.S. and E.U. proposed as the successor to the Safe Harbor agreement – can best be understood as only a short-term, partial solution for enabling transatlantic data flows.

i. Recommendation: *702 surveillance should only be conducted for carefully defined national security purposes*.

In order to rebuild U.S. commercial relations and the U.S. reputation as a champion for human rights, Congress should require that the federal government only collect and use information under Section 702 for the purposes outlined in PPD-28. This would require that collection and use only occur for purposes of detecting and countering: 1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests, 2) threats to the United States and its interests from terrorism, 3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction, 4) cybersecurity threats, 5) threats to U.S. or Allied Forces or other U.S. or allied personnel, and 6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named above. This change would provide significant comfort to non-U.S. persons abroad who are concerned about the impact that Section 702 surveillance would otherwise have on their human rights. In addition, it would increase the likelihood that Section 702 surveillance would meet international human rights standards, and thereby facilitate trans-Atlantic trade by increasing the chances that the EU-US Privacy Shield will survive court review in the future.

B. Problem: *Overbroad Upstream Collection of Communications "About" Targets*

Even though Congress did not have any meaningful debate about the issue, the Intelligence Community interprets Section 702 as permitting it to collect communications that are not even to or from non-U.S. person targets. Instead, it interprets 702's authorization to "target" as an authorization to collect communications that are to, from *or about* a targeted person. It collects "about" communications upstream – at various collection points along the Internet backbone – in program appropriately called "Upstream." [37] Targeting in this program consists of searching a vast

[34] Case C-362/14 at ¶ 93.
[35] Presidential Policy Directive/PPD-28 (Jan 17, 2014) *available at* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[36] http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf.
[37] PCLOB Report at 36-37.

communications stream for identifiers like email addresses and IP addresses that are tied to a person.[38] Even though it amounts to only 9% of the communications collected under Section 702,[39] "about" collection is particularly concerning: it is a search of communications content in the United States without a warrant for communications that are not even to or from a person thought to have valuable intelligence information. It is far different from Section 702's PRISM program, in which the NSA compels disclosure of content and metadata in communications to or from the target.

This approach results in an astonishingly vast amount of data ending up in government hands. As of 2011, the NSA acquired approximately 26.5 million internet transactions per year as a result of the Upstream collection program.[40] Such transactions include "multi-communication transactions," (MCT's) which include tens of thousands of wholly domestic communications each year.[41]

Finally, "about" collection is not authorized by the Section 702 statute. Section 702 authorizes the government to target the communications "of persons" reasonably believed to be abroad.[42] Although the statute never defines the term "target," throughout the statute the term is used to refer to the targeting of an individual rather than the content of a communication. Moreover, the entire congressional debate on Section 702 includes no reference to collecting communications "about" a target, and significant debate about collection of communications to or from a target.

i. Recommendation: *Congress should amend Section 702 to permit the collection only of communications to or from a target and end Upstream collection*

Abandoning Upstream and "about" collection would eliminate the collection of tens of thousands of wholly domestic communications in contravention of the statute, make surveillance under Section 702 consistent with congressional intent, and end the "dragnet" nature of 702 surveillance that led the CJEU to conclude that Europeans' data are searched in a generalized, indiscriminate manner when

[38] Earlier reports indicated that the NSA conducted this surveillance by "temporarily copying and then sifting through the contents of what is apparently most emails and other text-based communications that cross the border." *See* Charlie Savage, *N.S.A. Said to Search Content of Messages to and from the U.S.*, N.Y. TIMES (Aug. 8, 2013), *available at*: http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?_r=0. However, a more recent report asserts that it's the telecom partners who do the copying and sifting on the NSA's behalf, and they then forward the communications content that results from running selectors against the data stream.[38]. *See* Julia Angwin, Charlie Savage, Jeff Larson, Henrik Moltke, Laura Poitras, and James Risen, "AT&T Helped U.S. Spy on Internet on Vast Scale," N.Y. TIMES (Aug. 15, 2015), http://www.nytimes.com/2015/08/16/us/politics/att-helped-nsa-spy-on-an-array-of-internet-traffic.html.

[39] Memorandum Opinion at 29-30, [*Caption* Redacted], [Docket No. Redacted] (FISA Ct. Oct. 3, 2011) [Hereinafter Judge Bates 2011 Opinion], *available at*: https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2013/08/162016974-FISA-court-opinion-with-exemptions.pdf.

[40] PCLOB Report at 37.

[41] Judge Bates Opinion at 33.

[42] 50 U.S.C. § 1881a(a).

transferred overseas to the United States.[43] In connection with its assessment of this recommendation, Congress should ask the Director of National Intelligence to disclose the extent to which Upstream surveillance as opposed to PRISM surveillance has been effective in thwarting terrorist attacks.

III. Oversight and Transparency

The USA FREEDOM Act enacted several welcome reforms to U.S. surveillance law, including improvements to the Section 702 oversight process. However, Congress can enhance the oversight and transparency 702 program during the reauthorization process in the following ways:

A. Recommendation: *Give FISC amici the ability to appeal decisions made in favor of the government*. Section 401 of the USA FREEDOM Act authorized the presiding judge of the FISC to establish a panel of at least five "amicus curiae" who represent privacy and civil liberties concerns before the FISC. Although a welcome step in the right direction, these amici do not have the power to appeal a FISC decision. Instead, it's the FISC itself that must certify a legal question for appellate review. Even if it does, the amici may not be permitted to participate in the appellate process. As but one example, Judge Hogan's recently released November 2015 opinion,[44] which responded to a lengthy, complex Fourth Amendment argument against the FBI's ability to query 702 data with U.S.-person identifiers in a mere five pages, suggests a need for the possibility of further review. Currently, only the government can seek review of an adverse decision. Given the uniquely invasive nature of the 702 surveillance program, as much consideration should be given to privacy and civil liberties interests as is given to the government's interests when the FISC makes decisions about important questions of law. Granting the FISC amici the ability to appeal to the FISA Court of Review would also encourage the highest quality of judicial decision-making at the FISC level.

B. Recommendation: *Create a genuine ability for individuals whose communications might be subject to secret surveillance to obtain redress for any abuses*: In the *Schrems* decision, the CJEU emphasized the need for individuals to have some type of access to judicial review of decisions pertaining to their personal data.[45] The Judicial Redress Act was a limited first step to affording some non-U.S. persons a small degree of judicial review under the Privacy Act.[46] However, the Privacy Act provides no meaningful

[43] The CJEU found in the *Schrems* decision that laws allowing government authorities to have "access on a generalised basis to the content of electronic communications" violate "the essence of the fundamental right to respect for private life." Case C-362/14 at ¶ 95.
[44] *See* Hogan Opinion, *supra* n. 18.
[45] Case C-362/14 at ¶ 95.
[46] For CDT's analysis of the Judicial Redress Act, see https://cdt.org/blog/the-eu-us-umbrella-agreement-and-the-judicial-redress-act-small-steps-forward-for-eu-citizens-privacy-rights/; *see generally* 32 CFR § 322.7(a).

redress for targets of intelligence agency surveillance under Section 702 because of national security exceptions.[47] Congress should provide an effective judicial redress mechanism for individuals whose communications might be subject to Section 702 surveillance. This can be achieved by providing a right to standing for people who can produce evidence that they may have been unlawfully surveilled.

C. Recommendation: *Permit companies to disclose more detailed statistics on U.S. government requests for data*: Currently, companies are only allowed to disclose the number of requests they receive under the Foreign Intelligence Surveillance Act within broad ranges (such as 0 to 999 requests), and they are only allowed to disclose such information six months in arrears. However, in order to more accurately evaluate U.S. surveillance practices and their impact on privacy and civil liberties, companies should be permitted to make more granular disclosures.

IV. Conclusion

CDT appreciates the opportunity to present its views to the Senate Judiciary Committee as it prepares to reexamine one of the largest, most complex, and most controversial government surveillance programs in American history. For more information, please contact Greg Nojeim, CDT's Director, Project on Freedom, Security & Technology, gnojeim@cdt.org; or Jadzia Butler, CDT's Privacy, Surveillance, and Security Fellow, jbutler@cdt.org.

[47] 5 U.S.C. § 552a(k).