KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of Harley Geiger

Senior Counsel and Deputy Director, Project on Freedom, Security, and Technology
Center for Democracy & Technology

Hearing Before the Senate Select Committee on Intelligence
On
the USA FREEDOM Act, H.R. 3361

June 5, 2014

Chairman Feinstein, Vice Chairman Chambliss, and members of the Committee,

Thank you for the opportunity to testify today on behalf of the Center for Democracy & Technology. We applaud the Committee for holding this rare open hearing to advance a diligent and thoughtful analysis of the USA FREEDOM Act (H.R. 3361), and for the significant amount of time and energy this Committee and its members have devoted to the important debate on government surveillance that has occurred over the last year.

I am Senior Counsel and Deputy Director of the Project on Freedom, Security, and Technology at the Center for Democracy & Technology (CDT). CDT is a nonpartisan, non-profit technology policy advocacy organization dedicated to protecting civil liberties such as privacy, free speech, and access to information. Our Project on Freedom, Security, and Technology works to develop and promote policies that safeguard individuals from overbroad government surveillance while also preserving the government's ability to protect national security from evolving threats. We believe those threats are real, substantial and persistent, and we appreciate the work the intelligence community does to protect the nation against them, and this Committee's efforts to oversee that work.

Introduction

The past year has seen public disclosure of multiple national security programs involving the collection – by the National Security Agency (NSA), a highly secretive military intelligence agency – of sensitive data of many millions of Americans and non-Americans with no

connection to a crime or terrorism.[1] This has prompted a thorough, impassioned, and much-needed debate regarding the appropriate scope of government surveillance, including numerous hearings from various Congressional committees, and comprehensive reports from the President's Review Group on Intelligence and Communications Technologies and the Privacy and Civil Liberties Oversight Board.[2] The stakes in this debate are high because the technological capabilities to collect and analyze information in very large quantities, and to glean intimate details and patterns about individuals, will rapidly grow more sophisticated as computing power continues to expand and digital services become more interwoven into everyday life. Congress has a responsibility to safeguard privacy not just from the surveillance programs and technologies of today, but those of the future as well. The surveillance reforms Congress settles on may not be revisited for decades, and we may be living in quite a different world by the time Congress considers the next major privacy update to national security surveillance authorities.

Although questions remain and further debate is needed in many areas, a near consensus has emerged on a critical issue that has been of central focus to the American public: The government's bulk collection of records of phone calls and emails to, from and within the United States is both intrusive and unnecessary, and Congress must act to prohibit this activity.[3] The vehicle with the most headway in accomplishing this goal is the bicameral, bipartisan USA FREEDOM Act.[4] The USA FREEDOM Act directly takes on the bulk collection problem, attempting to prohibit untargeted mass collection while preserving the key requirement of prior court approval for surveillance demands, without unreasonably interfering with the government's

---

[1] These programs include the bulk collection of telephone and Internet metadata under Section 215 of the PATRIOT Act and the pen/trap statute, respectively. *See*, Amended Memorandum Opinion, *In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things*, No. BR 13-109 (FISA Ct. Aug. 29, 2013), available at http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf. *See also,* Opinion and Order, No. PR/TT [redacted] (FISA Ct.), available at http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

[2] The President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, (Dec. 12, 2013), available at http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, hereafter President's Review Group Report. The Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court*, (Jan. 23, 2014), available at http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf, hereafter PCLOB §215 Report.

[3] President's Review Group Report, pgs. 104, 118: "Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders.... Even without collecting and storing bulk telephony meta-data itself, there are alternative ways for the government to achieve its legitimate goals, while significantly limiting the invasion of privacy and the risk of government abuse." *See also*, PCLOB §215 Report, pgs. 15, 155: "We have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a counterterrorism investigation. Moreover, we are aware of no instance in which the program directly contributed to the discovery of a previously unknown terrorist plot or the disruption of a terrorist attack.... Given the limited value this program has demonstrated to date, as outlined above, we find little reason to expect that it is likely to provide significant value, much less essential value, in safeguarding the nation in the future." *See also*, *First Unitarian Church of Los Angeles v. National Security Agency,* Brief of Amici Curiae Senator Ron Wyden, Senator Mark Udall, & Senator Martin Heinrich, Case No. 3:13-cv-03287 JSW, N.D. Cal., Nov. 18, 2013, pg. 2, https://www.eff.org/files/2013/11/18/senatorsamicibrief.pdf. "[We] have reviewed this surveillance extensively and have seen no evidence that the bulk collection of Americans' phone records has provided any intelligence of value that could not have been gathered through less intrusive means."

[4] H.R. 3361, S. 1599.

ability to make targeted record requests. The legislation also pursues other important reforms, including permitting greater company disclosure regarding national security orders, and enhancing transparency of the Foreign Intelligence Surveillance Court (FISC).

The USA FREEDOM Act was never intended to resolve all of the profound civil liberties problems raised by overbroad national security surveillance. For example, the bill would make only very limited reforms to Sec. 702 of the Foreign Intelligence Surveillance Act (FISA), does not provide significant additional privacy protections for non-U.S. persons abroad, and takes no steps to prevent the undermining of cryptography standards.[5] These matters need to be addressed in other legislation. From the outset, USA FREEDOM was a compromise. Nonetheless, the Center for Democracy & Technology, numerous civil society organizations spanning the political spectrum, and many of America's largest technology companies initially lent strong public support to these efforts.[6] This support continued after a House Judiciary Committee markup weakened the bill's provisions on private party reporting, government transparency, FISC reforms, and the modest improvements to Sec. 702 of FISA.[7]

However, the compromise ultimately went too far. Additional last-minute changes were made to the USA FREEDOM Act prior to final passage in the House of Representatives – notably, changes to the requirement that a "specific selection term" be used as a means of preventing bulk collection. This sudden change raised serious concerns regarding the bill's effectiveness in limiting overbroad surveillance activity, causing CDT, many tech companies, and other civil society groups to remove support for the bill for which we had fiercely advocated for more than half a year.[8] When the weakened USA FREEDOM Act went to the House Floor for final passage, a bipartisan majority of the bill's own cosponsors voted against it, and a majority of the votes against the bill were cosponsors.[9] The bottom line is that there are strong, widespread doubts that the bill that passed the House achieves its stated goal of ending the government's bulk collection of Americans' personal information.

The Senate – and this Committee – now have the opportunity to shore up weaknesses in the USA FREEDOM Act and pass legislation that would significantly advance the privacy interests of Americans while protecting national security. However, in order to ensure that the USA FREEDOM Act actually achieves its goals and fulfills the public's strong desire to prohibit overbroad surveillance, additional protections and clarity must be provided.

---

[5] Jospeh Menn, *NSA infiltrated RSA security more deeply than thought – study*, Reuters, Mar. 31, 2014, http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331.

[6] Sen. Leahy, *USA FREEDOM Act draws bipartisan praise*, Nov. 1, 2013, https://www.leahy.senate.gov/press/usa-freedom-act-draws-bipartisan-praise. *See also*, CDT letter to Senate and House endorsing USA FREEDOM Act, Center for Democracy & Technology, Oct. 29, 2013, https://cdt.org/insight/cdt-letter-to-senate-and-house-endorsing-usa-freedom-act.

[7] *See*, e.g., Harley Geiger, *USA FREEDOM Act Moves Forward*, Center for Democracy & Technology, May 5, 2014, https://cdt.org/blog/usa-freedom-act-moves-forward.

[8] Center for Democracy & Technology, *House Leadership Moves to Gut USA FREEDOM Act*, May 20, 2014, https://cdt.org/press/house-leadership-moves-to-gut-usa-freedom-act. *See also*, Dustin Volz, *Google, Facebook Warn NSA Bill Wouldn't Stop Mass Surveillance*, May 21, 2014, http://www.nationaljournal.com/tech/google-facebook-warn-nsa-bill-wouldn-t-stop-mass-surveillance-20140521.

[9] Jim Cook, *Amash: USA Freedom Act was Flipped so badly, a Majority of Cosponsors Voted Against It*, Irregular Times, May 23, 2014, http://irregulartimes.com/2014/05/23/amash-usa-freedom-act-was-flipped-so-badly-a-majority-of-cosponsors-voted-against-it.

I. Further Action is Necessary to End Bulk Collection of Americans' Private Information

The driving force behind the USA FREEDOM Act has been the need to prohibit bulk collection of Americans' sensitive personal information. Ending "bulk collection" does not just mean ceasing nationwide untargeted surveillance dragnets, but prohibiting large-scale government collection and retention of non-public records about persons who are not connected to national security threats. It would merely perpetuate existing problems to allegedly prohibit nationwide "bulk collection" while permitting collection on the scale of a state or city, or of millions of users of an Internet service provider, with a single FISA order.[10] Unfortunately, the USA FREEDOM Act, as passed by the House of Representatives, does not clearly prohibit such activity, nor does it take sufficient steps to protect the privacy of innocent individuals that would be swept up in such broad surveillance.

The primary means that the USA FREEDOM Act, as passed by the House of Representatives, seeks to prevent bulk collection is by requiring that the government use a "specific selection term" as the basis for production in requests for information under Sec. 215 of the PATRIOT Act, the FISA pen/trap authority, and national security letters (NSLs).[11] Applying this requirement to all intelligence authorities that could be used for the domestic collection of data is critically important: it can prevent the migration of bulk collection activities from one provision of the law to another. The requirement must be designed to ensure that every surveillance order describes the information targeted, thereby preventing virtually limitless surveillance orders that could vacuum up records about masses of people, or even the entire nation. As the lynchpin of the bill's purported prohibition on bulk collection, the definition of "specific selection term" is quite important.

When the USA FREEDOM Act unanimously passed the House Judiciary Committee and the House Permanent Select Committee on Intelligence, "specific selection term" was defined as "a term used to uniquely describe a person, entity, or account."[12] However, prior to consideration before the full House, this critical definition was significantly weakened. The new definition of "specific selection term" was "a discrete term, such as a term specifically identifying a person, entity, account, address, or device, used by the Government to limit the scope of information or tangible things sought pursuant to the statute authorizing the provision of such information or tangible things to the Government."[13] This change to the bill, more than any other, caused major technology companies, civil society groups, and a majority of the bill's cosponsors to pull their support for the USA FREEDOM Act.[14]

There is a major lack of clarity regarding what this new definition of "specific selection term"

---

[10] "The Board also recommends against the enactment of legislation that would merely codify the existing program or any other program that collected bulk data on such a massive scale regarding individuals with no suspected ties to terrorism or criminal activity. While new legislation could provide clear statutory authorization for a program that currently lacks a sound statutory footing, any new bulk collection program would still pose grave threats to privacy and civil liberties." PCLOB §215 report, pg. 169.

[11] H.R. 3361, as engrossed, 113th Cong., Secs. 103, 201, and 501.

[12] H.R. 3361, as reported, 113th Cong., Sec. 107.

[13] H.R. 3361, as engrossed, Sec. 107.

[14] Harley Geiger, *Why We Can't Support the New USA FREEDOM Act*, Just Security, May 21, 2014, http://justsecurity.org/10689/guest-post-support-usa-freedom-act.

would authorize and prohibit in practice. At its core, the definition requires "a distinct term to limit the scope of information sought," but there is no indication as to how stringent the limit must be. Although agencies may currently use selection terms to query data collected under surveillance authorities, this is an internal process and there is no history of the use of selection terms in law. Ambiguity is the point – the bill's definition is deliberately open-ended to provide the government with broad flexibility in making surveillance requests. One could argue that any term the government uses to limit in any way the scope of the information or tangible things it seeks using its domestic intelligence authorities fits the definition. Yet the highly controversial domestic telephony and Internet metadata bulk collection programs that prompted Congressional action were themselves borne of the government's exploitation of ambiguous terms in existing statutes and the FISC's willingness to accept these interpretations – "relevant to an authorized investigation" led to authorizations to collect the phone and email records of virtually everyone in the United States.[15] Similarly broad interpretations of the USA FREEDOM Act's definition of "specific selection term" could effectively perpetuate mass collection of data about people in the U.S.

For example, if a government application for email records used as selection terms the names of the top four email services in the United States, how would this meaningfully differ from the very type of mass, untargeted data collection that the USA FREEDOM Act was created to prevent?

Another example – it is entirely unclear whether the new definition of "specific collection term" would allow the government to use geographic regions such as a state, city, or zip code as the basis for production of information. If the government demanded the credit card transaction records of everyone in Georgia and Maine, would that not be a limit on the scope of collection, as compared to nationwide surveillance? Congress should amend "specific selection term" with negative language making clear that the definition does not include broad geographic regions such as a state, city, zip code, or area code. It should include other negative language to preclude use of other overly broad specific selection terms.

Adding the words "device" and "address" to the definition of "specific selection term" also opens up the potential for collection of large amount of Internet communications that are not related to the particular target. Some routers – which qualify as "devices" – can handle the email messages of thousands, perhaps millions, of people, so permitting collection by device identifier does not effectively limit collection to particular targets or those targets' *personal* devices. "Address" may include Internet Protocol (IP) address, yet thousands of computers and users

[15] The PCLOB labeled the telephony bulk collection program as "not statutorily authorized" for four independent reasons. *See*, PCLOB §215 Report, pgs. 57-58. "First, the telephone records acquired under this program have no connection to any specific FBI investigation at the time the government obtains them. Instead, they are collected in advance to be searched later for records that do have such a connection. Second, because the records are collected in bulk — potentially encompassing all telephone calling records across the nation — they cannot be regarded as "relevant" to any FBI investigation without redefining that word in a manner that is circular, unlimited in scope, and out of step with precedent from analogous legal contexts involving the production of records. Third, instead of compelling telephone companies to turn over records already in their possession, the program operates by placing those companies under a continuing obligation to furnish newly generated calling records on a daily basis. This is an approach lacking foundation in the statute and one that is inconsistent with FISA as a whole, because it circumvents another provision that governs (and limits) the prospective collection of the same type of information. Fourth, the statute permits only the FBI to obtain items for use in its own investigations. It does not authorize the NSA to collect anything."

may be assigned a single IP address, such as through web hosts or Network Address Translation devices. If the bill meant to limit "address" to *physical* address, then this should be made clear.

At the same time, we understand the government's legitimate need for flexibility to address a multitude of scenarios and to engage in new investigations that cannot be currently contemplated. If the USA FREEDOM Act were to prescribe a narrow and exclusive list of selection terms, this might inappropriately obstruct effective investigative techniques to address true threats. On the other hand, even the use of specific selection terms thought to be more particularized, such as "person" or "entity" may not effectively end mass collection since (for example) major corporations with millions of users are "persons" and "entities." Clear legislative history can clarify the meanings of these words to preclude unintended results. While the definition of "specific selection term" must be narrowed and clarified, Congress should also establish meaningful statutory privacy protections that go beyond the definition.

II. Enhanced Minimization Procedures

In addition to narrowing and clarifying the definition of "specific selection term," Congress should also strengthen existing minimization procedure, and establish minimization or privacy procedures where there are none. Specifically, the USA FREEDOM Act should require minimization or privacy procedures that are *reasonably designed to minimize the acquisition and prohibit the retention and dissemination, of non-public information concerning individuals who are not – based on reasonable, articulable suspicion – foreign powers, agents of foreign powers, or in direct contact with foreign powers or agents of foreign powers*. The FISC should be required to review the procedures for compliance with the statute before entering an order for the production of records. The procedures should be reviewed by an independent body, such as the Privacy and Civil Liberties Oversight Board, on a regular basis and prior to any significant change to the procedures. These procedures should be applied to the authorities for which the USA FREEDOM Act seeks to end bulk collection – Sec. 215 of the PATRIOT Act, the FISA pen/trap statute, and NSLs.

An advantage to this approach is that the procedures would be adaptable multiple scenarios, and address both front-end acquisition and back-end retention of information about individuals who are not agents of foreign powers or in contact with such. That way, the government is required to seek the means of collecting information with minimal impact on non-targets, but is also required to purge information unrelated to agents of foreign powers if acquisition of such information is unavoidable.

Another advantage to this approach is that the government has a base of experience with this framework because provisions of FISA already require minimization procedures. Section 215 of the PATRIOT Act and Sec. 702 of FISA both require more limited forms of minimization procedures that apply to the retention and dissemination of data. Section 215 requires the minimization procedures to minimize the retention and prohibit the dissemination of nonpublic information concerning U.S. persons, consistent with the need of the U.S. to produce foreign intelligence information, and prohibits dissemination of information that identifies a U.S. person

unless identification is necessary to understand foreign intelligence information.[16] Section 702 requires similar procedures, but also requires that acquisition be minimized, which we view as an essential feature.[17] The pen/trap statute and NSL authorities currently do not require any minimization procedures. What we are proposing would go further than existing minimization procedures insofar as it would 1) require minimization or privacy procedures for Sec. 215, FISA pen/trap, and NSLs, 2) require minimization of acquisition, not just retention and dissemination, 3) prohibit retention and dissemination, not just dissemination, and 4) create new criteria for acquisition, retention, and dissemination – namely, whether the information concerns a foreign power, agent of foreign power, or person in contact with such, based on reasonable, articulable suspicion.

The USA FREEDOM Act, as passed by the House, takes some very modest steps in this direction. Section 104 of the bill would alter Sec. 215 of the PATRIOT Act to require FISC review of the minimization procedures for compliance with the statutory standard prior to issuing an order, though the bill does not alter the current statutory standard for minimization procedures. Section 202 of the USA FREEDOM Act would establish new privacy procedures for the FISA pen/trap statute, which currently have no such procedures, requiring "appropriate policies" that "include protections for the collection, retention, and use" of U.S. persons' information.[18] The bill does not establish procedures for NSLs.

To be clear, strong minimization or privacy procedures should not replace a narrower, clearer definition of "specific selection term." Nor should the procedures replace other useful safeguards present in the USA FREEDOM Act, such as the panel of amicus curiae, the government transparency reporting requirements, or the requirement to declassify or publicly summarize FISC opinions that interpret "specific selection term."[19] Rather, the strengthened procedures would be a partial safeguard that should be added to the partial safeguards present in the bill. We remain open to considering other potential solutions, but believe this approach would help achieve the dual goals of protecting both privacy and flexibility.

III. In Addition to Prohibiting Bulk Collection, the USA FREEDOM Act Should Address Other Surveillance Reforms

Prohibiting large-scale collection and retention of information about individuals who are not connected to an investigation is the most critical issue the Senate must address in its consideration of the USA FREEDOM Act. However, Congress should also consider other important surveillance reforms related to Sec. 702 of FISA, private party reporting of

[16] 50 U.S.C. 1861(g)(2)(A)-(B).

[17] 50 U.S.C. 1881a(e)(1), 50 U.S.C. 1801(h)(1)-(4).

[18] Earlier iterations of the bill established minimization procedures that were virtually identical to those currently in Sec. 215. In the earlier iteration of the bill, Government applications for pen/trap were required to include a statement of minimization procedures, the FISC was able to review whether the minimization procedures meet the statutory standard, and the FISC was able to review compliance with minimization procedures involving U.S. persons. These procedures were stripped out of the bill prior to final passage in the House.

[19] H.R. 3361, as engrossed, 113th Cong., Secs. 401, 601-603, 605.

surveillance orders, and a FISC Special Advocate.

A. Section 702 of FISA

While much of the focus of this past year's debate on government surveillance has been bulk collection pursuant to Sec. 215 of the PATRIOT Act, it is also essential that Congress address Sec. 702 of FISA. Surveillance under Sec. 702 threatens the privacy rights of Americans, the human rights of those abroad, the continued growth of American tech companies,[20] and the future development of a global Internet.[21]

First, Congress should limit the scope of surveillance that is permissible under Section 702. Under current law, the government can compel U.S. tech companies to assist with surveillance of any non-U.S. person abroad in order to collect "foreign intelligence information" – a term broadly defined to include even information that is only related to U.S. foreign affairs.[22] Instead, the government should be permitted to compel such assistance only in response to significant security threats, such as those outlined in Presidential Policy Directive 28 for use of information collected in bulk. This would require that collection pursuant to Section 702 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 Armed 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.[23]

Second, Congress should close the "backdoor search loophole" that Sec. 702 surveillance has opened, a reform that was in the USA FREEDOM Act as introduced, but which was removed to final passage in the House.[24] Under Sec. 702, the NSA collects huge quantities of communications contents and metadata about both U.S. persons and non-U.S. persons – 250

---

[20] Recent studies by the Information Technology and Innovation Foundation and Forrester Research estimate that NSA surveillance will cost the U.S. tech industry between $35 billion and $180 billion over the next three years, a loss of up to 25 percent of total industry revenue. Daniel Castro, The Information Technology and Innovation Foundation, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?*, Aug. 5, 2013, *available at* http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry. James Staten, Forrester Research, *The Cost of PRSIM Will Be Larger Than ITIF Projects*, Aug. 14, 2013, available at http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

[21] NSA surveillance – notably surveillance of persons abroad conducted under Section - has fueled efforts abroad to require data to be stored locally, in particular countries. This could have enormous negative repercussions for the competitiveness of the American tech industry, the global free flow of information, and the international entrepreneurship and innovation that the Internet has engendered. *See*, Dean Garfield, *Written Testimony to the Privacy and Civil Liberties Oversight Board* Mar. 19, 2014, *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/Testimony_Garfield.pdf. "We are facing the possibility of a Balkanized Internet, and global innovation will certainly suffer. Brazil, for example, is considering a legislative proposal that could lead to the requirement that certain data be stored in that country."

[22] 50 USC Sec. 1801(e)(2)(B).

[23] Center for Democracy & Technology, Comments to PCLOB on Section 702 Reform, Apr. 11, 2014, available at https://cdt.org/insight/cdt-comments-to-pclob-on-section-702-reform.

[24] H.R. 3361, as introduced, 113th Cong., Sec. 301.

million Internet communications per year, according to a 2011 court estimate.[25] In October 2011, the minimization procedures required under Sec. 702 were changed to permit NSA personnel to query information collected under Sec. 702 using U.S. person identifiers.[26] The minimization procedures permit the NSA to retain and disseminate U.S. persons' communication if it contains foreign intelligence information[27] or if the communication contains evidence of a crime that may have been or may be committed.[28] As a result, a military intelligence agency is using a statute specifically designed to permit collection that targets non-U.S. persons abroad to amass, analyze, and share U.S. persons' communications without court approval, even though the government would have to ask the FISC for permission to directly obtain those U.S. persons' information if they were targeted directly. Congress should amend Sec. 702 to require, absent a life-threatening emergency, judicial approval to search information collected under Sec. 702 for the communications contents of U.S. persons.[29]

Third, the use of Sec. 702 to collect communications "about" surveillance targets that are neither to nor from a target should be prohibited.[30] Section 702 authorizes the government to target the communications of persons reasonably believed to be abroad, but it never defines the term "target." However, throughout Sec. 702, the term is used to refer to the targeting of an individual, rather than the content of a communication.[31] Further, the entire congressional debate on Section 702 includes no reference to collecting communications "about" a foreign target, and significant debate about collecting communications to or from a target.[32] The practice of collecting "about" communications is inconsistent with the legislative history of the statute, raises constitutional problems, and directs the focus of surveillance away from suspected wrongdoers while permitting the NSA to monitor the communications of Americans with no link to national security investigations. The USA FREEDOM Act, as approved by the House,

---

[25] Oct. 2011 FISC opinion, available at https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional.

[26] James Ball and Spencer Ackerman, *NSA loophole allows warrantless search for US citizens' emails and phone calls*, The Guardian, Aug. 9, 2013, available at http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

[27] 50 U.S.C. 1801(e) defines "Foreign intelligence information" broadly to include information "necessary to the conduct of the foreign affairs of the United Sates."

[28] National Security Agency, 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, Sec. 5, Oct. 31, 2011, http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

[29] This recommendation was echoed in the President's Review Group Report, pgs. 145-146.

[30] *See*, Statement of Brad Wiegmann, Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (March 19, 2014), available at http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf. "Why 'about' collection is different is it's not necessarily communications to or from that bad guy but instead about that selector."

[31] 50 U.S.C. 1881a(a).

[32] See, e.g., U.S. Senate Select Committee on Intelligence, FISA Sunset Extensions Act of 2012 Report (S. Rpt. 112-174, Appendix), available at http://www.gpo.gov/fdsys/pkg/CRPT-112srpt174/pdf/CRPT-112srpt174.pdf. "Section 702 permits the FISC to approve surveillance of terrorist suspects and other targets who are non-U.S. persons outside the United States.... The FISC may approve surveillance of these kinds of targets when the Government needs the assistance of an electronic communications service provider."

includes mention of "about" collection in proposed statutory language,[33] which would give this practice the seal of Congressional approval. Instead, Congress should specifically limit the scope of Sec. 702 surveillance to communications to or from a target. If the legislation does not explicitly prohibit the practice of collecting "about" communications, the reference to "about" communications should be removed.

These are some of the most important issues regarding reform of Section 702, but there are many more. While the focus of the Senate's consideration of the USA FREEDOM Act will continue to be how to effectively prohibit bulk collection, Congress should make a clear commitment to engaging in a comprehensive review of Sec. 702 in the future, and enacting reforms to address the range of problems that have come to light. The upcoming report of the Privacy and Civil liberties Oversight Board on Sec. 702 will provide Congress with a good opportunity to do so.

B. Transparency, Immunity, & FISC Reform

Congress should strengthen the transparency provisions of The USA FREEDOM Act, as passed by the House, especially those regarding company reporting of the intelligence surveillance demands they receive. Currently, the legislation provides a convoluted framework with three options.[34] The option that permits the most particularized reporting allows companies and other persons to report the number of orders received and accounts affected, in ranges of a thousand, separated by NSLs and distinct titles of FISA – except Title VII. The other two options permit reporting in ranges of 500 and 250, but doing so sacrifices the ability to distinguish which authority was used for collection and to estimate the accounts affected by surveillance demands. The ability to separate reports by legal authority is essential to effective reporting, as these different authorities permit government collection of different types of information and require different showings before an independent court. In addition, the bill's references to permitting reporting of "selectors targeted" should be replaced with reporting on accounts affected. The number of selectors targeted is not an accurate representation of the number of accounts affected since one selector can encompass multiple accounts, while bulk collection may not be reported at all since it is not selector-based.[35]

Moreover, we are also concerned about the change the bill makes to the liability provision in Sec. 215. The threat of liability for unlawfully turning over of records to an intelligence agency is a powerful incentive for private parties to protect privacy. If a company acts within the law and turns over records to the government that a Sec. 215 order requires it to provide, it should have immunity for doing so. If it proves with factual evidence subjected to the rigors of the adversarial process that it had attempted in good faith comply with the law when it turned over those records, but failed, the law should give the company a strong affirmative defense to a claim against it based on that failure. However, USA FREEDOM goes well beyond this: it removes the good faith requirement in current law and provides blanket immunity for companies that produce

[33] H.R. 3361, as engrossed by the House, Sec. 301.

[34] H.R. 3361, as engrossed by the House, Sec. 604.

[35] Harley Geiger, *Two Ways the Surveillance Transparency Rules for Companies are not Transparent*, Center for Democracy & Technology, Mar. 19, 2014, https://cdt.org/blog/two-ways-the-surveillance-transparency-rules-for-companies-are-not-transparent.

information or tangible things pursuant to a Sec. 215 order, and provides additional blanket immunity for the provision of technical assistance to the government in connection with fulfilling a Sec. 215 order. This could mean, for example, that if a company contracts with its customer to hold customer records only in encrypted form, and the company decrypted the information and turned it over to the government in response to a Sec. 215 order, the customer could bring no cause of action to enforce the contractual commitment for which it had bargained. This immunity provision, because it is overbroad, will erode trust in U.S. tech companies.

Finally, a Special Advocate should be created to participate in select FISC proceedings. Trust in the FISC has been eroded because it operates in secret and issues sweeping decisions with profound civil liberties implications in proceedings during a one-sided process in which only the government is represented. Although the USA FREEDOM Act, as passed by the House, encourages, but does not compel, amicus participation, the amicus is given no statutory charge regarding what issues to advocate, and could well argue for even broader surveillance authority than the government is seeking in the proceeding. In addition to providing for amicus participation, the USA FREEDOM Act should include a Special Advocate specifically tasked with vigorously defending privacy, civil liberties, and transparency in FISC proceedings. This would more effectively prevent unnecessarily broad surveillance, enhance the value of Court declassifications, and help restore public trust in the FISC. While concerns have been raised that such an Advocate might reduce efficiency, the USA FREEDOM Act, as introduced, alleviated this concern by giving the Court discretion over the Advocate's participation, so that an adversarial debate would precede significant interpretations of law, but routine court decision-making would proceed without such process.[36]

These additional reforms should be given thorough consideration, but they are no substitute taking bold steps to prevent bulk collection of information. Without a more effective solution to this issue, we cannot support the legislation now under consideration.

Conclusion

We appreciate the opportunity to testify before this committee and present our views on the USA FREEDOM Act and Congress' continued consideration of how best to address the complex issue of government surveillance reform. Many positive steps have been made and a significant achievement is now within your reach, but obstacles remain to effectively prevent unnecessary mass surveillance. We look forward to working with you to craft a solution that definitively prohibits mass surveillance, permits necessary surveillance, and protects the values that are so critical to our democratic society and our future.

[36] Steve Vladek, *Judge Bates and a FISA "Special Advocate,"* Lawfare, Feb. 4, 2014, http://lawfareblog.com/2014/02/judge-bates-and-a-fisa-special-advocate.