THE CONSTITUTION PROJECT
Safeguarding Liberty, Justice & the Rule of Law

April 11, 2014

Privacy and Civil Liberties Oversight Board
2100 K St. NW, Suite 500
Washington, D.C. 20427

Re: March 19, 2014 Public Hearing

Dear Chairman Medine and Board Members:

The Constitution Project (TCP) welcomes this opportunity to comment on the March 19, 2014 public hearing and to offer our views on whether the federal government's surveillance programs operated under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. § 1881a, properly balance efforts to protect the Nation with the need to protect privacy and civil liberties.

TCP is a non-profit think tank and advocacy organization that brings together unlikely allies—experts and practitioners from across the political spectrum—to develop consensus-based solutions to some of the most difficult constitutional challenges of our time. TCP's bipartisan Liberty and Security Committee, comprised of former elected officials, former members of the law enforcement and intelligence communities, as well as legal academics, practitioners and advocates, previously made recommendations for statutory amendments to add warrant requirements and increase judicial and congressional oversight of Section 702 programs. See TCP's September 2012 *Report on the FISA Amendments Act*. Liberty and Security Committee members convened following the PCLOB's March 19, 2014 hearing, discussed the witness testimony and other newly available information, and agreed to reaffirm their previous policy on Section 702, with the following additional comments and recommendations.[1]

I. The Operation of Section 702

Our comments are supported by information about the operation of Section 702 recently revealed through declassified Foreign Intelligence Surveillance Court (FISC) opinions and leaks by National Security Agency (NSA) contractor Edward Snowden. These documents have shown that NSA's mass acquisition of Internet communications under Section 702 is accomplished primarily through two programs, known as PRISM and "upstream collection."

[1] Special thanks to Hogan Lovells attorneys Christopher Wolf, Harriet Pearson, Bret Cohen, Jaclyn DiLauro, Nathan Foell, and Adam Solomon, who served as rapporteurs and pro bono counsel to TCP's Liberty and Security Committee in the preparation of these comments. Hogan Lovells did not take part in TCP's policy deliberations, and the resulting recommendations do not represent Hogan Lovells' or any of its individual attorneys' views.

PRISM, which was established in December 2007, involves the collection of live communications and stored information about non-U.S. persons located overseas from U.S.-based electronic communication service providers.[2] Of the over 250 million Internet communications acquired each year by the NSA pursuant to Section 702, the vast majority are obtained through the PRISM program.[3] While PRISM acquires data stored by service providers, upstream collection involves the acquisition of Internet communications as they travel over fiber optic cables from one data center to another.[4] Upstream collection constitutes approximately 9% of the total Internet communications acquired by NSA under Section 702.[5] But this 9% is particularly significant because it encompasses "tens of thousands of wholly domestic communications" incidentally collected by the NSA each year.[6]

The newly revealed information about PRISM and upstream collection raises significant constitutional concerns that TCP believes that the PCLOB should address: (1) incidental collection of U.S. person communications is too broad; (2) minimization procedures are inadequate to avoid capturing U.S. person communications; and (3) policies for retention, search, and use of data collected under Section 702 are inadequate to avoid capturing U.S. person communications.

Incidental collection of U.S. person communications

Although Section 702 prohibits the targeting of U.S. persons and requires the government to take steps to minimize the collection of U.S. person communications, NSA draws presumptions that err on the side of expanding the scope of its data collection, increasing the risk of incidental collection of U.S. person communications. For example, to intentionally target a person for surveillance, an NSA analyst need have only 51% confidence that the target is a foreign national.[7] And in the absence of actual knowledge as to whether a target is a U.S. person or is in the United States, NSA presumes that person to be a non-U.S. person unless the person can be positively identified as a U.S. person.[8]

Mr. De's testimony, explaining that the 51% rule is a misconception, fails to respond to the underlying concern that NSA relies on a low standard of certainty to establish foreignness. The "totality of the circumstances test" that Mr. De describes with such genuine effort at transparency unfortunately does not speak to the sufficiency of the evidence relied on. *See Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act, March 19, 2014*, http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf, at 40-42 (henceforth "Transcript").

---

[2] Nick Hopkins, *UK Gathering Secret Intelligence Via Covert NSA Operation*, THE GUARDIAN, June 7, 2013.

[3] *In re DNI/AG 702(g)*, Dkt. No. 702(i)-11-01, at 29 (Foreign Int. Surv. Ct. Oct. 3, 2011) [hereinafter FISC Op. of Oct. 3, 2011].

[4] Barton Gellman, Ashkan Soltani & Andrea Peterson, *How We Know the NSA Had Access to Internal Google and Yahoo Cloud Data*, WASH. POST, Nov. 4, 2013.

[5] FISC Op. of Oct. 3, 2011, at 29-30.

[6] *Id.* at 41.

[7] Robert O'Harrow, Jr., Ellen Nakashima & Barton Gellman, *U.S. Company Officials: Internet Surveillance Does Not Indiscriminately Mine Data*, WASH. POST, June 8, 2013.

[8] Glen Greenwald & James Ball, *The Top Secret Rules That Allow NSA to Use US Data Without a Warrant*, THE GUARDIAN, June 20, 2013.

Moreover, NSA's overly broad definition of "foreign intelligence" results in the collection of massive amounts of data with only a remote connection to the underlying foreign intelligence purpose for which collection is authorized. According to targeting procedures filed with the clerk of the FISC on July 29, 2009, NSA considers that a person's telephone number or electronic address or identifier may be targeted for a "foreign intelligence purpose" if:

(1) it has been used to communicate directly with another number/address reasonably believed by the U.S. intelligence community to be used by an individual associated with a foreign power or foreign territory;
(2) it has been used to communicate with an individual reasonably believed to be associated with a foreign power or foreign territory;
(3) it is in the directory or "buddy list" of an account reasonably believed by the U.S intelligence community to be associated with a foreign power or foreign territory;
(4) it has been transmitted during a call or communication with an individual reasonably believed by the U.S. intelligence community to be associated with a foreign power or foreign territory;
(5) publicly available information sources match the telephone number or electronic address to a person reasonably believed by the U.S. intelligence community to be associated with a foreign power or foreign territory;
(6) information in NSA databases acquired lawfully reveals that the address has been used by an individual associated with a foreign power or foreign territory;
(7) information made available to NSA analysts as a result of lawful processing of metadata reveals that phone number or address was used by an individual associated with a foreign power or territory; or
(8) information indicates that IP ranges or identifiers are extensively used by individuals associated with a foreign power or foreign territory.[9]

Indeed, merely being on the contact list of a person whom NSA suspects of being associated with a foreign government or terrorist group can result in the presumption that a person is a non-U.S. person.

Minimization procedures

Recently released documents demonstrate that Section 702's required minimization procedures have insufficiently filtered out U.S. person communications. In a declassified October 3, 2011 opinion, the FISC held that NSA's proposed minimization procedures for upstream collection were inadequate when sampling revealed that NSA likely acquired tens of thousands of wholly domestic communications annually, and tens of thousands of communications of persons who had

[9] NAT'L SEC. AGENCY, 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, Exh. A (2007) (filed with FISC July 29, 2009), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf.

little or no relationship to the target but who were protected under the Fourth Amendment.[10] In addition, the court expressed concern that thousands of wholly domestic communications would be retained for at least five years "despite the fact that they have no direct connection to a targeted selector and, therefore, are unlikely to contain foreign intelligence information."[11]

In response, the government amended and the FISC accepted the minimization procedures to require (1) the post-acquisition segregation of those types of transactions that are most likely to contain non-target information concerning a United States person or persons in the United States; (2) special handling and marking requirements for transactions that have been removed from or that are not subject to segregation; and (3) a two-year default retention period for all upstream acquisitions.[12] Recently released documents, however, demonstrate that these measures are still not being implemented in a manner consistent with NSA's Fourth Amendment obligations.

In August 2013, the Attorney General and Director of National Intelligence declassified a heavily redacted semiannual assessment of compliance with its minimization obligations that detailed a number of compliance incidents.[13] These included tasking issues (related to initiating collection), detasking issues (related to how NSA aborts its efforts when a collection is deemed illegal or unnecessary), notification delays where minimization is required, documentation issues, and over-collection.[14] For example, U.S. persons have been affected by errors that led to the tasking of telephone lines or computers used by U.S. persons, delays in detasking telephone lines or computers after NSA determined that the user of the selector was a U.S. person, and the unintentional querying of Section 702 repositories using a U.S. person identifier.[15] In one instance, an email account remained on collection for five weeks after its user had been discovered to have traveled to the United States because the analyst had detasked only some of the telephone lines or computers used by this individual.[16]

Moreover, although the 2011 NSA minimization procedures note that collection must be stopped if signals intelligence is acquired on a U.S. person (in most instances), a document dated November 1, 2011 and leaked by Snowden explains that incidentally obtained information about a U.S. person does not require that collection be stopped immediately.[17] Rather, the analyst must only apply USSID minimization procedures, which allow for the retention of U.S. person

---

[10] FISC Op. of Oct. 3, 2011, at 29.

[11] *Id.* at 61.

[12] *In re DNI/AG 702(g)*, Dkt. No. 702(i)-11-01 (Foreign Int. Surv. Ct. Nov. 30, 2011) [hereinafter FISC Op. of Nov. 30, 2011].

[13] U.S. DEP'T OF JUSTICE & OFFICE OF THE DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE, REPORTING PERIOD: JUNE 1, 2012 – NOVEMBER 30, 2012 (2013), *available at* http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

[14] *Id.* at 25.

[15] *Id.* at 28.

[16] *Id.* at 33.

[17] *See* NAT'L SEC. AGENCY, LESSON 4: SO YOU GOT U.S. PERSON INFORMATION?, OVSC1400, Dual Authorities (SIGINT/IA) Online Training Job Aid (2011), *available at* http://apps.washingtonpost.com/g/page/national/whats-a-violation/391.

communications "if necessary for the maintenance of technical databases" and "focus" on the foreign end of the communication.[18]

Policies for retention, search, and use of data

Recent disclosures relating to NSA's retention and use of data also raise constitutional concerns. For example, "contact chaining" allows NSA analysts to connect one information source to another in analyzing collected data.[19] Prior to 2010, analysts were required to stop chaining if they discovered a U.S. person's contact identifier.[20] That process changed in 2010, allowing contact chaining even through U.S. person contacts and expanding NSA's ability to establish communications networks.[21] In November 2010, NSA Signals Intelligence (SIGINT) signed a directive permitting contact chaining from and through any selector, irrespective of nationality or location, to follow or discover valid foreign intelligence targets.[22] This directive allowed communications metadata collected under Executive Order 12333 to be "fully exploited," allowing tracking of connections between foreign intelligence targets and second-party or U.S. person connections as well as large-scale graphing analysis of very large sets of communications metadata "without having to check foreignness of every node or address in the graph."[23]

XKeyscore is NSA's search engine, which "allows analysts to search with no prior authorization through vast databases containing emails, online chats and the browsing histories of millions of individuals."[24] Analysts can use XKeyscore to "mine enormous agency databases by filling in a simple on-screen form giving only a broad justification for the search."[25] A request is not reviewed by a court or any NSA personnel before processing.[26] Analysts can use XKeyscore and other NSA systems to acquire ongoing, "real-time" interception of an individual's internet activity.[27] XKeyscore provides the technical capacity to target U.S. persons for extensive electronic surveillance without a warrant, so long as some identifying information (email, IP address) is known to the analyst.[28]

DNI Presenter, another NSA tool, allows analysts to read the content of stored emails, Facebook chats, or private messages.[29] NSA slides indicate that analysts can have access to "nearly

---

[18] *See id.*; NAT'L SEC. AGENCY, USSID SP0018: LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES § 6(a)(1) (2011), *available at* http://www.dni.gov/files/documents/1118/CLEANEDFinal%20USSID%20SP0018.pdf.

[19] NAT'L SEC. AGENCY, NEW CONTACT-CHAINING PROCEDURES TO ALLOW BETTER, FASTER ANALYSIS (2011), *available at* http://www.nytimes.com/interactive/2013/09/29/us/documents-on-nsa-efforts-to-diagram-social-networks-of-us-citizens.html.

[20] James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, Sept. 28, 2013.

[21] *Id.*

[22] *Id.*

[23] NAT'L SEC. AGENCY, NEW CONTACT-CHAINING PROCEDURES, *supra, n. 19.*

[24] Glenn Greenwald, *XKeyscore: NSA tool collects 'nearly everything a user does on the internet'*, THE GUARDIAN, July 31, 2013.

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

everything a typical user does on the internet."[30] An analyst can "work backward" from a specified website to determine the IP addresses of every person who has visited that site.[31] An NSA report from 2007 indicates that there were 850 billion "call events" collected and stored in NSA databases and close to 150 billion internet records, with one to two billion records added every day.[32] Analysts can store "interesting" content for a longer period in other databases, such as Pinwale, which can store data for up to five years.[33] In 2012, there were at least 41 billion total records collected and stored in XKeyscore for a single 30-day period.[34] Although NSA has attempted, in recent years, to segregate exclusively domestic U.S. communications in separate databases, some of those communications travel on foreign systems and are not swept up in these efforts.[35]

II. Protection of Constitutional Rights and Interests

The Fourth Amendment protects the "right of the people to be secure . . . against unreasonable searches and seizures."[36] Warrantless searches are "per se unreasonable under the Fourth Amendment"—subject only to a few specifically established and well-delineated exceptions.[37]

But even when a search or seizure is covered by one of the carefully circumscribed exceptions to the warrant requirement, it still must be constrained by privacy protections sufficient to "alleviate the risks of government error and abuse."[38] Section 702 intelligence gathering lacks such constraints on both its "front end"—concerning the acquisition and retention of private communications—and its "back end"—concerning the search and use of private communications once acquired. Because Section 702 intelligence gathering lacks privacy protections sufficient to alleviate the risks of government error and abuse, it is unsound under the Fourth Amendment.

The scope of U.S. person data collected incidentally during the front-end acquisition and retention of private communications under Section 702 is so vast that it raises the same constitutional concerns as other government programs that collect intelligence in bulk. The obvious parallel is the bulk telephone records program operated by the NSA under Section 215 of the USA PATRIOT Act (the Bulk Telephony Metadata Program), which this Board and one recent court to consider the issue have found to raise constitutional issues.[39] Under both Section 215 and Section 702, the government collects large amounts of personal, sensitive data without particularized suspicion from large numbers of individuals. It follows, then, that the significant collection of U.S.

---

[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*
[34] *Id.*
[35] *Id.*
[36] U.S. CONST. amend. IV.
[37] *Katz v. United States*, 389 U.S. 347, 357 (1967).
[38] *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (Foreign Int. Surv. Ct. Rev. 2008).
[39] *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 2015 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT 103-36 (2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf; *Klayman v. Obama*, No. CV 13-0881 (RJL), 2013 WL 6598728 (D.D.C. Dec. 16, 2013).

person data incidental to the collection of the data of non-U.S. persons ostensibly targeted under Section 702 raises constitutional concerns.

The government essentially takes the position that if it is blind as to whether data collected at the front end is that of a U.S. person, it is constitutionally permitted to search that data on the back end, and it does so on a mass scale that significantly intrudes upon the privacy interests of U.S. persons. When it appears before the Foreign Intelligence Surveillance Court (FISC), the government does not identify individuals as foreign intelligence targets under Section 702. Instead, it identifies "certain *categories* of foreign intelligence targets whose communications may be collected, subject to FISC-approved targeting and minimization procedures."[40] Then, the "determination of which *individuals* to target pursuant to these FISC-approved certifications is made by NSA without any additional FISC approval."[41] This means that judicial review of the "more than two hundred fifty million Internet communications" NSA acquires each year under Section 702 is confined to approving broad categories of targets for collection,[42] like "international terrorists and individuals involved in the proliferation of weapons of mass destruction."[43] Permitting the search of these communications on the back end provides the government with a dangerous incentive to maximize the incidental collection of communications on the front end. Recent revelations appear to indicate that the government takes this opportunity by employing presumptions that err in favor of designating a particular individual a non-U.S. person, such as its collection of data from persons for whom it has only 51% confidence is a foreign national.[44]

Given the government's use of broad presumptions and the generality of judicial review of Section 702 intelligence gathering, it is no surprise that under Section 702 the NSA annually acquires "tens of thousands of wholly domestic communications."[45] These communications "are among the four items that are specifically listed in the Fourth Amendment as subject to protection against unreasonable search and seizure."[46] Not only are these constitutionally protected communications swept into Section 702's wide net; but the government also asserts the right to retain them for years despite their constitutionally protected status. Even under the most stringent set of minimization procedures that have been publicized, the government is still allowed to retain private communications collected under Section 702 for two years.[47]

All of these characteristics of Section 702 intelligence gathering demonstrate that incidental collection raises the same concerns as bulk collection—regardless of how the government defines bulk collection so as to distinguish them.[48] One judge has already struck down the bulk collection of

---

[40] PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 135-36 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.
[41] *Id.* at 136.
[42] FISC Op. of Oct. 3, 2011, at 29.
[43] PRESIDENT'S REVIEW GROUP, *supra, n. 40* at 136.
[44] Robert O'Harrow, Jr., Ellen Nakashima & Barton Gellman, *supra, n. 7*.
[45] FISC Op. of Oct. 3, 2011, at 41.
[46] *Id.*, at 73.
[47] *See* FISC Op. of Nov. 30, 2011, at 7.
[48] *See* Mr. Litt's opening statement, Transcript at 10, insisting that Section 702 "is not bulk collection"; *see* Presidential Policy Directive 28: Signals Intelligence Activities (Jan. 17, 2014) (henceforth "PPD-28") at n. 5, distinguishing data "temporarily acquired to facilitate targeted collection" from the definition of "bulk" collection. It is somewhat puzzling that the government defines incidentally collected data, even when retained for several years, as "temporarily acquired."

telephony metadata under Section 215 of the Patriot Act because the program involved "almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States."[49] Intelligence gathering under Section 702 strikes just as close to the heart of the Fourth Amendment prohibition against warrantless searches. Incidental collection under Section 702 is just as expansive in its breadth and intrusive in its effects as bulk collection. And regardless of how one compares the revelations made available by metadata or by content, certainly when both types of data are acquired and analyzed, the "nature of the government intrusion" calls for particularly powerful protections to "alleviate the risks of government error and abuse."[50]

In addition, the back-end *search and use* of private communications under Section 702 is constitutionally suspect because it, too, resembles the same troublesome business records programs that acquire intelligence in bulk. The collection of telephony metadata under Section 215 involved the "collection *and retention* of personal data on virtually every single citizen for purposes of *querying and analyzing it* without prior judicial approval."[51] Similarly, the government has asserted before this Board that it need not seek prior judicial approval before searching and using intelligence gathered under Section 702, even when that intelligence consists of private communications only incidentally collected by Section 702's wide net. (*See, e.g.*, Transcript at 27-28). This aggressive assertion of government power is particularly troubling given the massive scope of data collection and the ease with which it is collected and retained using advanced technology available to the government.

Where incidentally collected, constitutionally protected communications are concerned, the government's adoption of massive databases and sophisticated search tools such as XKeyscore discredits the simplistic view that whatever the government collects it should be able to search and use without limit. The least the government should do to protect the privacy of U.S. persons whose communications are collected solely because the government has chosen to gather intelligence in bulk, or through the use of broad filters, is to purge those communications once they are detected in its databases. If, instead, the government can search and use intelligence collected under Section 702 without significant limit, law enforcement will face a strong temptation to "use Section 702 in an effort to gather evidence against United States persons in a way that would circumvent the underlying values of both FISA and the Fourth Amendment."[52]

In sum, there are principled reasons to insist upon front-end limitations on Section 702 intelligence gathering as well as stringent limitations to back-end review of the data. But the most basic point to be made about Section 702 intelligence gathering is that it does not include privacy protections sufficient to "alleviate the risks of government error and abuse."[53] The precise limitations that need to be imposed on Section 702 intelligence gathering for the sake of constitutional values will need to be crafted, with robust leadership from the PCLOB, in an ongoing dialogue among government officials and congressional policymakers, courts, and citizen advocates. What follows is The Constitution Project's contribution to that dialogue.

---

[49] *Klayman*, at *20.
[50] *In re Directives*, *supra n. 38* at 1012.
[51] *Klayman*, at *64 (emphasis added).
[52] PRESIDENT'S REVIEW GROUP, *supra n. 40* at 150.
[53] *In re Directives*, *supra n. 38* at 1012.

III. TCP's Recommendations

Collection

TCP proposes that when U.S. persons are likely to be parties to the communications collected, the list of permissible collection purposes should be narrowed. When targeting foreseeably involves collection of U.S. person data, the government should collect only intelligence related to the most severe national security risks—such as acts of terrorism; development, possession, proliferation or use of weapons of mass destruction; or other risks of death or serious bodily injury.

Narrowing the definition of "foreign intelligence information" in the context of Section 702 would be one way to accomplish this goal of reining in over-collection of U.S. person information (and, indeed, of non-U.S. person information as well). Just as the president has committed to six purpose restrictions for the *use* of data collected in bulk, the PCLOB could recommend similar purpose restrictions for the *collection* of data defined as non-bulk.[54] However, TCP would caution against legislative or regulatory reforms of the scope of 702 collection that adopt the exact limits set forth in PPD-28 at Section 2. Certainly, not all cybersecurity threats or transnational crimes (the fourth and sixth purpose limitations in Section 2) reach the standard of risk of serious bodily injury. Whereas other purposes not enumerated in Section 2, such as internal or international armed conflicts, or public health emergencies that threaten the security and stability of the United States or other nations, do meet the standard of severe risk.

Retention

PCLOB should seek to ensure that the government purges any US person information on detection unless it has the type of foreign intelligence value that could prevent serious bodily harm. TCP's Liberty and Security Committee members recommend adopting the President's Review Group's Recommendation 12 (1),[55] and urge the PCLOB to reinforce the Review Group's position. In addition, the PCLOB should recommend policies and guidelines for purging of the data of non-U.S. persons so as to protect the privacy of foreigners who are not legitimate targets of investigations.

Queries of the Data

The Government must not query 702 acquisitions to identify communications of a particular U.S. person without 1) a warrant for probable cause to believe that the US person is planning or engaged in acts of international terrorism, or 2) evidence of the need to prevent imminent serious bodily harm (to be submitted for judicial review at the earliest opportunity). Again, TCP's Liberty and Security Committee members recommend adopting the President's Review Group's Recommendation 12 (3),[56] and urge the PCLOB to reinforce the Review Group's position.

---

[54] *See* PPD-28, at Section 2, enumerating six limitations on the use of signals intelligence collected in bulk; *see supra,* n.48, discussing PPD-28 at note 5, excluding incidental collection under Section 702 from the definition of "bulk" collection.
[55] PRESIDENT'S REVIEW GROUP, *supra, n. 40* at 146.
[56] *Id*.

The government maintains that if the Constitution permits the acquisition of electronic data without a warrant, it follows that the government must also be permitted to search that data to identify individuals and analyze their communications without a warrant.[57] Indeed, Mr. Wiegman testified that he could think of no other "contexts . . . in which a warrant is required to search information already in [the government's] custody." Transcript at 28. TCP has long argued to the contrary. Surveillance technologies with far-ranging scope and capabilities may be lawfully operated without a warrant while collecting data on numerous individuals indiscriminately, or incidentally. But once the government seeks to review the data to identify, track, or investigate particular individuals or groups of individuals with constitutional rights, a warrant is required. *See* TCP's 2007 Guidelines for Public Video Surveillance, pp. 27-28. The lawful "incidental" interception of electronic communications under Section 702 becomes an unlawful search if, and when, the government proceeds, without a warrant, to focus in on specific U.S. persons. As Judge Wald indicated, the government's protests against operational burdens or inconvenience to the agencies and the FISA Court do nothing to save the constitutionality of warrantless querying of U.S. person data. Transcript at 49.

Use

No Section 702-derived information that was obtained without a warrant should be permitted to be introduced or used in *any* proceeding against a U.S. person. Once again, we recommend adopting the President's Review Group's Recommendation 12 (2),[58] but urge the PCLOB to clarify that "any proceeding" must include any agency action, whether military or civil, such as addition to a no-fly list or other watch list; denial of a license; or other deprivations of life, liberty or property that do not necessarily involve or lead to legal proceedings.

Constitutional Principles and the Rights of Non-U.S. Persons

TCP supports extending PLCOB's oversight mandate to include the conduct of all foreign intelligence activities. However, TCP believes that the Board is now fully empowered under its current mandate to consider the effect of 702 programs on the rights of non U.S. persons—both as a matter of treaty obligation and constitutional principle.

Our constitutional safeguards enshrine universal aspirations to be free from oppressive government. They should not be wielded to create an elite level of protection for U.S. persons or to serve as a wedge between us and our allies. When we invoke the Bill of Rights to champion U.S. persons only, or to export disparate impacts, we seriously weaken the significance of our founding charter in the eyes of the world and weaken our government's ability to confront abuses elsewhere.[59]

---

[57] *See, e.g.*, Mr. Wiegmann's testimony, Transcript at 27-28: "Once you've lawfully collected that information, subsequently querying that information isn't a search under the Fourth Amendment, it's information already in the government's custody."

[58] *Id.*

[59] *See* Freedom House's *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*, Oct. 3, 2013, avail. at http://freedomhouse.org/sites/default/files/resources/FOTN%202013_Full%20Report_0.pdf, documenting the decline of internet freedom worldwide for the third year in a row. Numerous governments impose violent retribution

We urge the PCLOB not to seek to harmonize our government's conduct with that of other nations at sub-constitutional standards. Rather, we should be the standard bearer and export our constitutional principles of limited government, including the principles of privacy and due process, whenever possible.

TCP urges the PCLOB to recommend conforming U.S. conduct overseas to constitutional principles to the greatest extent possible. And we believe that foreign agencies acting on behalf of, or in conjunction with the U.S., must comply with the Constitution as well.

Secret Law and Secret Programs

The president committed to increased transparency and oversight of foreign intelligence surveillance activities, both in PPD-28 and in the December 2013 Open Government Partnership National Action Plan. Needless to say, the operation of secret law to justify secret programs belies the president's commitments.

Indeed, secret law has no place in a democracy. It operates in direct violation of the core constitutional principles of government by the people and separation of powers. As the exposure of the Section 215 telephony metadata program has demonstrated, Congress and the FISA Court were unable to provide adequate checks on the executive without the public's scrutiny of the program and its legal framework as well. Where public acknowledgement of the very existence of a surveillance program is forbidden, the risk that the program violates privacy, due process, and free speech is necessarily exacerbated, and there can be no redress for those violations as long as the program remains secret.

Given the importance of the problem, the President's Review Group's Recommendation 11 regarding secret law was disappointing.[60] We urge the PCLOB to take any opportunity presented by its review of Section 702 programs to challenge the Review Group's view that executive officials may unilaterally determine the legality and appropriateness of clandestine activities. TCP is relying on the PCLOB to investigate and report, to the greatest extent possible, on all aspects of the programs operating under the actual or putative authority of Section 702. We trust that the PCLOB will not review and tacitly approve executive branch law-making, policies, or activities that far exceed Congressional authorization or public knowledge.

We urge the PCLOB to ensure that the government provides more periodic reporting to Congress and to the public on such statistics as the total number of targets affected by Section 702 surveillance; the total number of non-targeted persons affected; the number of communications purged, and the number of communications retained, searched, shared, and used. We urge the PCLOB to seek declassification, redacted only as necessary, of all FISC opinions or orders authorizing the current surveillance programs under 702, whether or not they include statutory or constitutional analysis, but certainly those opinions at a minimum. And we urge the PCLOB to seek increased analysis and reporting to the FISC of the success of the program in protecting the Nation

---

and prolonged detention for acts of free expression online. The cost of unrestrained U.S. surveillance overseas includes the loss of our ability to confront these abuses.

[60] *See* PRESIDENT'S REVIEW GROUP, *supra n. 40* at 28 and 124.

from severe threats, as well as the success of the government's minimization procedures in protecting unsuspected persons' data from warrantless review.

Thank you for the opportunity to submit these comments. The Constitution Project congratulates the Board and PCLOB staff on your work so far. We look forward eagerly to your next report, and we hope that you bring to your study of Section 702 the same depth of legal analysis and the same exigent calls for reform that you provided in your first report.

Sincerely,

Katherine E. Stern
Senior Counsel,
The Constitution Project