COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION REGARDING SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE AMENDMENTS ACT TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD[1]

Introduction

The Electronic Frontier Foundation ("EFF") is a membership-supported organization based in San Francisco, California. We fight for privacy and civil liberties in the courts, in Congress, and through public activism. The EFF is at the forefront of litigation in the United States challenging the legality and constitutionality of the National Security Agency's ("NSA") surveillance programs, including challenges to the mass collection of telephone records and the bulk collection of communications and communications records from access to fiber-optic cables inside the United States beginning in early 2006.[2] In addition, blending the expertise of lawyers, policy analysts, technologists, and activists, we educate policymakers, the press, and concerned citizens.

EFF's comments focus on the mass spying purportedly conducted under Section 702 of the FISA Amendments Act of 2008 (FAA),[3] which we understand to be the current basis upon which the government claims it may

[1] The views expressed in these comments are those of EFF as an organization and not of EFF's clients.
[2] *See generally* Electronic Frontier Foundation, "*NSA Spying on Americans*," https://www.eff.org/nsa-spying.
[3] 50 U.S.C. § 1881a.

engage in mass collection of communications from fiber-optic cables. Publicly disclosed surveillance programs ostensibly authorized under Section 702 are unconstitutional as the modern-day equivalent of "general warrants". EFF contends that Section 702 does not on its face authorize bulk collection; violates the warrant requirement of the Fourth Amendment, and that simply targeting non-U.S. persons outside the United States cannot eliminate the Fourth Amendment rights of U.S. persons. Accordingly, we urge the PCLOB to:

1) Work with the NSA and Department of Justice ("DOJ") to disclose many of the unknown items concerning Section 702, the PRISM program, and "upstream" collection while protecting only the highest national security interests. This includes the number of orders sent and the number of U.S. person communications collected. It also includes technical aspects, procedures, and processes of PRISM and "upstream collection," sufficient to allow Americans to understand whether and how their non-suspect communications are being collected and analyzed.

2) Perform a diligent statutory and Constitutional analysis similar to the analysis in the PCLOB's report on the collection of Americans' calling records using Section 215 of the Patriot Act. In such a review, we urge the board to find that Section 702 is being used to authorize modern-day general warrants. The founders specifically rejected the so-called "hated writs" on the grounds, among others, that they did not require judicial approval, particularity and a finding or probable cause prior to seizure. They would not have taken a different position had the "writs" allowed British courts to approve only general "targeting procedures" and "minimization procedures" that then allowed the British authorities to collect any (or all) colonists' personal papers and specifically target a particular colonist with no additional judicial review and subject only to general "minimization procedures" rather than specific approval of what items were seized or searched. The complexity of the procedures simply cannot hide the underlying general seizure.

3) Perform a diligent analysis of our international commitments and responsibilities concerning surveillance and the right to privacy. Mass surveillance under Section 702 is not only bad public policy, but also violates international commitments like the International Covenant on Civil and Political Rights ("ICCPR") and international law and human rights law more generally.

4) Recommend legislative fixes to, or repeal of, Section 702 of the Foreign Intelligence Surveillance Amendments Act.

Overview of Known Collection programs Using Section 702 of the FISA Amendments Act: "PRISM," "Upstream," and Others

In June 2013, the public began to learn about how Section 702 is being used for mass spying to collect U.S. persons and non-U.S. persons' communications and to protect against computer network attacks. An October 3, 2011 FISA Court order ("Bates Opinion") noted that the NSA collects more than 250 million communications annually under Section 702.[4] The NSA's "upstream"[5] collection alone acquired 13.25 million "Internet transactions" from January 1, 2011 to June 30, 2011.[6] Since the law's passage in 2008, surveillance at this rate would account for the collection of over 1.5 billion Internet communications. As of April 5, 2013, there were 117,675 targets in the government's PRISM database alone.[7]

The mechanics of Section 702 are relatively simple. The Attorney General and the Director of National Intelligence ("DNI") jointly "authorize," for a period

---

[4] Pg. 29, Memorandum Opinion of October 3, 2011 by the Foreign Intelligence Surveillance Court ("Bates Opinion"). https://www.eff.org/document/october-3-2011-fisc-opinion-holding-nsa-surveillance-unconstitutional. Last accessed April 8, 2014.
[5] The Bates Opinion defines "upstream collection" on page 5 as referring "to NSA's interception of Internet communications as they transit [redacted], rather than to acquisitions directly from Internet service providers such as [redacted]," which presumably refers to PRISM collection).
[6] *Id.*, at 30.
[7] *"NSA slides explain the PRISM data collection program."* Washington Post, June 6, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Last accessed April 8, 2014.

of up to one year[8], the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[9] There are seemingly clear limits: The government may not target individuals located within the United States[10]; it may not "reverse target"[11]; it may not intentionally target U.S. persons located abroad[12]; and it may not intentionally acquire wholly domestic communications.[13] Outside of these prohibitions, however, the government has broad discretion to conduct its surveillance program.

Crucially, the FISA Court has little involvement in this process; it merely approves or disapproves of the broad contours under which the government's FAA surveillance will operate during the upcoming year by reviewing a "certification" submitted by the Attorney General and DNI as to compliance with the statute. The surveillance must include proposed "targeting procedures" that describe groups of people, countries, or topics from or about which the government wishes to collect communications,[14] and must include "minimization procedures,"[15] which are procedures for how and when collected

[8] Section 702 does not reasonably limit surveillance duration. By contrast, the Wiretap Act authorizes surveillance for 30 days, with the opportunity for the government to apply for extensions. 18 U.S.C. § 2518(5). Even the portions of FISA authorizing specific, particularized electronic surveillance are generally limited to 90 or 120 days. 50 U.S.C. § 1805(d)(1).
[9] 50 U.S.C. § 1881a(a)
[10] *Id.,* § 1881a(b)(1).
[11] *Id.,* § 1881a(b)(2). Reverse targeting refers to the practice of intentionally conducting surveillance on a particular foreign target as a pretext for surveilling a particular, known U.S. person.
[12] *Id.,* § 1881a(b)(3)
[13] *Id.,* § 1881a(b)(4)
[14] 50 U.S.C. § 1881a(d)
[15] 50 U.S.C. § 1881a(e)

communications can be retained, used or shared.[16] The Attorney General and DNI are responsible for both sets of procedures.

FISA Court approval of such certifications results in an "order" allowing surveillance pursuant to the approved targeting and minimization procedures, which effectively ends FISA Court involvement.[17] The FISA Court never authorizes surveillance on individual targets or approves the facility, places, or premises where the surveillance will occur.[18] Conversely, the government need never present to the FISA Court facts that any specific target is abroad, is likely to send or receive foreign intelligence information, or is involved in terrorism or criminal activity. The FISA Court's only additional involvement is to review petitions by companies if they challenge the broad surveillance directives issued by the government.[19]

Instead, once the FISA Court has approved the procedures, the Attorney General and DNI have general, programmatic authority to target persons reasonably believed to be outside the United States to acquire foreign intelligence information—including the power to issue directives compelling electronic communication service providers to obtain communications and other data information[20] to, from, or about "selector(s)."[21]

---

[16] 50 U.S.C 1881a(g)(2)
[17] *See In re Proceedings Required by § 702(I) of the FISA Amendments Act of 2008*, No. Misc. 08-01, 2008 WL 9487946, at *2 (Foreign Intel. Surv. Ct. Aug. 27, 2008) (noting the court's role is "narrowly circumscribed"); *see also* 50 U.S.C. § 1881a(a).
[18] 50 U.S.C. § 1881a(g)(4)
[19] 50 U.S.C. § 1881a(h)
[20] 50 U.S.C. § 1881a(h)(1)
[21] Selectors may not be exclusive to email address, phone calls, or other personally identifiable terms. Selectors are also called "targets" or "targeting selectors." In a March 19, 2014 PCLOB hearing, NSA General Counsel Rajesh De testified in front of the Board that upstream collection

U.S. persons' information, both communications content and non-content, can then be acquired and subject to further scrutiny and review. Once a person "reasonably believed" to be outside the United States is "targeted" for acquisition, protections for any U.S. person who communicates with or "about" her generally fall away. In other words, once a "foreign" target is established, in the government's view it may then acquire any communication to, from, or even "about" that target regardless of the participation in or impact on U.S. persons in those communications.[22]

Much of this expansive surveillance inheres in the broad purpose of acquiring "foreign intelligence information," which is any "information that relates to" the national defense, terrorism, sabotage, or even "the foreign affairs of the United States."[23] Thus, the acquisition need not be tied to terrorism or to any specific suspect or event. Media reports show that the government believes acquisition of foreign intelligence information justifies the tracking of smugglers and drug traffickers, as well as, for example, persons related to Brazilian oil companies,[24] UNICEF, the Swedish manufacturer

---

is not collection "based on key words." *See* Pg. 26, Privacy and Civil Liberties Oversight Board, March 19, 2014 Public Hearing ("PCLOB Hearing"). https://web.archive.org/web/20140406215418/http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf. We urge the PCLOB to determine if operational code names or selectors that are not-personally identifiable information can be considered "key words." In short, what is the NSA's definition of "key word?"

[22] 2009 Targeting Procedures, at 1 (noting interception allowed where "NSA seeks to acquire communications about the target that are not to or from the target").

[23] 50 U.S.C. § 1801(e)

[24] Watts, Jonathan. "*NSA Accused of spying on Brazilian oil company Petrobras.*" Guardian, Sep. 9, 2013. http://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras.

Ericsson,[25] and the Institute of Physics at the Hebrew University of Jerusalem.[26] Statutory minimization requirements allow for acquisitions to include any and all information related to "foreign intelligence"[27] and authorize the government to retain and disseminate evidence of a crime.[28] The 2011 minimization procedures also generally authorize retention of any communications that are encrypted or reasonably believed to contain secret meaning.[29] .

PRISM

On June 6, 2013, the *Washington Post* revealed slides detailing a program conducted by the Special Source Operations unit in the NSA called "PRISM."[30] Publicly available information indicates that PRISM directives compel electronic communication service providers to turn over data such as voice communications, email, video, chat messages, stored data, file transfers, VoIP calls, and other "digital network information,"[31] and also allow the NSA to obtain real-time notification of selector log-ins, sent email messages, and sent instant messages.[32] As shown in the "Introducing the Program" slide, PRISM relies greatly on the fact that much of the world's Internet traffic travels through U.S.

---

[25] Gellman, Barton. "*NSA broke privacy rules thousands of times per year, audit finds*" Washington Post, Aug. 15, 2013. http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_print.html.

[26] Glanz, James; and, Lehren, Andrew W. "*NSA Spied on Allies, Aid Groups and Businesses*." N.Y. Times, Dec. 20 2013. http://www.nytimes.com/2013/12/21/world/nsa-dragnet-included-allies-aid-groups-and-business-elite.html.

[27] 50 U.S.C. § 1801(h) ("consistent with the need to obtain, produce, and disseminate foreign intelligence information").

[28] 50 U.S.C. § 1801(h)(3).

[29] Fill cite?

[30] *"NSA slides explain the PRISM data collection program."* Washington Post, June 6, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Last accessed April 8, 2014.

[31] *Ibid*.

[32] *Ibid*.

companies.[33] Companies participating in the program include Microsoft, Yahoo!, Google, Facebook, YouTube, Skype, AOL, and Apple.[34]

Upstream

The *Washington Post* documents and declassified FISA Court opinions also mention "upstream" collection, which refers "to NSA's interception of Internet communications as they transit [redacted]."[35] Like PRISM, "upstream" collection also involves compelling providers to work with NSA to copy, scan, and filter Internet and phone traffic coming through their physical infrastructure.[36]

Part of upstream collection involves the collection of "Internet transactions," including "single communications transactions" and "multiple communications transactions."[37] "Internet transactions" are defined as "a complement of 'packets' traversing the Internet that together may be understood by a device on the Internet and, where applicable, rendered in an intelligible form to the user of that device."[38] "Multiple discrete communications" involve the capture of more than one "internet transaction," which may contain multiple communications.[39] Since 2006, EFF has been litigating against this and other types of illegal and unconstitutional bulk collection. In 2011, the Bates Opinion found that some aspects of "upstream" collection were illegal and unconstitutional.

---

[33] *Ibid*. *See* "Introducing the Program" slide.
[34] *Ibid*.
[35] See fn. 5.
[36] *"NSA slides explain the PRISM data collection program."* Washington Post, June 6, 2013. http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/. Last accessed April 8, 2014.
[37] *See* Pg. 27-28, Bates Opinion.
[38] *See* Pg. 28, footnote 23, Bates Opinion.
[39] *See* Pg. 20 and Pg. 31, Bates Opinion.

More Information is Needed

While some aspects of these collection programs and their legal justifications are public, as noted above, far too much remains unknown about PRISM and upstream collection and too much of the public information is scattered and fragmented. Assembling these pieces is both difficult and uncertain. The PCLOB must help the public put together and understand the information that has been publicly released to allow a national debate on the permitted scope of surveillance affecting Americans and people around the world.

For instance, while the government has said it "touches" only 1.6% of the Internet, the public does not know how many wholly domestic communications are obtained through either program, or how many communications involving a U.S. person are collected.[40] We do not even know what "touches" means or the parameters by which the government arrived at this assertion. The public also doesn't know how many exact orders the government sends to companies demanding information, or the exact number of accounts affected.

We do know that auditing reports maintained by NSA, DOJ, and any other agency collecting, receiving, or analyzing U.S. person information obtained using Section 702 exist.[41] One such report is a quarterly report to the President's

---

[40] Jarvis, Jeff. *"How much data the NSA really gets."* Guardian, August 13, 2013. http://www.theguardian.com/commentisfree/2013/aug/13/nsa-internet-traffic-surveillance. Last accessed April 8, 2014.

[41] *See* mention of "OGC Reports" in *"Discovery SIGINT Targeting Scenarios and Compliance,"* NSA Internal Wiki. https://web.archive.org/web/20140322024357/http://www.documentcloud.org/documents/1019062-discovery-sigint-targeting-scenarios-and.html. Last accessed April 8, 2014. *See also*, "Boundless Informant" tool used by NSA analysts.

Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight, which includes "details about noncompliance incidents."[42] Also, an annual report to the Attorney General includes:

> (i) the kinds of information that NSA is collecting and processing as communications metadata;
> (ii) NSA's implementation of the Supplemental Procedures Concerning Metadata Analysis procedures; and,
> (iii) any significant new legal or oversight issues that have arisen in connection with NSA's collection, processing or dissemination of communications metadata of U.S. persons.[43]

Other types of auditing programs include software like "Boundless Informant."[44] The PCLOB must investigate these numbers and demand they be declassified to inform the public.

The statute is supposed to provide nominal protections for U.S. persons through targeting procedures and minimization requirements. Targeting procedures, which are updated every year, have never been officially released to the public in redacted form.[45] In June, the *Guardian* released the 2009 targeting procedures to the public.[46] The PCLOB must push for all versions of the

---

[42] Pg. 2, 9 and 13, Senate Committee on the Judiciary, Continued Oversight of the Foreign Intelligence Surveillance Act, October 2, 2013. Questions for the Record for General Keith B. Alexander. https://web.archive.org/web/20140406215052/http://www.judiciary.senate.gov/imo/media/doc/100213QFRs-Alexander.pdf. Last accessed April 8, 2014.
[43] Pg. 2 and 13, Senate Committee on the Judiciary, Continued Oversight of the Foreign Intelligence Surveillance Act, October 2, 2013. Questions for the Record for General Keith B. Alexander. https://web.archive.org/web/20140406215052/http://www.judiciary.senate.gov/imo/media/doc/100213QFRs-Alexander.pdf.
[44] Greenwald, Glenn; MacAskill, Ewen. *"Boundless Informant: the NSA's secret tool to track global surveillance data."* Guardian, June 11, 2013. http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining.
[45] *See* http://icontherecord.tumblr.com/topics/section-702.
[46] "*Procedures used by NSA to target non-U.S. persons: Exhibit A—full document.*" Guardian, June 20, 2013. ("Targeting Procedures"). http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.

procedures to be published with redactions only protecting the highest needs for national security; the public is still largely unaware about how these procedures address collection of communications using PRISM and upstream techniques.

News reports also reveal a so-called "51% foreignness" distinction in the processing cycle for collecting communications under Section 702.[47] NSA General Counsel Rajesh De recently noted that this 51% foreignness determination is one variable in the "totality of circumstances" to determine the suitability of targeting for acquisition.[48] The Board must ask:

- Where did the rules about foreignness determinations come from, who created them, who enforces them, and who updates them?
- Who is responsible for assessing the accuracy of foreignness determinations?
- If someone at NSA learns something that calls the accuracy of foreignness determinations into question, does she have to act on that? Does this affect any retroactive searches? Who is notified?
- Is there any kind of adversarial process within NSA or in its oversight concerning how an analyst determines "foreignness?"
- What other factors are considered in this "totality of circumstances" analysis?
- What is the "processing cycle" under Section 702? For instance, the government recently claimed a 0.1 % error rate for foreignness determinations. If there are 115,000 targets under Section 702 at a particular time, does that mean that about 115 of those targets are U.S. persons?

---

[47] Lee, Timothy B. "*Here's everything we know about PRISM to date."* Washington Post, June 12, 2013. http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

[48] Pg. 41 and 42, Privacy and Civil Liberties Oversight Board, March 19, 2014 Public Hearing. https://web.archive.org/web/20140406215418/http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

Further, the public does not know about other uses of the statute. Other uses of Section 702 remain classified, including its use for computer network operations. DNI General James Clapper noted Section 702's use to obtain communications "regarding potential cyber threats" and to prevent "hostile cyber activities."[49] Richard Ledgett, Deputy Director of NSA, also noted the use of intelligence authorities to mitigate DDOS[50] and other cyber attacks.[51] But the public knows nothing else about these actions. It is imperative to know in what context the NSA is using Section 702 orders for any computer network operations. Such information should be released in a manner consistent with only protecting grave damage to national security.

All of these unknowns affect American businesses, especially the technology sector. A broader question is whether any of these programs limit or restrict the architecture or technology of private-sector systems. If a company wanted to better protect its users' privacy, would it be prevented from doing so under these programs, or under a FISA Court order? Has this already happened? Many of the technical aspects of these programs are unknown. The PCLOB must educate the public on how these surveillance programs are carried out.

---

[49] *Facts on the Collection of Intelligence Pursuant to Section 702.* Office of the Director of National Intelligence. June 8, 2013. https://web.archive.org/web/20140107062825/http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf. Last accessed April 8, 2014.

[50] DDOS attacks consist of flooding websites with traffic in order to make them unavailable to the public.

[51] *See* Ted2014, *Richard Ledgett: The NSA responds to Edward Snowden's TED Talk.* March 20, 2014. *https://web.archive.org/web/20140323232303/http://www.ted.com/talks/richard_ledgett_the_nsa_responds_to_edward_snowden_s_ted_talk.* Last accessed April 8, 2014.

The government has admitted that wholly domestic communications are being collected under the statute.[52] DNI General James Clapper recently lamented the fact that NSA should have disclosed the Section 215 Business Records FISA program collecting all Americans' calling records when the program first began. In particular, he said:

> ... had we been transparent about this from the outset right after 9/11—which is the genesis of the 215 program—and said both to the American people and to their elected representatives, we need to cover this gap, we need to make sure this never happens to us again, so here is what we are going to set up, here is how it's going to work, and why we have to do it, and here are the safeguards ... We wouldn't have had the problem we had.[53]

General Clapper should apply this advice to any and all intelligence agency programs collecting big data about Americans. The intelligence community must provide the public more information in order to have a democratic debate about the surveillance authorities used in their name. This includes more affirmative disclosures as opposed to reactive declassifications.

Section 702 of the Foreign Intelligence Surveillance Act is Unconstitutional

The President's Review Group on Intelligence and Communications Technology ("Review Group") noted that Section 702 "does not adequately protect the legitimate privacy interests of United States persons when their

---

[52] Letter from Office of the Director of National Intelligence to Senator Ron Wyden. July 26, 2011. https://web.archive.org/web/20140228051623/http://www.wyden.senate.gov/download/letter-from-odni-office-responding-to-wyden-udall-concerns-about-use-of-the-fisa-amendments-act-and-geolocation-tracking. Last accessed April 8, 2014.

[53] Lake, Eli. "*Spy Chief: We Should've Told You We Track Your Calls*." The Daily Beast, February 17, 2014. https://web.archive.org/web/20140317070031/http://www.thedailybeast.com/articles/2014/02/17/spy-chief-we-should-ve-told-you-we-track-your-calls.html.

communications are incidentally acquired under Section 702."[54] Recommendation 12 by the Review Group urged:

1) the President to purge all communications collected by Section 702 involving a U.S. person unless it had foreign intelligence value or it was necessary to prevent serious harm to others;
2) to ban the use of the U.S. person information in any proceeding against the U.S. person; and,
3) to only search U.S. person communications after obtaining a probable cause warrant or to prevent a threat of death or serious bodily harm.[55]

We agree, but we also maintain that Section 702 collection under the current scheme is both illegal and unconstitutional. Because they authorize the seizure and search of communications with no specificity or particularity and no judicial authorization or review of the actual searches conducted, Section 702 certifications constitute a modern analog to the writs of assistance and general warrants used by the British in the 1700s. As this panel is well aware, resistance to these "hated writs" was the basis for the Fourth Amendment.[56] Neither the "targeting procedures" nor the "minimization procedures" require particularity consistent with the Constitution. Moreover, both procedures reveal a lack of a neutral magistrate. The collection conducted under Section 702 is indiscriminate and untargeted mass surveillance.[57]

---

[54] Pg. 10, *Report and Recommendations of the President's Review Group on Intelligence and Communications Technology*. December 12, 2013. https://web.archive.org/web/20140222030059/http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[55] *Id.* at 29.

[56] *See e.g.* Snyder, *The NSA's "General Warrants": How the Founding Fathers Fought an 18th Century Version of the President's Illegal Domestic Spying*, https://www.eff.org/files/filenode/att/generalwarrantsmemo.pdf

[57] The administration has tried to claim that surveillance conducted under Section 702 is "targeted" and not "bulk" surveillance. *See* Pg. 10. Privacy and Civil Liberties Oversight Board, March 19, 2014 Public Hearing. https://web.archive.org/web/20140406215418/http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

So-called "about" and "backdoor" searches exemplify the lack of particularity in Section 702 collection. First, the NSA searches vast quantities of communications—those of Americans and otherwise—when it collects and searches communications "about" a target of surveillance.[58] The government has represented that "about" surveillance includes searching the content of communications that are neither to nor from a surveillance target, but which contain specific selectors, such as email addresses or phone numbers of a surveillance target.[59]

When conducting "about" surveillance, the only two known filters to protect the government's search of the contents of Americans' communications are "an Internet Protocol filter" and/or the targeting of "Internet links that terminate in a foreign country."[60] These "technical measures" are grossly imprecise,[61] in the past resulting in the collection of "tens of thousands of

---

Regardless of the label applied, it is clear that Section 702 surveillance sweeps up billions of communications—including tens of thousands of completely unrelated domestic communications—that stretch the ordinary meaning of "targeted" surveillance to its limits.

[58] *See* Pg. 5, Bates Opinion.

[59] Savage, Charlie. "*NSA Said to Search Content of Messages to and From U.S.*" N.Y. Times, Aug. 8, 2013. (The NSA is "searching the contents of vast amounts of Americans' e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance"), *available at* http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html; *see also* Pg. 55 and 57, of PCLOB discussing "about" collection.

[60] *See* Pg 1-2, Targeting Procedures.

[61] "Internet links" are not defined in the 2009 Targeting Procedures, but they presumably refer to elements of the backbone, such as telecom switches and hubs, which are located overseas. Internet Protocol ("IP") addresses are the numerical identifiers ISPs assign to devices connecting to the Internet. Because ISPs are allocated blocks of IP addresses on a geographic basis, filtering by non-American IP address may be a roughly effective way of targeting non-U.S. persons. However, there many scenarios under which such a filter would still include domestic communications, such as when people using the Internet in the United States are assigned a foreign IP address because they connect using a foreign Virtual Private Network ("VPN") or are using the Tor service to route their traffic through foreign servers. In 2011, the FISA Court confirmed that these "technical measures" were insufficient "given that NSA's upstream collection devices will acquire a wholly domestic 'about' [communication] if it is routed

wholly domestic communications."[62] Notably, even when these technical measures work properly to filter out wholly domestic communications, nothing prevents the government from collecting international communications of all Americans, such as conference calls or email with one sender or recipient outside the United States.

Second, under its implementation of Section 702, the government conducts "backdoor searches"—in which it queries its database of intercepted communications for the communications of specific Americans—without a warrant or any prior court authorization.[63] Section 702 provides for the "incidental" collection and retention of Americans' international communications; indeed, under current minimization guidelines, even unintentionally acquired domestic communications may be retained. Once acquired, these communications may be stored in government databases for several years. And, given the scope of the government's collection, the quantity

---

internationally." Pg 11, Bates Opinion. In addition to the domestic communications acquired because of foreign routing, the Court also noted that NSA had incidentally acquired thousands of additional purely domestic communications as a part of "Multi-Communications Transactions" ("MCTs") in which one of many discrete communications in the MCT was intentionally targeted for collection. *Id.*

[62] *See* Pg. 11, Bates Opinion. As NSA General Counsel Rajesh De acknowledged, "because of the nature of "about" collection . . . there is potentially a greater likelihood of implicating incidental U.S. person communication or inadvertently collecting wholly domestic communications that therefore must need to be purged." PCLOB Hearing 94:12-16. However, these purely domestic communications can still be initially retained for up to two years, *id.* 94:22-95:2, and indefinitely if they contain "foreign intelligence information." 2011 Minimization Procedures § 5.

[63] *See* Letter from James R. Clapper to Senator Ron Wyden, March 28, 2014, available *at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1100298/unclassified-702-response.pdf; *see also* Ackerman, Spencer; and, Ball, James. "*NSA loophole allows warrantless search for U.S. citizens' emails and phone calls."* Guardian, Aug. 9, 2013, available *at* http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls.

of communications—including communications of Americans—within these databases is vast.

Nevertheless, the government maintains that having "lawfully collected" these communications of Americans, the government does not need court approval to search "information that is [at] the government's disposal to review in the first instance."[64] The President's Review Group disagreed, concluding that this practice should be stopped:

> Because the underlying rationale of Section 702 is that United States persons are entitled to the full protection of their privacy even when they communicate with non-United States persons who are outside the United States, they should not lose that protection merely because the government has legally targeted non-United States persons who are located outside the United States under a standard that could not legally be employed to target a United States person who participates in that communication.[65]

Targeting Procedures are no Substitute for Probable Cause, Particularity, or a "Neutral and Detached" Magistrate

The review group's conclusion makes plain a fundamental problem of the government's implementation of Section 702 acquisition. These programs seize[66] communications protected by the Fourth Amendment by targeting "foreign" persons who supposedly lack Fourth Amendment rights and can be targeted without probable cause. Once seized, however, the protected

---

[64] *See* Pg 10 and 31, PCLOB Hearing.

[65] *Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies* 145-46 (2013) (emphasis in original).[65]

[66] It is well settled that government acquisition of communications is a Fourth Amendment seizure. In *Berger v. New York,* the "property sought" was intangible conversations and the Supreme Court repeatedly referred to the act of recording the aural conversations as a "seizure." 388 U.S. 41, 57, 59-60 (1967); *see also United States v. New York Telephone Co.*, 434 U.S. 159, 170 (1977). Similarly, in *United States v. Comprehensive Drug Testing, Inc.*, the Ninth Circuit repeatedly noted how the government had improperly "seized" data when it improperly copied computer files outside the scope of a search warrant. *See, e.g.,* 621 F.3d 1162, 1166 (9th Cir. 2010) (en banc) (per curiam) ("the government *seized* and promptly reviewed" computer files) (emphasis added).

communications of U.S. persons are "fair game" for further searching. The indiscriminate seizure and search of these protected communications eliminates U.S. persons' Fourth Amendment protections by eliding any probable cause determination, even the traditional FISA probable cause requirement. Instead, an acquisition is authorized if "a significant purpose of the acquisition is to obtain foreign intelligence information."[67]

Fourth Amendment case law provides for a probable cause warrant to be issued by a "neutral and detached" magistrate.[68] The requirement guards against the evils of general warrants and ensures that "those searches [that] are deemed necessary should be as limited as possible."[69] Particularity ensures that "the search will be carefully tailored to its justifications," eliminating the threat of a "general" search.[70] Even targeted requests focused on one particular person or one specific place can fail the particularity requirement if the warrant's description of what the government can search and seize is too "generic" or "general."[71] There is no particularity under Section 702.[72]

Similarly, no neutral, detached magistrate approves Section 702 seizure or search. Interposing a magistrate "between the citizen and the law enforcement officer 'engaged in the often competitive enterprise of ferreting out crime'" is designed to make the probable cause and particularity

---

[67] 50 U.S.C. 1881a(g)(2)(v).
[68] *Coolidge v. New Hampshire*, 403 U.S. 443, 443 (1971).
[69] *Id.*, at 467.
[70] *Maryland v. Garrison*, 480 U.S. 79, 84 (1987).
[71] *United States v. Spilotro*, 800 F.2d 959, 963-64 (9th Cir. 1986) (Kennedy, J).
[72] *See* 50 U.S.C. § 1881a(g)(4) ("certification made under this subsection is not required to identify the specific facilities, places, premises, or property at which an acquisition").

requirements meaningful.[73] Judicial "scrutiny is intended to eliminate altogether searches not based on probable cause."[74] And by insisting the government's search be "particularized," a judge ensures that "as to what is to be taken, nothing is left to the discretion of the officer executing the warrant.'"[75]

Under Section 702, however, the FISA Court cannot exercise this critical role in the Fourth Amendment scheme. Indeed, the programmatic nature of FISA Court authorizations under Section 702 means that the FISA Court cannot uphold the Fourth Amendment's warrant requirement because it does not even receive details of the programs or how they are actually implemented with regard to individual U.S. or foreign persons.

As noted earlier, a Section 702 certification need not specify who the surveillance targets are, what evidence supports the conclusion that surveillance of their communications is likely to yield foreign intelligence information, what communications accounts or websites it will subject to surveillance, or what information the government's surveillance seeks. In the FISA Court's 2011 Upstream opinion, Judge Bates commented that he could not assess "for certain" details of how the program operated as to "multiple communications transactions,"[76] despite his having met with senior DOJ officials to voice "serious concerns" about "whether the Court could make the findings necessary

---

[73] *Treasury Employees v. Van Raab*, 489 U.S. 656, 667 (1989) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948))
[74] *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).
[75] *Andresen v. Maryland*, 427 U.S. 463, 480 (1976) (quoting *Stanford v. Texas*, 379 U.S. 476, 485 (1965)).
[76] *See* Pg. 10, Bates Opinion.

to approve the acquisition of such transactions pursuant to Section 702."[77] Ultimately, the government did not provide the full details requested by Judge Bates, and the FISA Court based its ruling in part on conjecture.[78] Such authorizations fly in the face of the warrant requirement as well as the court's Article III function as a check on executive action, but this is the limited role of the FISA Court under Section 702.[79]

Instead, Executive branch officials—the Attorney General and the DNI—have enormous discretion to decide whom to target, when, where, and under what circumstances. Executive branch officials issue the actual "directives" that compel providers to assist in surveillance. The Fourth Amendment, however,

> does not contemplate the executive officers of Government as neutral and disinterested magistrates. Their duty and responsibility is to enforce the laws, to investigate, and to prosecute. . .But those charged with this investigative and prosecutorial duty should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks.[80]

In short, "there could hardly be a more appropriate setting than this for a *per se rule of disqualification*...prosecutors and policemen simply cannot be asked to maintain the requisite neutrality with regard to their own investigations—the 'competitive enterprise' that must rightly engage their single-minded attention."[81]

That the FISA Court reviews targeting and minimization procedures

---

[77] See Pg. 3, Bates Opinion.
[78] See Pg. 11, footnote 32, Bates Opinion.
[79] *See* 50 U.S.C. § 1881a(i).
[80] *United States v. United States Dist. Court*, 407 U.S. 297, 317 (1972) (citation omitted).
[81] *Coolidge*, 403 U.S. 443, at 454-55 (emphasis added) (citing *Mancusi v. DeForte*, 392 U.S. 364, 371 (1968)).

cannot alter this conclusion. First, the targeting procedures are neither specific nor "targeted." Second, the minimization procedures are intended to overcollect and overretain completely innocent communications—communications that, in any other context, would have to have been collected with a probable cause warrant or FISA warrant.

The statutory meaning of "targeting" in Section 702 has become extremely misleading. The most glaring problem, revealed in the discussion of "about" searches, is that the government interprets "targeting of persons" to include communications "about" the person. We do not normally think of surveillance targets this way: the law of domestic surveillance thinks of targets as parties to communications (senders or receivers), not topics of discussion. The government's interpretation that it has a roving commission under Section 702 to acquire "about" communications subjects any person who discusses a "target"—even a public figure—to surveillance.

This interpretation makes no sense under the statute. On its face, Section 702 is about procedures for targeting non-U.S. persons outside the United States, which is consistent with the normal notion of targets as senders or receivers. But one's location is constitutionally irrelevant to whether one can be targeted as the topic of an email. Indeed, this interpretive move makes "targeting" about the content of the communication, seemingly requiring searches of content in order to determine whether the acquisition is properly targeted.

We had also understood that Section 702 sought to exploit the notion

that a person must be "of the people" to be protected by the Fourth Amendment.[82] In that context, U.S. person status is constitutionally significant. The operative statutory text, however, focuses on location, not status. The authority is to "target[] persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[83] The targeting procedures must be "reasonably designed to ensure that any acquisition authorized by 702 is limited to targeting persons reasonably believed to be outside the United States."[84]

But the targeting procedures need not be reasonably designed to prevent targeting of U.S. persons. They could be poorly designed to prevent such targeting, so long as they do not "intentionally" target. Unsurprisingly, the leaked targeting procedures presume that anyone reasonably believed to be abroad or whose location is unknown is a non-U.S. person absent positive identification as a U.S. person or contradicted by the "nature or circumstances of the person's communications."[85]

The government's linguistic prestidigitation is compounded by inadequate filtering. The publicly released targeting procedures reveal NSA conducts some post-acquisition filtering to the communications it obtains under Section 702. In targeting procedures filed in 2009, the NSA noted that "about"

---

[82] United States v. *Verdugo-Urquidez*, 494 U.S. 259 (1990)
[83] 50 U.S.C. § 1881a(a).
[84] 50 U.S.C. § 1881a(d)(1)(A).
[85] 2009 Targeting Procedures, at 4.

communications[86] are filtered by IP address or "target Internet links that terminate in a foreign country."[87] Such filters do not ensure the collected communications will be located outside the United States or will not contain a U.S. person communication.

U.S. persons routinely communicate with foreign servers. One Stanford University PhD Candidate has noted that many domestic websites—including the U.S. House of Representatives' house.gov—loads content from an international website.[88] The Bates Opinion pointed to the filters based on IP addresses and the routing information of the communications as one way to select for foreign-ness; however, the opinion does not mention that IP addresses are an imprecise tool for determining whether a communication is international as an IP address has no fixed geographical correlate.[89] The Board must ask what counts as "foreign" when it comes to IP address filtering, since the filtering can only reveal the country where the machine connecting to the Internet is from.

Another example of the difficulty in using IP addresses is the use of virtual private networks (VPNs). VPNs tunnel traffic from one country to another, so the address where it appears to originate from is not the ultimate origin. VPNs are also used with origination and termination in every country. But

---

[86] Communications involving two innocent third parties whose communications include a given selector.
[87] Ball, James; Greenwald, Glenn. "*Exhibit A—Full Document*." Guardian, June 20, 2013. http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.
[88] Mayer, Jonathan. *Comments to the President's Review Group on Intelligence and Communications Technology*. October 23, 2013. https://web.archive.org/web/20140321223121/https://jonathanmayer.org/papers_data/dni_comment13.pdf. Last accessed February 21, 2014.
[89] *See* Pg. 45-46, Bates Opinion.

the "proper" handling of VPN traffic presumably depends on what the NSA thinks makes traffic "foreign."

This problem is not specific to VPNs. A shared email server by persons of different countries can send outbound traffic from any one of the shared persons' countries. Such an example begets the problem of trying to decipher just what is and is not a U.S. or non-U.S. person communication. Yet another problem with IP filtering are periodic errors in commercial IP geolocation databases. This is sometimes seen to cause conflict over access to items like country-restricted video.[90] While infrequent, IP address shuffling could cause major problems for the mass collection of communications filtered by IP address ranges.

Apart from these examples, the targeting procedures do not prevent the intentional acquisition of a wholly domestic communication or limit targeting to persons reasonably believed to be located outside the United States. The Bates Opinion ascertained that the NSA was collecting at least tens of thousands of wholly domestic U.S. communication under its upstream collection everyday.[91] The FISA Court concluded that the targeting procedures were "reasonably designed" to prevent the intentional acquisition of communications outside the US, in part, because the NSA's upstream collection devices lacked the capacity to detect wholly domestic communications at the time of acquisition.[92]

---

[90] *See* Smith, Chris Silver. *Geolocation: Core to the Local Space and Key to Click-Fraud Detection*, Search Engine Land, August 13, 2007. http://searchengineland.com/geolocation-core-to-the-local-space-and-key-to-click-fraud-detection-11922.

Nor are the targeting procedures consistent with the limitations provided in the statute. Section 702 requires that the targeting procedures be "reasonably designed" to "prevent the intentional acquisition" of wholly domestic communications.[93] Yet they plainly are not. As the Bates Opinion notes: "a person intends to produce a consequence either (a) when he acts with a purpose of producing that consequence or (b) when he acts knowing that the consequence is substantially certain to occur."[94] It is clear from the lack of particularity in the targeting procedures that wholly domestic communications are "substantially certain to occur."[95] If the targeting procedures were "reasonably designed" to not collect wholly domestic communications, the NSA would—at minimum—aggressively limit collection in the first instance, perhaps through filtering, to ensure that wholly domestic communications are only collected at the outset with a probable cause warrant.

Even beyond filtering, reasonably designed targeting procedures would account for the architecture of the Internet and the fact that visitors of everyday websites, and users of VPNs and anonymizing sources who are U.S. persons, will have their communications acquired under a Section 702 general warrant. The lack of technical filtering or other steps taken to avoid domestic communications results in the intentional acquisition of a massive set of domestic communications—a general seizure and search.

Regarding the targeting procedures, we urge the Board to:

---

[93] *See* Pg. 14, Bates Opinion.
[94] *See* Pg. 46, footnote 43 , Bates Opinion
[95] *See* ibid.

- Declassify and perform a statutory analysis of the current targeting procedures;
- Analyze how broad the current targeting procedures are applied.
- Declassify past targeting procedures;
- Analyze how the targeting procedures conform to the Constitutionally required particularity requirements when collecting U.S. person communications.

At the minimum, we urge the Board to submit a detailed analysis and summary of the current targeting procedures in order to study whether or not the procedures comport to the statutory requirements and with the Constitution.

Minimization Procedures Intended to Overcollect U.S. Person Communications, Overretain U.S. Person Communications, and Disseminate U.S. Person Communications Everywhere Without a Probable Cause Warrant

The minimization procedures present another constitutional problem. They plainly and inevitably over-collect and over-retain American communications, communications that could otherwise only be seized and searched after issuance of a probable cause warrant or FISA warrant. The procedures acknowledge this directly, providing specific guidelines for when "wholly domestic communications" can be collected, retained, and searched. Yet wholly domestic communications should not be collected, retained or searched under 702, since that process is far weaker than what the Fourth Amendment requires.

Wholly domestic communication obtained through upstream collection (which the regulations call "inadvertent") can be kept in six different scenarios and (in some of those cases) retained in searchable NSA databases forever.[96] As mentioned in the description of "backdoor searches," any of these communications—including American communications—may be searched without a probable cause warrant, or even a lower-standard FISA warrant.

For instance, the Director of NSA must approve the retention of any domestic communication under what we call a "Section 5 Minimization Procedures" exemption.[97] Such Director-level approval appears protective, but covers a tremendous range of communications. The Director can choose to retain any communication: containing foreign intelligence information (which can then be sent unminimized to the FBI),[98] showing evidence of a crime,[99] containing "technical data base" information (which includes encrypted communications or communications needed for "traffic analysis"),[100] or pertaining to serious harm of life or property.[101]

Thus, while the NSA is supposed to be limited to foreign intelligence and is not supposed to be an extension of domestic criminal law enforcement, NSA's minimization procedures allow for it to use, share, and retain *any* communication which may indicate a domestic crime. Plainly, these Section 5 exemptions are beyond the scope of the NSA's mission. The communications at issue – wholly

[96] The communications can be kept in accordance with Section 4, Section 5(1), Section 5(2), Section 5(3), Section 5(4)
[97] Minimization Procedures, Section 5.
[98] Minimization Procedures, Section 5(1).
[99] Minimization Procedures, Section 5(2).
[100] Minimization Procedures, Section 5(3).
[101] Minimization Procedures, Section 5(1)-(4).

domestic communications—should have never have been acquired in the first place under the statutory limitations and so, rather than serving as a "freebie" for domestic law enforcement, they should be destroyed. Even if one believes the Director of NSA provides nominal protection, the NSA Director simply is not a neutral and detached magistrate.

Moreover, the procedures provide that wholly domestic communications can be retained without approval of the Director if they are attorney-client communications[102] and/or if they are shared with foreign governments.[103]

Communications that are not wholly domestic but that include a U.S. person, such as a communication where a U.S. person sends/receives a message from a non-U.S. person, may be retained by an analyst for the same reasons as above. This type of collection and retention occurs even if the U.S. person is not communicating with a target, such as when the communication is "about" (more clearly, when a communication references in any way) a selector. When such a communication involves a U.S. person, the U.S. person information and conversation should—at the minimum—be obfuscated. Unfortunately, this is not the case. The communications can be kept without obfuscating U.S. person information where:

- The U.S. person information is necessary to understand foreign intelligence.[104]
- The communications concerns the unauthorized disclosure of national security information.[105]

[102] Minimization Procedures, Section 4.
[103] Minimization Procedures, Section 8.
[104] Minimization Procedures, Section 6(b)(1).
[105] Minimization Procedures 6(b)(5).

- There is evidence that a crime has been, is being, or is about to be committed.[106]

These communications are "incidentally" (or "inadvertently")[107] collected, but are not guaranteed Fourth amendment protections. This should not be the case, especially when such communications can be queried or disseminated to other government agencies. At the minimum, a probable cause warrant or FISA warrant should be obtained prior to government access to the speech of the U.S. person.

Of particular note in all of these retention scenarios is an exemption to keep communications “reasonably believed to contain technical data base information.”[108] The phrase “technical data base” is a specifically defined term that means “information maintained for cryptanalytic, traffic analytic or signal exploitation purposes.”[109] "Cryptanalytic" use involves any use of encryption or ciphertext. According to the procedures, NSA is allowed to retain communications solely because one uses encryption, regardless of whether the communication is otherwise subject to targeting.[110] The communication will be retained forever, or at least until it is decrypted whether or not the communication is wholly domestic or foreign. This is plainly a general

[106] Minimization Procedures 6(b)(8).
[107] The government defines "incidental" collection as collection that occurs under any legal mechanism. This is opposed to "inadvertent" collection, which the government defines as collection not authorized by law. Pg 102. PCLOB Hearing.
[108] Minimization Procedures, Section 5(3) and Section 6(a)(1).
[109] Minimization Procedures, Section 2(j).
[110] Minimization Procedures, Section 5(3) and Section 6(a)(1).

collection—collection based upon the secrecy method chosen rather than any indicator of intelligence or illegal activity. This is plainly overreach.

Furthermore, the definition of "technical data base" suggests that NSA believes it can keep domestic communication to the extent that they can be used for traffic analysis. Any communication, again regardless of intelligence or domestic criminal import, can be used for "traffic analysis." An expansive reading of the definition could lead to a conclusion that NSA can keep all communications and doesn't have to discard any. Taken as a whole, these loopholes show that many communications involving U.S. person can be retained without a probable cause warrant.

All of the above scenarios assume the location of every recipient is known. A grave problem with the minimization procedures is the fact that it rewards behavior that neglects to identify where a person is located. If a communicant's location is unknown, the targeting and minimization procedures presume that the communicant is a non-U.S. person.[111]

This presents a serious problem for U.S. persons who seek to protect their privacy by using anonymity tools that may that mask their location. There is a Constitutional right to anonymous speech, and exercising this right cannot be grounds for the government to invade your privacy by collecting your communications.[112] Indeed, *Doe v. 2themart.com Inc.* concluded: "the

---

[111] Minimization Procedures, Section 5(3) and Section 6(a)(1). These communications will be kept forever or until no longer needed.

[112] *See Buckley v. Am. Constitutional Law Foundation*, 525 U.S. 182, 200 (1999) (invalidating, on First Amendment grounds, state statute requiring initiative petitioners to wear identification badges); *Talley v. California,* 362 U.S. 60, 65 (1960) (holding anonymity protected under the

constitutional rights of Internet users, including the First Amendment right to speak anonymously, must be carefully safeguarded."[113] The minimization procedures do not acknowledge these issues for anonymous communications; in the NSA's view, if you use anonymizing software like Tor, the protections for a U.S. person simply do not apply.

In short, the targeting procedures allow for over-collection and the minimization procedures allow for over-retention, effectively making Section 702 a general warrant. Some communications involving a U.S. person may be kept forever,[114] and cannot be considered "reasonable."

As noted above, the Fourth Amendment, and indeed the entire American Revolution, was spurred in part by the founders' rejection of the so-called "hated writs" on the grounds, among others, that they did not require judicial approval, particularity and a finding or probable cause prior to seizure. It simply strains credulity to posit that they would not have taken a different position had the "writs" allowed British courts to approve only general "targeting procedures" and "minimization procedures" that then allowed the British

---

First Amendment because forced "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance"). As the Supreme Court has held, "Anonymity is a shield from the tyranny of the majority," that "exemplifies the purpose" of the First Amendment: "to protect unpopular individuals from retaliation...at the hand of an intolerant society." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 357 (1995)

[113] *Doe v. 2themart.com Inc.,* 140 F. Supp. 2d 1088, 1097 (WD Wash. 2001)

[114] The retention period differs upon the use of the communication. Communications used for traffic analysis and communications never identified as domestic communications could be kept forever in the NSA's databases, while other communications used for foreign intelligence information are only kept for five years. In the March 19, 2014 PCLOB public hearing, NSA General Counsel Rajesh De testified that 2 years is the standard time period of retention for upstream collection. For the testimony, *see* page 47 and 94 of *PCLOB Public Hearing Panel I Transcript,* March 19 2014. https://web.archive.org/web/20140324224540/http://www.pclob.gov/Documents/19%20March%202014%20PCLOB%20Public%20Hearing_Panel%20I%20Transcript.pdf.

authorities to collect any (or all) colonists' personal papers and specifically target a particular colonist with no additional judicial review and subject only to general "minimization procedures" rather than specific approval of what items were seized or searched. The complexity of the procedures simply cannot hide the underlying general seizure.

In short, Section 702 creates a process by which the government can issue a general warrant. No court approves the analyst's decisions, or the NSA Director's decisions, no court reviews how those decisions are actually applied, and no court sees the actual communications (specifically or in general) that are being shared or retained.

Foreign Intelligence Exception

The Foreign Intelligence Exception does not apply categorically to Section 702 surveillance; the Supreme Court has never ruled that there even is a foreign intelligence exception to the warrant requirement, although various circuit courts have recognized it in cases that did not deal with bulk collection, and focused on the involvement of foreign powers.[115]

Quite plainly, the constitutional problems with Section 702 come from the collection of U.S. persons' communications, not those of non-U.S. persons.[116] Specifically, as noted above, they arise from the fact that the U.S.

---

[115] *See*, *e.g., United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), *cert. denied,* 454 U.S. 1144 (1982); *but see Zweibon v. Mitchell,* 516 F.2d 594 (DC Cir. 1975) (en banc) (plurality opinion), *cert. denied,* 425 U.S. 944 (1976). In *Zweibon v. Mitchell,* the court found that there is no foreign intelligence exception for surveillance of U.S. citizens in the U.S. who are neither agents of a foreign power or acting in collaboration with a foreign power. The "foreign" aspect of the surveillance was reiterated in *United States v. Truong Dinh Hung,* which found a foreign intelligence exception only if 1) the U.S. citizen is a foreign power's agent, or a collaborator; and 2) the surveillance was conducted primarily for foreign intelligence reasons.

[116] As noted below, the effect on non-US persons is a separate problem.

communications collected under Section 702 concern communications between two untargeted U.S. persons, and domestic or foreign communications of or concerning a U.S. person. In many of the collections, the U.S. person was not a target, was not an agent of a foreign power, or a collaborator of an agent of a foreign power. As shown above, the conducting of indiscriminate mass surveillance, the inability for targeting procedures to exclude protected communications like U.S. person communications, and the retention and potential analysis of U.S. person communication as retained by the minimization procedures, will undoubtedly include Fourth Amendment protected U.S. person communications. The collection is overbroad and overretained. And once collected—and before any "post-acquisition" phase—the Fourth Amendment is implicated. Thus, the Foreign Intelligence exception, to the extent that it exists, simply does not apply here.

Section 702 On Its Face Does Not Authorize Bulk Collection

On its face, Section 702 simply does not authorize bulk acquisition of communications records or content, such as the government's access to fiber optic cables of American telecommunications companies.[117] Most importantly, for purposes of statutory interpretation, the statute does not use the terms "bulk" or "mass" collection or otherwise suggest that the government may

[117] EFF has presented evidence of such access in *Jewel v. NSA*. *See generally* Declaration of J. Scott Marcus filed in support of Plaintiffs' Motion for Partial Summary Judgment, *Jewel v. NSA*, No. C-08-4373-JSW (N.D. Cal. Nov. 2, 2012), ECF No. 89. Additionally, public statements by government officials and the declassified FISC opinions provide such evidence. *See* Pg. 2, footnote 3, Bates Opinion discussing the NSA's "upstream" collection, the "interception of Internet communications as they transit [redacted]"; *see also* Pg. 22 and 26. PCLOB Hearing statement of NSA General Counsel Rajesh De that upstream collection is achieved through the "Internet backbone."

obtain “all” communications that travel over a particular fiber-optic cable or via some other transit process. Such words would have made the congressional intent clear and the statutory language plain. Moreover, given the severe constitutional infirmities in any such bulk acquisition program, the statute should be presumed to avoid these constitutional infirmities.[118]

Any such words also would have sparked an actual public discussion of the advisability of mass collection (as opposed to targeted acquisition) of innocent Americans’ domestic or international communications when the law was enacted. That no such discussion occurred, but is loudly and prominently occurring now, demonstrates that the ordinary reading of the statute does not even hint at the possibility of imposing a mass acquisition program on the American public.

Lacking an express Congressional authorization, the government’s position appears to attempt to squeeze mass, untargeted acquisition into the statutory language of 702. Yet as the Supreme Court has reminded us, "Congress does not...hide elephants in mouseholes."[119]

First, the statute itself is solely concerned with targeting procedures and minimization procedures. Specifically, it addresses

> (a) . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information

and strictly limits that authority to acquisition:

---

[118] *Cf. INS v. St. Cyr*, 533 U.S. 289, 299-300 (2001) (When faced with several “fairly possible” statutory constructions, Court is obligated to construe statute by adopting construction that avoids “serious constitutional problems”).

[119] *Whitman v. Am. Trucking Association* 531 U.S. 457, 468 (2001).

> (b)(1) may not intentionally target any person known at the time of acquisition to be located in the United States . . .
>
> (b)(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.

It similarly requires that any targeting procedures under subsection (d) must be "reasonably designed to" meet the same terms: both ensuring that the acquisition is limited to targeting persons reasonably believed to be located outside the United States; and preventing the intentional acquisition of communications as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.

Thus, the statute is framed in terms of "targeted" acquisition in the first place, not untargeted acquisition. It strains credulity to think that mass collection from the fiber optic cables located inside the U.S. is either "reasonably designed" to ensure that acquisition is limited to persons believed to be outside the U.S. or that all communicants are known to be inside the U.S. The cables plainly carry both international and domestic traffic.[120]

In fact, the government's mass acquisition through access to the fiber optic cables inside the United States is the opposite of acquisition based upon "targeting." By design, this kind of general acquisition system makes no distinction between relevant and irrelevant information.

The government seeks to shift the question of "targeting" from the point of the government's acquisition of the data to some point post-acquisition when the government queries the information based on "selectors." That shift

---

[120] *See* Pg 16, Bates Opinion.

cannot find any justification in Section 702. The statute's "targeting" limitations apply to the "acquisition" of information, that is, at the time the government obtains custody.

Nor do the minimization procedures remedy this problem. Those procedures do not provide that what is being "minimized" is everything, rather than material that was targeted from collection. Under § 1801(h), those procedures must be:

> Reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain produce, and disseminate foreign intelligence information.

The government may contend that the mass, untargeted acquisition of content and records, such as via fiber optic cables, is "reasonably designed in light of the purpose and technique of the particular surveillance" under § 1801(h). The argument is that the mass acquisition is a "technique" used to detect contacts between foreign terrorists and potentially unknown associates within the United States. And so, using circular logic, if the "technique" requires collection of everything, the collection of everything under the "technique" is "reasonable. Yet this improperly shifts the question from pre-acquisition requirement "targeting" to a post-acquisition "minimization" procedure. And nothing in the text of Section 702 can be used to attribute to Congress that intent.

Section 702's Impact on Innocent Foreigners

Section 702 is also problematic in its impact on innocent non-U.S. persons both abroad and in the United States. The United States is party to

numerous international human rights agreements that are implicated by Section 702.[121] It has supported the adoption of the Universal Declaration of Human Rights (UDHR) and has ratified the International Covenant on Civil and Political Rights (ICCPR). The ICCPR obligates Member States that have ratified the treaty to protect and preserve basic human rights, including that of human dignity; equality before the law; freedom of expression, assembly, and association, and the right of privacy. Ratified treaties are binding on the United States as a matter of international law and constitute the "supreme Law of the Land" under the United States' Constitution.[122] In other words, the United States must implement and comply with the provisions of the treaty, subject to Reservations entered when it ratified the treaty.[123]

In the case of Section 702, and other provisions dealing with surveillance, the United States has an obligation to ensure that its statutes comply with UDHR and ICCPR's standards on (in particular) the right to privacy, the right of freedom of expression and information, and the interference with human rights such as the right of association. Activities that constitute an interference with human rights, such as communications surveillance, can only be justified when they are prescribed by law, when they are necessary to achieve a legitimate aim, and when they are proportionate to the aim pursued. This "permissible

---

[121] United States of America, Common core document forming part of the reports of States parties, HRI/CORE/USA/2011, 2011, http://tbinternet.ohchr.org/_layouts/treatybodyexternal/SessionDetails1.aspx?SessionID=625&Lang=en

[122] While the U.S. maintains that its treaty obligations are not self-executing, that does not impact its obligation to ensure that its laws fit within those obligations.

[123] U.S. reservations, declarations, and understandings, International Covenant on Civil and Political Rights, 138 Cong. Rec. S4781-01 (daily ed., April 2, 1992) http://www1.umn.edu/humanrts/usdocs/civilres.html

limitations" test applies equally to the rights to privacy, freedom of expression, and freedom of association of everyone, without discrimination on the basis of nationality or place of residence.[124]

The United States also has extraterritorial obligations to uphold individual human rights outside its borders. While it currently denies this, its position has been soundly rejected by the U.N. Human Rights Commission,[125] as detailed below. Moreover, then-Legal Advisor to the U.S. State Department official, Harold Koh,[126] urged revision of this position. Given the extraordinary capabilities and programs of the United States to extend its power across the world's population and monitor global communications, the Board should affirm the true scope of the U.S. obligation and urge the United States to accept that its human rights and other international legal obligations apply extraterritorially to all persons whose communications it scans or collects. Put another way, the U.S. obligations to protect human rights extend coincident with their power to violate those human rights—the power to surveil, which the U.S. obviously has extraterritorially, must be bounded by basic human rights protections. To accept otherwise would defeat a core object and purpose of the ICCPR, and

---

[124] *See e.g.* International Principles on the Application of Human Rights to Communications Surveillance, available at https://en.necessaryandproportionate.org/text. The legal underpinning of each of these requirements in more detail will be published in a forthcoming publication that should be available at the above-referenced website by May 1, 2014: "Background and Supporting International Legal Analysis of the International Principles on the Application of Human Rights Law to Communications Surveillance.

[125] *See* http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FUSA%2FCO%2F4

[126] *See* http://www.ejiltalk.org/harold-kohs-legal-opinions-on-the-us-position-on-the-extraterritorial-application-of-human-rights-treaties/

indeed of all international human rights law, which is to ensure that States recognize and protect the rights for all persons.

Universality, Equal Protection, and Non-Discrimination

The U.S. government's position is also discriminatory in violation of international human rights law. The "protections" of 702, such as the "targeting" and "minimization" procedures described above, are aimed at solely protecting the rights of U.S. persons whose information may be collected along with the collection of information from non-U.S. persons. Moreover, historically, the United States has asserted no legal protection to the privacy rights of non-U.S. persons outside of the United States and has recognized no limits on the U.S. government's' ability to monitor these communications to any extent and for any reasons.[127] This position should be soundly rejected. International human rights law protects the rights of everyone without discrimination on the basis of nationality or place of residence. As the Universal Declaration of Human Rights provides: "All human beings are born free and equal in dignity and rights." That includes the right to privacy and freedom of expression and association.

Mass Surveillance is Inherently Disproportionate

The U.S. mass surveillance programs, including Section 702, fail to meet the standard of necessity and proportionality in international law, in that the dragnet collection of information about non-suspicious individuals is a far too inclusive method.

---

[127] *See http://www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=14383&LangID=E.* Any limitations are applied pursuant to Executive Order or other Executive power alone.

This requirement of proportionality is particularly important in the context of mass surveillance, which is based on the indiscriminate collection and retention of communications and metadata without any form of targeting or reasonable suspicion. The European Court of Human Rights jurisprudence may be helpful to the Board in this regard. In the case of *S. and Marper*, for example, the Grand Chamber of the European Court of Human Rights held that the "blanket and indiscriminate" retention of DNA data amounted to a "disproportionate interference" with the private lives of those persons from which the data had been taken.[128] The Grand Chamber placed particular weight on the fact that the material was "retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected." As explained above, the retention of material unrelated to the basis for the targeting is a serious concern under Section 702's procedures.

In another case involving the use of search powers, the Grand Chamber found the absence of any requirement on the police to have "reasonable suspicion" that the person being searched was involved in criminality meant that the search power lacked "adequate legal safeguards against abuse."[129] Most recently, in its decision in *Digital Rights Ireland Ltd*, the Grand Chamber of the Court of Justice of the European Union held that, although the retention of communications data under the Directive was for the legitimate aim of combating "serious crime," the blanket nature of the obligation entailed "an interference with the fundamental rights of practically the entire European

[128] *See* Pg. 125, *http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-90051*
[129] Case of Gillan and Quinton v. UK, application 4158/05. Jan. 12, 2010.

population," including "to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."[130] Of course, the same concerns exist with bulk collection methods occurring under Section 702's authority.

By its very nature, mass surveillance does not involve any form of targeting or selection—let alone any requirement on the authorities to show reasonable suspicion or probable cause. Accordingly, mass surveillance is inevitably disproportionate as a matter of simple definition.

We urge the Board to state that the U.S. government must conduct its surveillance of non-U.S. persons, in the United States or abroad, within the limits of international human rights law. We suggest that the International Principles on the Application of Human Rights to Communications Surveillance (the "Necessary and Proportionate Principles") can serve as an important guiding framework for the implementation of existing human rights protections into communication surveillance law, authorities and powers.[131] The Principles have been endorsed by 400 organizations, and have gathered support from European and Canadian Parliamentarians, political parties, and prominent individuals.[6]

United Nations Human Rights Committee Raises Concerns About Section 702 and Non-U.S. Persons

The United Nations' Human Rights Committee, which monitors compliance with ICCPR, noted in its fourth periodic report on the United States that non-

[130] Case 239/12, Digital Rights Ireland Ltd. v. The Minister for Communications, Marine and Natural Resources [2014] http://curia.europa.eu/juris/documents.jsf?num=C-293/12
[131] *See* https://en.necessaryandproportionate.org/take-action/redpatodos

U.S. persons "enjoy only limited protection against excessive surveillance." The committee specifically highlighted surveillance under Section 702 as being of particular concern.[132]

The report concludes that the United States should ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance, adding that the collection, access and use of communications data should be tailored to specific legitimate aims, sufficiently precise in describing circumstances, categories of person, limits on duration, and procedures for use and storage, and effective safeguards against abuse.

As we have described elsewhere in this document, these basic principles of privacy are not reached by the supposed protections of the "targeting" and "minimization" procedures provided by Section 702. Non-U.S. persons do not receive even this limited protection. The much lower standards for non-U.S. persons include:

- A definition of "foreign powers" that includes foreign political organizations, even when those groups exercise legitimate political activities, do not threaten the national security of the United States, and have no connection to a foreign state or faction. [133]

- A differing definition of "foreign intelligence information"[134] which requires only that the information collected "with respect to a foreign power or territory" may "relate to" (as opposed to "be necessary to" in the case of

---

[132] *See* Pg 22, UN. Hum. Rts. Comm. CCPR/C/USA/CO/4. http://tbinternet.ohchr.org/_layouts/treatybodyexternal/Download.aspx?symbolno=CCPR%2FC%2FUSA%2FCO%2F4&

[133] 50 USC 1801(a)(5)

[134] 50 USC 1801(e)(2)(B)

U.S. persons) the conduct of the foreign affairs of the United States. This is an extremely overbroad categorization which could potentially include millions of foreigners with the most tenuous connection to U.S. foreign affairs.

- No statutory minimization procedures[135] to prevent dissemination, or identification, or retention of private data regarding non-U.S. persons.
- No oversight or transparency: neither the certification[136] provided by the executive, nor regular assessments[137] mandated by Section 702 make any claims to assert protections or document violations of non-U.S. persons' privacy.

PRISM, Upstream and similar programs have disturbed and angered many non-U.S. persons[138], more so when they discovered the flimsy protections for the data of foreigners in current U.S. law, as guarded on United States soil by United States companies.

Section 702 was supposedly introduced, in part, to deal with the mixture of foreign and domestic data on U.S. soil.[139] Its misuse has led to serious economic and reputational damage to the United States, which can only be repaired by strong, enforceable assurances to America's global market of non-U.S. Internet users. In particular, Section 702 provides no guarantee either through process or by appearance that the United States will restrain through rule of law any

---

[135] 50 USC 1801(h)
[136] 50 USC 1881(g)
[137] 50 USC 1881(l)
[138] See e.g, European Parliament report on NSA Surveillance Program, 2013/2188(INI) http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2013/2188%28INI%29
[139] *See* the discussion of "foreign-to-foreign" communications by Senator Jon Kyl, Congressional Record Volume 154, Number 105 (Tuesday, June 24, 2008), ppS6006 of http://www.gpo.gov/fdsys/pkg/CREC-2008-06-24/html/CREC-2008-06-24-pt1-PgS6006-5.htm

secret program of global mass surveillance that impacts millions of people around the world.

The indiscriminate collection, analysis, and retention of the private data of innocent non-U.S. persons is as much a violation of the tenet that surveillance should be necessary and proportionate as is the mass surveillance of innocent Americans. We urge the Board to make this clear in its report.

Some Suggested Fixes to Section 702: Statutory Changes, the Role of Courts, and Increased Transparency

The PCLOB must review each of the above-mentioned topics—from minimization procedures to the fact that Section 702 serves as a general warrant. We urge PCLOB to go farther, however, and offer at least general legislative recommendations to cure these ills. Namely, the PCLOB can:

- Recommend the repeal of Section 702 of the Foreign Intelligence Surveillance Amendments Act.
- Ensure that a probable cause warrant must issue before U.S. persons' communications are collected regardless of any other procedures that may apply.
- Introduce and recommend individuality and particularity requirements into Section 702. This includes mandating certifications specify the target and the facilities the acquisition is intended to take place in. It could also include limiting targets to foreign powers or agents of a foreign power.
- Stop the "back door search" loophole. Mandate that even if U.S. person communications are obtained, intelligence agencies are not allowed to search the data in a way that will obtain U.S. person information, such as for any U.S. selector, unless a probable cause warrant is obtained.
- Recommend changes to the targeting procedures so that any collection pursuant to Section 702 is certain, or as close to certain as possible, that it will not collect any U.S. person data unless that U.S. person is the judicially approved target of a order.

- Narrow the definition of "foreign intelligence information."

- Ensure that innocent foreigners and their private data are not discriminated against under the law, including through the inclusion of non-U.S. persons in targeting and minimization reform. Section 702 must not violate international standards of human rights, either within the United States or extra-territorially, nor enable the bulk indiscriminate acquisition of innocent foreigners' data on U.S. soil or outside the US.

- Ensure that limitations consistent with international human rights law apply to U.S. collections whether they occur within or outside the United States.

Beyond the legislative fixes above, the Board should address the role of the FISA Court under Section 702, which is currently grossly inadequate in the Section 702 context. *Coolidge v. New Hampshire* stressed that judicial "scrutiny is intended to eliminate altogether searches not based on probable cause."[140] In the FISA context, judicial scrutiny must be heightened and expanded. Specifically,

- The FISA Court must determine there is probable cause or reasonable suspicion that the "about" communications searched will yield foreign intelligence information.

- The FISA Court must confirm that all of the collected communications exclusively concern a foreign power or agent of a foreign power.

- The FISA Court must review the search terms used pursuant to Section 702.

- The FISA Court must note with particularity the communications the acquisition seeks.

[140] *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

Much more must also be done outside of the statutory and judicial contexts. As detailed above, the American public—and legislators, especially those not on the intelligence committees—require more information to engage in a national dialogue about the government's surveillance programs. The PCLOB can increase transparency around the Section 702 programs, and specifically can help by focusing on documents describing government oversight and compliance related to the surveillance programs, and documents providing the legal rationales under which the programs operate. It can do so by working with the DOJ and NSA to publicly identify and name documents that should be declassified and released to the public and pushing for declassification of many of the materials sent to Congress. This could involve immediate disclosure of past documents, and the recommendation of setting up a produce for releasing future Congressional disclosures. If details can't be released, then the public needs recommendations for declassification. Even without agency agreement, the PCLOB could and should publish an index of such documents, perhaps identifying them by author, date, title, general subject matter, relevant statutory provision, and number of pages. Such information cannot be properly classified, and its release could help the public identify, and prioritize the release of, those documents most critical to the ongoing national debate.

Overall, the Board must serve as a guiding light for the larger public. In all the documents the Board reviews, it should make its own determination of the necessity of its classification level, and ask the executive to declassify the documents.

Conclusion

We look forward to the Section 702 report and are able to answer any further questions the Board may have.

Respectfully submitted,

ELECTRONIC FRONTIER FOUNDATION

Lee Tien

Senior Staff Attorney

Mark M. Jaycox

Legislative Analyst