KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

COMMENTS TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD REGARDING REFORMS TO SURVEILLANCE CONDUCTED PURSUANT TO SECTION 702 OF FISA

April 11, 2014

The Center for Democracy & Technology (CDT),[1] submits the following comments detailing the organization's recommended reforms to Section 702 of the Foreign Intelligence Surveillance Act (FISA) in connection with the Privacy and Civil Liberties Oversight Board's (PCLOB) ongoing assessment of Section 702. Congress charged PCLOB with analyzing actions the executive branch takes to protect the U.S. from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties, and that liberty concerns are appropriately considered in the development and implementation of anti-terrorism laws, regulations and policies.[2] These comments are intended to help PCLOB achieve those goals by (i) narrowing the scope of Section 702 surveillance, (ii) decreasing the likelihood that targets of such surveillance are Americans, and (iii) strengthening the minimization procedures designed to ensure that the statute is used as intended and not for other purposes.

Section 702 permits the government to compel communications service providers to assist with intelligence surveillance that targets non-U.S. persons (persons other than U.S. citizens and lawful permanent residents) reasonably believed to be abroad. Though it is defended as a necessary counterterrorism and national security power, Section 702 broadly authorizes collection, retention, and use of communications content unnecessary for national security and unrelated to counterterrorism. The overbroad use of Section 702 infringes upon the privacy rights of both U.S. persons, and of non-U.S. persons abroad, has already caused some damage to the American tech industry globally, and could cause much more.[3]

---

[1] The Center for Democracy & Technology is a non-profit public interest organization dedicated to keeping the Internet open, innovative and free. Among our priorities is preserving the balance between security and freedom. CDT's Vice President for Policy, James Dempsey, is a member of the PCLOB.

[2] 42 U.S.C. 2000ee.

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

I. Collection: Focusing section 702 surveillance on national security threats posed by targets abroad.

A. Narrowing the purposes for which Section 702 surveillance may be conducted.

Section 702 permits overbroad surveillance because the purposes for which the surveillance may be conducted are overly broad. To understand why this is so, it is necessary to understand FISA itself, and how procedures under Section 702, which was added to FISA in 2008, differ from those originally authorized by Congress in FISA for intelligence surveillance of targets in the U.S. thirty years before.

The FISA provisions that govern intelligence surveillance of targets in the U.S. permit the government to engage in electronic surveillance to collect "foreign intelligence information." For purposes of surveillance that targets a non-U.S. person, it is defined broadly as: (1) information that relates to the ability of the U.S. to protect against a hostile attack, espionage, sabotage or international terrorism or proliferation of weapons of mass destruction; or (2) information with respect to a foreign territory or foreign power (a foreign government, political party, or entity controlled by a foreign government, or a foreign terrorist organization) that relates to the security of the U.S. or to the conduct of U.S. foreign affairs.[4] When the government applies to the Foreign Intelligence Surveillance Court (FISC) for permission to conduct surveillance of targets in the U.S., it must certify that a significant purpose of the surveillance it will conduct is to collect foreign intelligence information.[5]

Because "foreign intelligence information" is defined so broadly, and because the FISC never actually rules on whether the significant purpose test is met, the purpose limitation that governs FISA surveillance of targets in the U.S. is easily met. FISA surveillance in the U.S. is instead effectively constrained by an additional requirement: the requirement that the government prove to the FISC that there is probable cause to believe the target of surveillance is a terrorist, spy, or other agent of a foreign power. Thus, Congress effectively constrained FISA surveillance of targets in the U.S. by permitting that surveillance to target only a narrow class of persons and entities.

For surveillance of people reasonably believed to be outside the U.S., Section 702 adopts the broad purpose requirement, but couples it with a broad class of surveillance targets. Section 702 is not constrained by the requirement that the target be an agent of a foreign power. Instead, the target need only be a non-U.S. person reasonably believed to be abroad. Effectively, Congress borrowed the broad purpose for FISA intelligence surveillance (collect "foreign intelligence information") and applied it to surveillance abroad without limiting the class of potential targets to "agents of a foreign power."

This has prompted concern globally that surveillance under Section 702 is broadly directed at individuals not suspected of wrongdoing, and could include targeting based at least in part on political activities. A peaceful protest at a U.S. base in Germany or a demonstration against rising food prices in India "relate to" U.S. foreign policy; non-U.S. persons involved in those

[4] 50 U.S.C. Section 1801(e).

[5] 50 U.S.C. 1881a (g)(2)(A)(v).

protests could be monitored under Section 702. A 2012 cloud computing report to the European Parliament included a finding that under Section 702, it is lawful in the U.S. to conduct purely political surveillance on non-U.S. persons' data stored by U.S. cloud companies.[6] Such actions raise serious human rights concerns. Further, fear of the mere possibly that this overbroad surveillance is occurring has significantly damaged the U.S. tech industry abroad.

The Presidential Policy Directive that President Obama issued on January 17, 2014 (PPD-28),[7] while remarkable in many ways, does not sufficiently address this problem. It prohibits the government from collecting signals intelligence for the purpose of suppressing or burdening criticism or dissent, but that prohibition permits the continued collection of information about such expressive activities merely because they are relevant to U.S. foreign affairs.

On the other hand, PPD-28 does include very important restrictions on the use of information collected in bulk for foreign intelligence purposes. They seem carefully thought out, and each permitted use of information collected in bulk would directly advance U.S. national security interests. These are among the most significant provisions of PPD-28, but they do not apply to Section 702 because it is not considered a bulk collection program.[8]

To address the problem of overbreadth in Section 702 collection, PCLOB should recommend that Section 702 surveillance be conducted only for carefully defined national security purposes. While there are different ways to do this, the best way would be to turn the "use restrictions" in PPD-28 that govern bulk collection into the permissible purposes for Section 702 surveillance.

This would require that collection pursuant to Section 702 only occur for purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests, (2) threats to the United States and its interests from terrorism, (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction, (4) cybersecurity threats, (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel, and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named above. This change would provide significant comfort to non-U.S. persons abroad who are concerned about the impact on their human rights that Section 702 surveillance would otherwise have. Indeed, it would increase the likelihood that Section 702 surveillance would meet human rights standards.

---

[6] Didier Bigo et al., European Parliament Directorate General for Internal Policies Policy Department C: Citizens' Rights and Constitutional Affairs, *Fighting cyber crime and protecting privacy in the cloud* (October 2012), available at http://www.bakchich.info/sites/bakchich.info/files/article_files/fisaa_0.pdf ("it is lawful in the US to conduct purely political surveillance on foreigners' data accessible in US Clouds").

[7] Presidential Policy Directive 28 (PPD-28): Signals Intelligence Activities (January 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

[8] During the PCLOB's March 19 public hearing on Section 702, government officials maintained that surveillance pursuant to Section 702 is not bulk collection and that this rule does not apply to such surveillance. *See generally*, *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (March 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf. While we believe that upstream collection raises legitimate questions about whether collection pursuant to Section 702 should be labeled as bulk collection, we put forward this recommendation based upon our assessment of the measure as effective policy, rather than a contention that the government is already obligated to do so in accordance PPD-28.

It would also focus Section 702 surveillance on true national security threats and still provide significant leeway to intelligence officials. We note that each time intelligence officials at the March 19 PCLOB hearings on Section 702 described the DNI certifications that identify the categories of foreign intelligence information that may be collected pursuant to Section 702, they mentioned one of these six categories of information.

Another way to limit to national security the purposes for collection pursuant to Section 702 would be to remove "the conduct of foreign affairs" as a basis for collection. If adopted, this reform would permit collection under Section 702 for the purpose of obtaining (1) information that relates to the ability of the U.S. to protect against a hostile attack, espionage, sabotage or international terrorism or proliferation of weapons of mass destruction, or (2) information with respect to a foreign territory or foreign power (a foreign government, political party, or entity controlled by a foreign government, or a foreign terrorist organization) that relates to the security of the U.S. Such a change would be consistent with the stated counterterrorism purpose of Section 702. Refining the purpose for which surveillance under Section 702 may be conducted would not prevent the Intelligence Community from gathering information related to the conduct of foreign affairs, but rather would merely remove the highly invasive practice of compelled company disclosure of communications content absent judicial review as a means of doing so.

B. The standard for designating a target should be raised to prevent improper targeting of U.S. persons.

Because of the constitutional implications of collecting the communications content of a person in the U.S. without a court order based on a finding of probable cause, PCLOB should recommend that Section 702 should be amended to require a high standard of certainty in the "foreignness" of a designated target.

Section 702 requires that surveillance not intentionally target U.S. persons or individuals located in the United States,[9] and it requires that the DNI issue Targeting Guidelines designed to ensure that surveillance is directed at persons reasonably believed to be outside the United States.[10] These targeting requirements are designed to focus Section 702 surveillance on non-U.S. persons abroad because targeting any U.S. person or person in the U.S. requires a more exacting FISC finding of probable cause that the person is an agent of a foreign power,[11] as compared to the much more relaxed standards for Section 702.

Last summer, reports resulting from disclosures by Edward Snowden created serious doubt as to whether existing restrictions on Section 702 surveillance effectively limit that surveillance to targeting non-U.S. persons abroad. According to a *Washington Post* report, a "supervisor must endorse [an NSA] analyst's 'reasonable belief,' *defined as 51 percent confidence*, that the

[9] 50 U.S.C. § 1881a(b).

[10] 50 U.S.C. § 1881a(d).

[11] 50 U.S.C. 1805(a)(2).

specified target is a foreign national who is overseas at the time of collection."[12] Such a "coin-flip" standard of 51 percent certainty would effectively render meaningless the "foreignness" requirements.

During PCLOB's March 19 public hearing on Section 702, NSA officials disputed the 51% certainty standard and stated that NSA internal training materials support using a "totality of circumstances" approach to determining foreignness.[13] However, the 51% standard, as described, involved the assessment of a variety of factors that add to or diminish the likelihood that a target is outside the U.S. Further, a "totality of circumstances" approach does not necessarily require that there be a high level of certainty that the target is a non-U.S. person abroad.

The Targeting Guidelines are likewise deficient. They vaguely require information "indicate" a potential target's location as foreign.[14] Further, the Guidelines lack standardized procedures for this determination other than a crosscheck against an apparent master list of U.S. person identifiers.[15] Finally, the Guidelines contain a presumption that every person reasonably believed to be located outside the U.S. is a non-U.S. person "in the absence of specific information" indicating otherwise.[16]

The low requirements for determining that a target is a non-U.S. person located outside the United States are insufficient to prevent improper targeting. Even if current internal procedures generate a high rate of accuracy in "foreignness" determinations, the government could move to a more lax system in the absence of legal restrictions that prevent it from doing so.

In order to ensure that Section 702 surveillance actually targets non-U.S. persons reasonably believed to be abroad, PCLOB should insist on a probable cause requirement. It should recommend that the Targeting Guidelines be required to ensure that surveillance under Section 702 be, "limited to targeting persons with respect to whom there is probable cause to believe that the target is a non-U.S. person located outside the United States." No court review of individual targeting decisions would be required – an analyst would make the probable cause determination.

---

[12] See, The Washington Post, *NSA slides explain the PRISM data-collection program* (June 6, 2013), available at http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ (emphasis added), hereafter, *Section 702 Slides*; *see also*, Barton Gellman and Laura Poitras, The Washington Post, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program* (June 6, 2013), *available at* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story_2.html ("Analysts who use the system from a Web portal at Fort Meade, Md., key in 'selectors,' or search terms, that are designed to produce at least 51 percent confidence in a target's 'foreignness.'").

[13] See, Statement of Rajesh De, *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (March 19, 2014), *available a*t http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf.

[14] *See generally*, *Procedures used by NSA to target non-US persons: Exhibit A – full document* (June 20, 2013), *available at* http://s3.documentcloud.org/documents/716633/exhibit-a.pdf.

[15] *See*, *Id.*

[16] *See*, *Id.*

C. Collection of communications "about" targets that are neither to nor from targets should be prohibited.

The Government takes the position that Section 702 permits it to collect not only communications that are to or from a foreign intelligence target, but also communications that are "about" the target because they mention an identifier associated with the target.[17] The practice directs the focus of surveillance away from suspected wrongdoers and permits the NSA to target communications between individuals with no link to national security investigations. Because this is inconsistent with the legislative history of the statute, and raises profound constitutional and operational problems, PCLOB should recommend that "about" collection be ended, and that Section 702 surveillance be limited to communications to and from targets.

Section 702 authorizes the government to target the communications of persons reasonably believed to be abroad, but it never defines the term "target." However, throughout Section 702, the term is used to refer to the targeting of an individual rather content of a communication.[18] Further, the entire congressional debate on Section 702 includes no reference to collecting communications "about" a foreign target, and significant debate about collecting communications to or from a target.[19]

To collect "about" communications, the NSA engages in "upstream" surveillance on the Internet backbone,[20] meaning "on fiber cables and infrastructure as data flows past,"[21] temporarily copying the content of the entire data stream so it can be searched for the same "selectors" used for the downstream or "PRISM" surveillance. As a result, the NSA has the capability to search any Internet communication going into or out of the U.S.[22] without particularized

---

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

[18] See generally, 50 U.S.C. 1881a(a).

[19] *See*, U.S. Senate, Committee on Intelligence. *FISA Sunset Extensions Act of 2012 Report* (S. Rpt. 112-174, Appendix), *available at* http://www.gpo.gov/fdsys/pkg/CRPT-112srpt174/pdf/CRPT-112srpt174.pdf ("Section 702 permits the FISC to approve surveillance *of terrorist suspects and other targets* who are non-U.S. persons outside the United States …. The FISC may approve surveillance *of these kinds of targets* when the Government needs the assistance of an electronic communications service provider") (emphasis added); *see also*, Senator Rockefeller, then Chair of the Senate Intelligence Committee, describing the necessity of minimization procedures for Americans' communication with a target, because surveillance is authorized only when a target is the party of a communication. Senator Rockefeller (WV). "FISA." Congressional Record 154 (June 26, 2008) p. S6181, *available at* http://tinyurl.com/FAASenate ("[Minimization] procedures protect the privacy of any Americans who might be *in contact with a foreign target*") (emphasis added).

[20] See, Statement of Rajesh De, *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (March 19, 2014), *available a*t http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf ("Upstream collection refers to collection from the … Internet backbone rather than Internet service providers").

[21] *See*, *Section 702 Slides, supra fn. 12.*

[22] The Guidelines require that any such collection of communications "about" a target be directed at a party outside the United States, essentially requiring that the communication include at least one foreign participant. *See*, *Procedures used by NSA to target non-US persons: Exhibit A – full document* (June 20, 2013), *available at* http://s3.documentcloud.org/documents/716633/exhibit-a.pdf.

intervention by a provider. Direct access creates direct opportunity for abuse, and should not be permitted to a military intelligence agency.

This dragnet scanning also results in the collection of "multi-communication transactions," (MCTs) which include tens of thousands wholly domestic communications each year.[23] The FISC required creation of new minimization rules for MCTs in 2011, but did not limit their collection.[24] The mass searching of communications content inside the United States, knowing that it the communications searched include tens of thousands of wholly domestic communications each year, raises profound constitutional questions.

Abandoning collection of communications "about" targets would remove any justification for upstream collection, eliminate the serious problems posed by direct government access to the Internet infrastructure, eliminate the collection of tens of thousands of wholly domestic communications in contravention of the statute, an make surveillance under Section 702 consistent with the congressional intent.

D. The FISC should be required to review surveillance directives.

Despite the importance of independent oversight, Section 702 requires no judicial authorization to target a particular person, and no judicial authorization of the surveillance directives sent to providers in connection with this surveillance. In order to enhance oversight in a feasible manner, Section 702 should be amended to require FISC review of surveillance directives.

Surveillance conducted in the U.S. pursuant to Section 702 is unique in its lack of judicial authorization to prevent abuse. A "selector," such as an email address or telephone number used by a surveillance target is chosen for surveillance when, according to the General Counsel of the DNI, an analyst has determined, "there is reason to believe the selector is relevant to a foreign intelligence purpose" that was described in a certification provided to the FISC.[25] Direct judicial review of that determination, particularly if the purpose of intelligence collection is limited to the six narrow national security purposes we suggest earlier, would help ensure that Section 702 surveillance is properly focused on threats and potential wrongdoers. However, given the current scale of the program – as of April 2013, there were over 117,000 targets[26] – such review may not be feasible.

In addition to providing lists of selectors on which surveillance is to be conducted, the Attorney General and Director of National Intelligence issue directives to electronic communications service providers requiring them to offer "all information, facilities or assistance necessary" to conduct surveillance regarding targets designated under Section 702. This provision does not limit the types of aid that may be required of providers and raises questions about the scope of

---

[23] *In Re DNI/AG 702(g)*, Docket Number 702(i)-11-01 (FISC October 3, 2011).

[24] *In re DNI/AG 702(g)*, Docket Number 702(i)-11-01 (FISC November 30, 2011).

[25] See, Statement of Robert Litt, *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (March 19, 2014), *available a*t http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf ("It is targeted collection based on selectors such as telephone numbers or email addresses where there's reason to believe that the selector is relevant to a foreign intelligence purpose").

[26] See, *Section 702 Slides*, *supra fn. 12*.

assistance that government agents seek.[27] Directives must be provided in writing and may require compliance immediately. No additional requirements or details regarding the nature of the directives are set forth in the statute. No directive has ever been declassified and made public. Providers may petition to the FISC to modify or strike a directive if it is not in compliance with law. However, directives currently do not receive any systematic judicial review.

In order to enhance oversight and accountability, PCLOB should recommend that a representative directive pertaining to upstream collection and a representative directive pertaining to downstream collection be declassified and released to the public, with any redactions strictly necessary to protect national security. In addition, the FISC should automatically review all directives to ensure that each directive: (1) is in compliance with FISA, other law, and the Constitution, (2) does not involve intentional targeting of Americans, including through "reverse targeting" of a non-U.S. person with the actual goal of monitoring a U.S. person, and (3) targets people reasonably believed to be outside the United States and prevents acquisitions of wholly domestic communications.

FISC access to the directives increases certainty that surveillance rules and guidelines are being followed. Further, it would discourage over-collection, an especially important issue in light of the FISC's acknowledgement that tens of thousands of "multi-communication transactions" containing wholly domestic communications are being gathered. Finally, it would provide added perspective for the FISC regarding how surveillance pursuant to Section 702 is conducted, enhancing the quality of its review of Targeting and Minimization Guidelines in the future. Because this reform would involve review rather than authorization, it is unlikely to significantly slow time-sensitive surveillance.

II. Retention and Use: New protections should be created regarding government's retention and use of information collected

Even with reasonable reforms that refine purpose and limit collection, the scale of surveillance conducted pursuant to Section 702 will continue to be immense. In order to adequately protect privacy of individuals whose communications are incidentally acquired and remove perverse incentives to engage in over-collection, PLCLOB should recommend additional measures limiting government's retention and use of information collected under this program. Specifically, the "backdoor search loophole" and the cryptoanalytic loophole should be closed, and the exception for retention and use of information regarding domestic criminal activity should be significantly narrowed.

A. Close the "backdoor search loophole."

The government is using Section 702, which was authorized to collect foreign intelligence information about non-U.S. persons abroad, to access information about U.S. persons in the United States without judicial oversight. PCLOB should recommend that this loophole be closed. The government should be required obtain judicial approval to search for the communications content of particular U.S. persons in the information that is obtained through Section 702 surveillance.

[27] 50 U.S.C. 1881a(h).

Once the NSA has collected communications content under Section 702, there are no restrictions in law – or in the Minimization Guidelines that govern Section 702 – that prevent the NSA from searching its databases for communications of U.S. persons that are inadvertently or incidentally acquired in the targeting of persons reasonably believed to be abroad. The government recently confirmed that it uses this "backdoor search loophole,"[28] deliberately gathering U.S. persons' communications absent judicial review.

When Congress enacted Section 702, it explicitly barred use of this broad authority to intentionally target U.S. persons for surveillance. To prohibit targeting of U.S. persons, then permit the NSA to search for U.S. persons' communications that are inadvertently or incidentally swept into NSA databases, violates the spirit of the law and undermines protections that were included. To guard against this abuse, PCLOB should recommend that, absent an emergency, a search of the database for an identifier of a U.S. person be prohibited unless the FISC has determined that there is probable cause that the U.S. person is a terrorist, spy, or other agent of a foreign power – the same legal standard required to authorize direct surveillance of that person under 50 USC Section 1805. While it may be unusual for the government to get a court order in order to search information it has already collected, it is unprecedented to permit the government to collect in the U.S. a huge trove of information without judicial authorization that includes the communications content of U.S. persons, and to permit those communications to be searched absent court review. This reform was recommended by the President's Review Group[29] and is included in the USA FREEDOM Act, legislation supported by over 160 members of Congress.[30]

B. Close the cryptanalysis loophole.

Minimization Guidelines for Section 702 surveillance generally permit retention of the product of that surveillance for five years if it contains foreign intelligence information, but they except Americans' encrypted communications from the 5-year limitation.[31] Instead, the Guidelines allow for unlimited retention and dissemination of communications that could aid cryptanalysis – recovering hidden or obfuscated meaning from encrypted or enciphered data, including "all communications that are enciphered or reasonably believed to contain secret meaning."[32]

---

[28] *See*, *Letter of Director of National Intelligence James Clapper to Senator Ron Wyden* (March 28, 2014), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1100298/unclassified-702-response.pdf.

[29] *See*, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (December 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("we recommend that … the government may not search the contents of communications acquired under section 702, or under any other authority covered by this recommendation, in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism").

[30] See, H.R. 3361, Sec. 301 and S. 1599, Sec. 301.

[31] Office of the Director of National Intelligence, *Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702, as amended* (August 21, 2013), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf, hereafter, *Minimization Guidelines*, Sec. 6(a)(1)(a).

[32] *Id.*

Average individuals, whether they know it or not, are rapidly increasing their use of encryption because the services they use increasingly encrypt communications by default. Though strong encryption was once a tool reserved for militaries, it is now commonly used in the commercial sector to protect personal data and prevent identity theft. Encrypting a communication in no way implies that it includes information relevant to a national security threat. In fact, the sensitive nature of information contained – such as inclusion of medical information or financial data – often provides a strong motivation to encrypt communications. The move toward encryption could, over time, make a five-year retention period the exception, rather than the rule, for Section 702 surveillance.

Closing the cryptanalysis loophole would not allow malicious use of encryption to override legitimate foreign intelligence needs. The government would still be permitted to retain encrypted communications collected in situations where there they are reasonably believed to contain foreign intelligence, however encryption could no longer serve as the sole basis for retaining a communication. Absent a justification that has not yet been publicly provided, PCLOB should recommend that this exception be deleted from the Minimization Guidelines.

C. Narrow the criminal activities loophole.

The Minimization Guidelines governing Section 702 surveillance permit the NSA to retain and share with domestic law enforcement any U.S. persons' communications that are reasonably believed to contain evidence of any crime that has been, is being, or is about to be committed, regardless of whether these communications contain foreign intelligence.[33] Reports indicate that the DEA has been initiating investigations using information provided by the Intelligence Community,[34] and that the NSA has provided communications between attorneys and their clients for use in criminal prosecutions,[35] conduct the Guidelines permit so long as the client is not under indictment.[36]

The retention and dissemination of U.S. persons' communications for law enforcement purposes permits an end run around the Fourth Amendment, which would bar the collection of those communications without a probable cause order from a court. It can involve information about crimes completely unrelated to FISA's foreign intelligence and national security purposes. Finally, the rule creates a perverse incentive to collect information under Section 702 in a way that increases the inadvertent collection of U.S. persons' communications without a warrant so they can be used to prosecute Americans. The President's Review Group was so disturbed by this practice that it recommended outlawing the use of information about U.S. persons obtained through Section 702 surveillance in any judicial proceeding against them.[37]

---

[33] *Minimization Guidelines*, *supra fn. 31,* Sec. 6(a)(3), Sec. 6(b)(8).

[34] John Shiffman and Kristina Cooke, Reuters, *Exclusive: U.S. directs agents to cover up program used to investigate Americans* (August 5, 2013), *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

[35] Nicholas Niarchos, The Nation, *Has the NSA Wiretapping Violated Attorney-Client Privilege?* (February 4, 2014), available at http://www.thenation.com/article/178225/has-nsa-wiretapping-violated-attorney-client-privilege#.

[36] *Minimization Guidelines*, *supra fn. 31,* Sec. 4.

[37] *See*, *Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies* (December 12, 2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf ("We recommend that, if the

In order to address the problem in a way that does not endanger Americans, communications collected under Section 702 should be disseminated to law enforcement only if such communications pertain to: (1) a crime of terrorism under 18 U.S.C. 2331 that has been, is being, or is about to be committed, (2) an imminent threat of death or serious bodily harm, or (3) a serious threat to minors, including sexual exploitation and threats to physical safety. These limitations are adapted from Section 704(g)(2) of S. 3414 (released January 19, 2012), the leading cybersecurity bill in the Senate in the last Congress. The authors of that legislation, knowing that cybersecurity activities would inadvertently uncover information about crimes and threats, drafted a similar standard after significant internal debate. PCLOB should recommend that the Minimization Guidelines be changed to adopt this standard for dissemination to law enforcement.

Conclusion

We appreciate the opportunity to present our views to PCLOB as it formulates its findings and recommendations to protect privacy and civil liberties in the context of surveillance activities pursuant to Section 702 of FISA. For more information, please contact CDT's Greg Nojeim, Director, Project on Freedom, Security & Technology, gnojeim@cdt.org; or CDT's Jake Laperruque, Fellow on Privacy, Surveillance and Security, jlaperruque@cdt.org, (202) 637-9800.

government legally intercepts a communication under section 702 …. any information about the United States person may not be used in evidence in any proceeding against that United States person").