KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

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

Statement for the Record of **Gregory T. Nojeim,**
Director, CDT's Project on Freedom, Security & Technology

At the Privacy and Civil Liberties Oversight Board Workshop Regarding

SURVEILLANCE PROGRAMS OPERATED PURSUANT TO PATRIOT ACT SECTION 215 AND FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702

July 9, 2013
(Submitted August 1, 2013)

Members of the Privacy and Civil Liberties Oversight Board:

The Center for Democracy & Technology (CDT),[1] submits this statement for the record summarizing the organization's testimony presented at the July 9th workshop on Section 215 of the Patriot Act and Section 702 of the Foreign Intelligence Surveillance Act (FISA). 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]

This statement first examines the mass gathering of telephony metadata under Section 215 of the PATRIOT Act, and the second examines the collection of metadata and content under Section 702 of the Foreign Intelligence Surveillance Act (FISA). Each section begins with a brief overview of the program and the statutory basis for the program. It then identifies the program's most serious problems and proposes solutions to those problems.

We ask that the PCLOB recommend an end to the Section 215 collection of telephony metadata because it is unlawful, may be unconstitutional, and unnecessarily encroaches on privacy. We call for increased transparency mechanisms for data collected under Section 702, including disclosure of the extent to which the communications of persons in the U.S. are collected, and further ask that the program be modified to make it consistent with internationally-recognized human rights norms.

[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.

NSA surveillance programs have strayed too far from the world envisaged by the Constitution – a world where an American does not have to worry about government surveillance unless there is evidence that he is up to no good. Although the Framers created the Fourth Amendment's protection from unlawful searches and seizures in the context of a physical home,[3] we now live our lives online. Private information that used to be found only in the home is now entrusted to third-party communications service providers. CDT urges PCLOB to account for technology's advance and to make findings and recommendations that are forward looking and that preserve individuals' reasonable expectations of privacy as those expectations evolve with technology.

I. NSA Surveillance Under Section 215 the PATRIOT Act

Classified documents leaked to *The Guardian*[4] have revealed that the Foreign Intelligence Surveillance Court (FISA Court) has interpreted Section 215 of the Patriot Act to permit the FBI to obtain orders that compel the largest telephone carriers in the U.S. (Verizon, AT&T, Sprint, and presumably others) to provide the NSA with records of phone calls made to, from and within the U.S. on a daily, ongoing basis. These millions of call records include: (i) numbers dialed to and from each telephone or cell phone; (ii) the time at which each call was made; (iii) the duration of each call; (iv) the number that uniquely identifies any cell phone (the International Mobile Station Equipment Identity number, or IMEI number); and (v) the number that identifies the SIM card used in the phone (the International Mobile Subscriber Identity number, or IMSI number). Combined, this information paints a clear, intimate picture of a person's daily life.[5]

The data are gathered in bulk, without any particularized suspicion about an individual, phone number or device. NSA analysts query the records not when the FISA Court or an independent magistrate determines such a search would be reasonable and lawful, but when the NSA analyst determines that, "there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization."[6] This standard appears in no statute. It requires no finding that the records queried pertain to a spy, terrorist, or other agent of a foreign power. A single "query" may consist of millions of phone numbers because each query can ask for records up to three "hops" from the phone number subject to analysis.[7] This record collection is inconsistent with Section 215, which requires "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation."[8]

[3] The Fourth Amendment can be attributed to both colonial experience as well as English traditions, such as the cherished maxim "Every man's house is his castle." In 1763, William Pitt made one of the most forceful expressions of this maxim in Parliament: "The poorest man may in his cottage bid defiance to all the force of the crown. It may be frail-its roof may shake-the wind may blow through it-the storm may enter, the rain may enter-but the King of England cannot enter." (http://www.gpo.gov/fdsys/pkg/GPO-CONAN-1992/pdf/GPO-CONAN-1992-10-5.pdf).

[4] *See e.g.*, Glenn Greenwald, "NSA collecting phone records of millions of Verizon customers daily," *The Guardian*, June 5, 2013. Available at: http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order.

[5] For more information, see: https://www.cdt.org/blogs/1706when-metadata-becomes-megadata-what-government-can-learn-metadata

[6] *New York Times*, "Comparing Two Surveillance Programs." June 7, 2013. Available at: http://www.nytimes.com/interactive/2013/06/07/us/comparing-two-secret-surveillance-programs.html.

[7] Thus, the analyst may examine whom a person contacted, who each of those contacts contacted, and who each of those contacts contacted. Statement of NSA Deputy Director John C. Inglis at House Judiciary Committee Hearing on Oversight of the Administration's Use of FISA Authorities, July 17, 2013, http://judiciary.house.gov/hearings/113th/hear_07172013.html.

[8] 50 U.S.C. 1861(b)(2)(A).

Prior to the PATRIOT Act, the government's ability to compel companies to turn over business records was limited in four ways.[9] First, only information that pertained to a terrorist, spy or other agent of a foreign power could be collected. Second, the records had to pertain to a particular person or entity. Third, only "business records" could be sought. Finally, the records could only be compelled from common carriers (such as airlines, trains and bus services), hotels, car rental agencies and physical storage facilities. The PATRIOT Act dramatically increased the government's authority with Section 215,[10] which authorizes orders to compel disclosure of any "tangible thing" (not just business records) from any person or entity (not just from travel and storage-related businesses). In addition, such "things" need not pertain to a suspected terrorist or spy; they need only pertain to an investigation. Section 215 is broad, but it is not so broad as to permit the telephone record collection the NSA has undertaken.

Problems and Recommendations

Problem 1: *The bulk collection of data is inconsistent with Section 215 because the records of every phone call made in the country are not relevant to an investigation.*

Under the guise of Section 215, the NSA has been collecting data on virtually all calls to, from and within the U.S. The only way such collection can be squared with Section 215 is if the "investigation" for which these records are sought is so broad that the telephone calls of every single person in the U.S. are "relevant." This is entirely too broad, and well beyond Congress's original intent when Section 215 was adopted.[11]

Because of the obvious privacy concerns when a military-intelligence agency collects records about virtually all phone calls made to, from and within the U.S., some have suggested that instead of permitting NSA to collect those records, telecoms be required to retain them for five years so NSA can later query them. Although the government's indiscriminate, mass retention of metadata is troubling, a government-subsidized data retention mandate imposed on the private sector would exacerbate, not alleviate, privacy concerns. Data minimization is a key privacy protection. If metadata are not retained, they cannot be hacked into or misused. In addition, a retention mandate that starts with phone records will almost certainly be extended to other information, including content. Finally, it would be extremely difficult to guard against mission creep. Metadata retained for national security purposes are accessible for criminal law enforcement purposes without a warrant when a law enforcement agent believes them relevant to a criminal investigation, and to civil litigants on a weak relevance standard. A mass data retention mandate is no step forward for privacy.

[9] Congress enacted Section 602 of the Intelligence Authorization Act in 1988. It created a very limited authority to obtain business records under FISA. Section 215 of the PATRIOT Act expanded that existing authority.

[10] 50 U.S.C. 1861(a).

[11] For example, at a June 13 hearing before the Senate Appropriations Committee this year, Sen. Jeff Merkley (D-OR) pulled out his Verizon-served smart phone and demanded that NSA Director Keith Alexander explain how Sen. Merkley's cell phone records could be relevant to an FBI investigation to prevent terrorism. Available at: http://thehill.com/video/senate/305139-merkley-waves-verizon-phone-demands-nsa-chief-share-grounds-for-seizing-data.

Recommendation: *PCLOB should recommend that the government cease its bulk collection of telephony metadata under Section 215, and should recommend that Section 215 be amended to require that the tangible things sought pertain to an agent of a foreign power.*

PCLOB should recommend that the FBI stop applying for orders from the FISA Court that result in disclosure to NSA of all of the phone call records of people who have no ties to terrorists. As outlined above, this collection is illegal under Section 215. It may also be unconstitutional under the reasoning of the Supreme Court in *U.S. v. Jones.* In that case, five justices of the Court signaled that long-term collection (28 days worth) of information about a person's location may be protected by the Fourth Amendment. By the reasoning of five concurring justices in that case, long-term collection (90 days worth) of information about a person's associations, as revealed through the phone calls they make and receive, would also be protected.

PCLOB should recommend that Congress amend Section 215 to require a finding of specific and articulable facts giving reasonable grounds to believe each piece of information sought pertains to spy, a terrorist or another agent of a foreign power. The government's self-imposed standard for querying the phone records database is quite different because those queries are made to obtain information that pertains to anyone, not a suspected terrorist or spy. Even permitting Section 215 to be used to obtain records of a person in contact with a person believed to be an agent of a foreign power would be a substantial improvement. Requiring a legitimate connection to an agent of a foreign power would not revert Section 215 orders back to pre-PATRIOT days: they could still be used to obtain any tangible thing (not just business records) from any entity (not just travel and storage-related entities).

Problem 2: *The Section 215 bulk metadata program involves prospective surveillance.*

The FBI uses Section 215 to compel disclosure of records that do not exist when an order is issued. Specifically, the Section 215 order published by *The Guardian* directs the provider to produce telephone metadata "on an ongoing daily basis"[12] for the duration of the order.

Such prospective surveillance is not sanctioned anywhere in Section 215. Instead, Congress gave the FBI the authority to conduct prospective surveillance of telephone metadata in the pen register statute, 50 USC Section 1842. Under this section, the FBI may obtain an order from the FISC authorizing the installation of a pen register (which records numbers dialed) or trap and trace device (which records the numbers of incoming calls) for the same kinds of investigations for which a Section 215 order may be used. However, Section 1842 orders may only be granted with a specified degree of particularity: The order must specify the attributes of the communications to which the order applies and the location of the telephone line if known, which means that the order must focus on a specific target (thus protecting everyone else).

Particularity is an element of every prospective surveillance authority in the U.S. code, whether criminal or intelligence-related.[13] Under the current Section 215 program, the government evades the particularity requirement by requiring daily disclosures from storage, allowing the NSA to obtain unparticularized information that could not have been obtained under the pen

[12] Verizon Court Order, pg. 2, available at: http://s3.documentcloud.org/documents/709012/verizon.pdf.

[13] *See, e.g.*, 18 USC 2518(1)(b)(particularity for criminal wiretaps), 18 USC 3123 (particularity for criminal pen register and trap and trace surveillance) and 50 USC 1804(a)(particularity for intelligence wiretaps).

register statute without a greater degree of specificity. Interpreting Section 215 to permit prospective surveillance is a very dangerous road down which to travel because similar statutes governing disclosure from storage could be re-interpreted to permit prospective surveillance without the additional protections that normally apply. For example, an order for the disclosure of the contents of records under 18 USC 2703(d) could be interpreted to require the communications service provider to disclose records "on an ongoing daily basis," effectively creating a wiretap without meeting the stringent requirements of the Wiretap Act. In the physical world, it could mean that a warrant to search a home could specify that the search would be conducted "on an ongoing daily basis," thus allowing law enforcement officials to return and search the targeted home at any given time, without having to obtain a new warrant.

Recommendation: *Prospective surveillance should be prohibited under Section 215.*

Prospective surveillance has no place in Section 215, as the government's authority to conduct ongoing surveillance is already provided for in the pen/trap statute. PCLOB should recommend that Congress bolster the particularity requirement in the pen/trap statute and add a proviso to make it clear that 50 USC Section 1842 is the exclusive means for the prospective collection of dialing, routing, addressing and signaling information for intelligence purposes. It should also recommend that Section 215 be amended to ensure that the "tangible things" sought must exist at the time the Section 215 order is served.

Problem 3: *Secrecy surrounding Section 215 orders permitted the surveillance to run amok.*

While some secrecy is necessary to some collection of information for national security purposes, too much secrecy can permit a program to spin out of control and undermine Congressional oversight. That has happened here.

Companies that receive a Section 215 order are gagged from informing their customers or, with limited exceptions, any one else, about it.[14] In other words, providers cannot even reveal that such orders exist, let alone the content of such orders. The government need not prove harm in order to impose such a gag. In addition, the FISA Court's legal opinions that show the basis for authorizing orders to reveal customer call records to the NSA are secret. Finally, government officials took advantage of the classified nature of intelligence collection under Section 215 by repeatedly misleading the public, and Congress, about the nature of this collection activity.[15]

Recommendation: *The government should be required to prove harm in order to gag a provider on which a Section 215 order is served, and providers should be permitted to disclose the number of Section 215 orders they receive*.

PCLOB should recommend that Congress revise Section 215 to require the government prove to the FISA Court that harm would result unless a provider was gagged from disclosing that the provider has received a Section 215 order. If the gag order is granted, it should expire by a certain date, but be renewable for additional periods upon a showing of harm. In addition,

[14] 50 USC 1861(d)(emphasis added).

[15] See, e.g., Center for Democracy & Technology, *NSA Spying Under Section 215 of the Patriot Act: Illegal, Overbroad, and Unnecessary* at p. 5, June 19, 2013, https://www.cdt.org/blogs/greg-nojeim/1906nsa-spying-under-section-215-patriot-act-illegal-overbroad-and-unnecessary.

PCLOB should recommend that the Administration change its policies and permit companies to report on an annual basis information about the number of Section 215 orders they have received and the number of accounts affected by such orders. The latter disclosure would give the public grounds for inquiry when there is a huge discrepancy between the number of orders issued and the number of accounts impacted. The next section recommends transparency of FISA Court opinions.

Problem 4: *The FISA Court provides inadequate protection of privacy and civil liberties in the telephony metadata program.*

Under the call records program, an intelligence agent, not the FISA Court, decides whether to access the telephone records based on whether or not the intelligence agent believes "there is a reasonable suspicion, based on specific facts, that the particular basis for the query is associated with a foreign terrorist organization." This so reduces the role of the FISA Court as to make its review insufficient when it comes to protecting individuals' civil liberties. Instead of the FISA Court determining whether the facts show that particular information is relevant to an investigation (as Section 215 requires explicitly), an intelligence agent makes a different determination based on a standard that an intelligence agency made up.

Last year, the FISA Court issued orders approving 1,789 full FISA applications and 212 applications for Section 215 orders. It sometimes writes opinions in connection with these orders that vastly expand government intelligence surveillance authorities,[16] but releases to the public almost none. It has created a body of secret common law with little to no public scrutiny.[17] The FISA Court hears only the government's side of each case, instead of hearing from both sides in an adversarial setting that would result in a full exposition of the civil liberties risks and better decision-making. Only the government can appeal a FISA Court decision.

Recommendation: *The FISA Court's opinions should be made public to the extent possible and the public's civil liberties interests should be represented in its important proceedings.*

PCLOB should recommend that significant legal interpretations of the FISA Court and the FISA Court of Review be made public, with classified information redacted to protect national security. In lieu of a redacted opinion, the government would be required to prepare a summary of the opinion that describes in general terms the context in which the matter arises, identifies with particularity each legal question that the opinion addressed and how it was resolved, describes the construction or interpretation of the law that makes the opinion significant, and indicates whether a prior decision of a FISA Court judge resolved the legal question differently. This process should be followed both for significant opinions already issued and for significant opinions issued going forward.

PCLOB should also recommend that the FISA Court's proceedings concerning significant legal interpretations benefit from the participation of an ombudsman who represents the civil liberties interests of people affected by the surveillance in question, including non-targets. In that very

[16] *New York Times*, "In Secret, Court Vastly Expands Powers of the NSA." July 6, 2013. Available at: http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=2&_r=1&hpw&pagewanted=all&.

[17] Id.

limited class of cases, the ombudsman could address: (i) whether the statute authorizes the government's proposed surveillance order; (ii) whether the Constitution permits the surveillance proposed; (iii) whether an order that is granted should be appealed to the FISA Court of Review because it is illegal or unconstitutional; and (iv) whether a summary of an opinion, or a redacted copy of the opinion, meets the statutory standard and recommend additional disclosures that would cause the redacted opinion or the summary thereof to meet the standard. With the approval of the FISA Court, the ombudsman would also solicit the participation of outside groups to submit amicus briefs to the FISA Court on significant legal questions before it.

II. NSA Surveillance Under Section 702 of FISA (the "PRISM" program)

Under Section 702 of the Foreign Intelligence Surveillance Act, the NSA has been compelling disclosure of content and metadata relating to emails, web chats, videos, images and other documents from at least nine large U.S. companies, including Google, Facebook, Microsoft and Apple.[18] The program, code-named "PRISM," is conducted under the FISA Amendments Act of 2008, which added Section 702 to FISA. This section permits the NSA to target the communications of non-U.S. persons who are reasonably believed to be located outside the United States in order to collect "foreign intelligence information."

The FISA Court does not approve any particular acquisition or any target. It does not authorize the surveillance. Instead, it approves targeting guidelines that are supposed to ensure that the surveillance focuses on non-U.S. persons reasonably believed to be outside the United States, and minimization procedures that are supposed to minimize the impact of this surveillance on U.S. persons.[19] The Director of National Intelligence has refused even to estimate the number of people in the U.S. whose communications have been collected under this program.

Service providers receive an annual written directive from the Attorney General and the Director of National Intelligence and "tasking orders" issued under that directive. The tasking orders, which can be narrow (e.g., a list of email addresses to and from which communications are to be provided to the NSA) or broad (e.g., a subject matter, such as the name of a terrorist organization) are dynamic. NSA analysts can change them rapidly, at least with respect to companies that participate in the PRISM program.

However, to the extent they are known, the circumstances surrounding this surveillance give cause for concern. Though the targeting guidelines do not say so, NSA analysts need only 51% confidence that the person being targeted is outside the United States. That would mean that roughly half of the targets are inside the U.S. – something Congress never intended in setting the "foreignness" requirements.[20] The NSA makes great use of information about U.S. persons and people in the U.S. that is collected "incidentally" in this surveillance program designed to target people abroad, and it makes great use of "inadvertently" collected communications of persons who turn out to be inside the United States.

[18] *Washington Post*, "NSA Slides Explain the PRISM Data-Collection Program." July 10, 2013. Available at: http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/.

[19] H.R. 6304 Sec. 702(d)(1) ; H.R. 6304 Sec. 702(e)(1).

[20] Id.

Problems and Recommendations

Problem 1: *Secrecy and misinformation surrounding Section 702 surveillance has left the public distrustful and confused.*

Classified slides published by the *Washington Post* stated that the government could tap directly into servers of the providers who participate in the PRISM program, but service providers vehemently denied this.[21] Nonetheless, according to subsequent reports, NSA analysts who use PRISM can search for and receive results from taskings directed to a provider's designated systems without further interaction with anyone working for the provider itself. Although government officials repeatedly assured the public that Section 702 surveillance cannot target Americans, they have failed to adequately convey that the government does, in fact, have great latitude when it comes to "incidentally" collecting Americans' communications. In addition, those government officials aver that domestic communications inadvertently collected under this program are "minimized," but they do not reveal that under the minimization guidelines, such communications are retained if they are reasonably believed to contain significant foreign intelligence information and are provided to FBI if they contain evidence of crime, and may be retained for five years. Finally, intelligence officials have led the public to believe that surveillance under the PRISM program is finely targeted while ignoring public information that there were, as of April 5, 2013, 117,675 people and entities targeted under the PRISM program and that upstream collection under Section 702 is conducted in bulk, and not on specific targets.

The lack of transparency regarding the government's interpretation and use of Section 702, and misleading and incomplete statements from government officials, feeds worldwide confusion and distrust of the program and the services of U.S. companies enlisted to carry it out. Moreover, secrecy has left the public unable to adequately evaluate the benefits of the program and the privacy costs of securing those benefits.

Recommendation: *PCLOB should push for declassification of much information about the use of Section 702, and for the government to release redacted opinions of the FISA Court that contain substantial interpretations of Section 702.*

Transparency with respect to the use of Section 702 should be near the top of the PCLOB's agenda. PCLOB should recommend that the government reveal more information about the breadth of Section 702 tasking orders, estimates of the number of people in the U.S. whose communications are "incidentally" collected under this program because they communicated with a person abroad, estimates of the number of people in the U.S., and the number of U.S. persons, whose communications are "inadvertently" collected under this program, and whether a 51% likelihood that a target is outside the United States is sufficient for that person or entity to be targeted for surveillance. As indicated above, PCLOB should recommend that an ombudsman be appointed to represent the privacy and civil liberties interests of persons whose communications may be collected under this program. The ombudsman would also seek disclosure of significant FISA Court opinions regarding Section 702 surveillance, after classified information has been redacted, and disclosure of summaries of such opinions when appropriate.

[21] *Washington Post*, "Misinformation on classified NSA programs includes statements by senior U.S. officials." Available at: http://www.washingtonpost.com/world/national-security/misinformation-on-classified-nsa-programs-includes-statements-by-senior-us-officials/2013/06/30/7b5103a2-e028-11e2-b2d4-ea6d8f477a01_story.html.

Problem 2: *The FISA Court's role in Section 702 surveillance is too limited to provide adequate protection.*

The FISA Court does not actually authorize the surveillance conducted under Section 702. Instead, it approves targeting and minimization procedures. The targeting procedures require that reports of non-compliance (such as the intentional targeting of a U.S. person abroad and intentional targeting of a person in the U.S.), and of over-collection by a company under a Section 702 order (such as targeting the communications of the wrong person) go to the Department of Justice and the Director of National Security, not to the FISA Court. When a judge issues a search warrant in the criminal context, the government agent conducting a search provides a "return" to the judge that reveals what was taken from the premises searched. Section 702 does not require the government to give the FISA Court returns on the surveillance conducted under Section 702, leaving the FISA Court less able to oversee this surveillance because it relies on voluntary disclosure of problems when they occur.

Recommendation: *PCLOB should recommend that Congress give the FISA Court more oversight over this surveillance. Instead of merely approving the procedures under which it is conducted, the FISA Court should decide whether the surveillance is conducted at all, including whether the surveillance proposed appears to be primarily for the purpose of collecting foreign intelligence information. It could be given authority to approve or reject "basket warrants" for the surveillance of a number of targets at once.*

In addition, PCLOB should recommend that the NSA provide the FISA Court with a return on surveillance authorized under a directive the Court has approved. The return would include an inventory of the number of communications collected, the number of communications collected that pertained to a U.S. person, the number that involved the communications of a person in the U.S., and any instances of inadvertently targeting the communications of a person in the U.S. or the communications of a U.S. person abroad. This would enable the FISA Court to assess whether or not the information collected was within the scope of Section 702.

Problem 3: *The minimization and targeting standards that govern Section 702 surveillance insufficiently protect the communications of U.S. persons and people in the U.S.*

Section 702 permits the government to target people "reasonably believed" to be non-U.S. persons outside the U.S. The targeting procedures that govern the surveillance must be "reasonably designed" to achieve that purpose.[22] The Targeting Guidelines indicate that "reasonable belief" assessment is based on the totality of the circumstances as reflected in information available to the analyst.[23] However, according to a report in the *Washington Post*, "reasonable belief" equals only 51% certainty.[24] As a result, though Section 702 requires that PRISM surveillance cannot purposefully target U.S. persons or persons reasonably believed to be located in the United States,[25] the test for determining whether the information sought will

[22] 50 USC 1881a.

[23] The Guardian, *Procedures used by NSA to target non-US persons: Exhibit A – full document* (June 20, 2013), p.1 *available at* http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.

[24] *Washington Post*, "U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program." 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.

[25] 50 USC 1881(b).

come from a person in the U.S. is not stringent; it applies coin-flip odds to a highly invasive, mass surveillance program.[26] Moreover, the targeting guidelines employ a "presumption of foreignness," which means that unless the NSA can determine that a target is a U.S. person, it may assume that any individual whose location is unknown is a non-U.S. person[27] who can be surveilled. The presumption could weaken NSA's commitment to determine the location of the target and whether it is a U.S. person.

The minimization procedures likewise are too lax. They permit examination of the content of purely domestic communications in some circumstances. "Inadvertently" collected purely domestic communications of U.S. persons are not destroyed unless they have been reviewed for evidence of crime or for foreign intelligence purposes. The minimization guidelines permit the NSA to turn over to the FBI any information collected for foreign intelligence purposes that shows evidence of any crime, regardless of the seriousness of the crime and even if the communications involve or are about a U.S. person. Finally, the minimization guidelines are not designed to protect the rights of non-U.S. persons; rather, they explicitly provide that foreign communications of or concerning non-U.S. persons can be retained, used and disseminated in any form consistent with law, regulation or policy.

Recommendation: *PCLOB should make inquiries about the targeting and minimization guidelines that govern intelligence surveillance under Section 702 and recommend changes.*

PCLOB should first determine whether NSA analysts conducting PRISM surveillance aim for only 51% likelihood that the target of surveillance is outside the U.S. If it confirms this goal, it should recommend raising the probability of "foreignness" substantially. Then it should investigate whether the presumption of "foreignness" should be retained because the NSA retains so much data on U.S. persons (which is troubling in and of itself) as to justify it. PCLOB should also recommend that the targeting guidelines be amended to require a report to the FISA Court of any noncompliance with the targeting procedures.

PCLOB should recommend that the minimization guidelines be amended to require destruction of inadvertently acquired domestic communications before their content is accessed. If a communication is recognized as domestic only after the contents are examined, and the contents reveal evidence of crime, PCLOB should recommend that the communication be provided to the FBI only if it contains evidence of a serious crime that involves threat to life or limb or serious damage to property.

Finally, PCLOB should recommend that the minimization guidelines require destruction of the untold number of communications of non-U.S. persons whose communications have nothing to do with terrorism or spying, but whose rights to privacy and free expression are plainly compromised by these progams. The United States should not be using its privileged position with respect to communications traffic to retain and put to unspecified uses the communications of people around the world, many of whom are speaking with their families or conducting

[26] For more information, see CDT, "We are the 49%." June 10, 2013. Available at: https://www.cdt.org/blogs/1006we-are-49.

[27] The Guardian, *Procedures used by NSA to target non-US persons: Exhibit A – full document* (June 20, 2013), *available at* http://www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.

business with American firms. At a minimum, those inadvertently collected communications should not be retained and put to other uses.

Problem 4: *The authorized purpose for Section 702 surveillance is overbroad and goes well beyond the anti-terrorism purpose that intelligence officials cite to justify the surveillance.*

Section 702 permits the government to compel communications service providers to assist with surveillance, involving both real time interception and disclosures from storage, [28] that targets people reasonably believed to be outside the U.S. if the U.S. Attorney General and the Director of National Intelligence certify that a "significant purpose" [29] of the surveillance it to collect "foreign intelligence information." The primary purpose of the surveillance can be wholly different and the definition of "foreign intelligence information" that can be sought is far too broad. When non-U.S. persons are targeted abroad, "foreign intelligence information" includes information with respect to a foreign territory, political party or government that relates to U.S. national security or the conduct of U.S. foreign affairs.[30] This definition covers information that relates to a wide range of activities that, in the United States, would be protected by the First Amendment, such as, for example, a protest at a U.S. base or even a protest about the price of gasoline. "Foreign intelligence information" also includes information that relates to a potential hostile act by a foreign power and sabotage, international terrorism and espionage.

While a broad "purpose" limitation in FISA may have made sense when only foreign powers and their agents in the U.S. were to be targeted on a finding of probable cause by the FISA Court, it makes less sense when the surveillance involves no such finding of a tie to a foreign power or agent and the FISA Court does not authorize the surveillance of the target.

Recommendation: *A narrower definition of the permissible purpose of the surveillance should be employed, and if one is already being used, it should be disclosed.*

PCLOB should recommend a narrowing of the permissible purposes of Section 702 surveillance and that the government make appropriate disclosures if it already effectively employs a narrower purpose limitation. The existing purpose limitation in Section 702 is cold comfort to people outside the U.S. because it is so broad. One option would be to limit the purpose of this surveillance to "foreign intelligence information" described in 50 USC 1801(e)(1). This would permit surveillance to protect against "[an] actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power." A national security purpose might also be included. However, the broad purpose of collecting information with respect to a foreign power or territory just because it relates to U.S. foreign affairs – and compelling U.S. providers to assist with that surveillance – is understandably troubling to people abroad who may be targeted.

[28] *See* European Parliament study, "Fighting Cyber Crime and Protecting Privacy in the Cloud" at 34. http://www.europarl.europa.eu/committees/en/studiesdownload.html?languageDocument=EN&file=79050.

[29] 50 U.S.C. Section 1881a(g)(2)(A)(v).

[30] 50 U.S.C. Section 1801(e).

In considering this recommendation, PCLOB should weigh the right to privacy codified in international human rights law. Article 17 of the International Covenant on Civil and Political Rights – to which the U.S. is a signatory – guarantees that no one shall be "subjected to arbitrary or unlawful interference with his privacy," and declares that, "everyone has the right to the protection of the law against such interference or attacks."[31] Article 8 of the European Convention on Human Rights guarantees that, "there shall be no interference by a public authority" with respect to an individual's right to privacy unless it is "necessary in a democratic society in the interests of national security, public safety . . . or for protections of the rights and freedoms of others."[32] Limiting the authorized purpose for this surveillance would be consistent with U.S. human rights obligations.

Problem 5: *Section 702 surveillance poses a grave threat to the right to privacy of all persons.*[33]

As outlined above, section 702 surveillance infringes not only on the rights of Americans; it infringes on the rights of anyone who uses the Internet. World leaders are recognizing the need to ensure that these rights are preserved as technology evolves. Just last year, the United Nations' Human Rights Council affirmed that these "same rights that apply to people offline must also be protected online."[34] During the Council's current session, Special Rapporteur Frank La Rue voiced concern that inadequate protections and legal frameworks "create a fertile ground for arbitrary and unlawful infringements of the right to privacy in communications and, consequently, also threaten the protection of the right to freedom of opinion and expression."[35] The Special Rapporteur's report details how new technologies have enabled "simultaneous, invasive, targeted, and broad-scale surveillance (section 33)," but laws are not keeping up in a way that adequately protects the privacy that civilians have the right to enjoy.[36]

Section 702 surveillance could provoke several unintended consequences.[37] From an economic standpoint, users abroad increasingly believe that U.S.-based Internet services have a privacy

[31] Article 17, International Covenant on Civil and Political Rights. Available at: http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx. Though the United States has signed the ICCPR, it has not yet ratified it. Article 2 of the ICCPR binds states to abide by the ICCPR with respect to individuals within the state's territory or subject to the state's jurisdiction. Interpreting that clause to put U.S. conduct within its own borders that denies or respects the human right to privacy of people outside the U.S. would be inappropriate in this surveillance context, where control over territory is not necessary to securing the privacy right at stake, and effective control over the means of communication is.

[32] Article 8, European Convention on Human Rights. Available at: http://www.echr.coe.int/Documents/Convention_ENG.pdf.

[33] For more information, see CDT, "It's Not Just About US: How the NSA Threatens Human Rights Internationally." June 12, 2013. Available at: https://www.cdt.org/blogs/1206it%E2%80%99s-not-just-about-us-how-nsa-threatens-human-rights-internationally.

[34] Human Rights Council Resolution 20/8, available at: http://daccess-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf?OpenElement.

[35] Human Rights Council, 23d Session, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue." April 17, 2013. Available at: http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[36] Id.

[37] *See* CNN.Com, "Why NSA Spying Scares the World." June 12, 2013. Available at: http://www.cnn.com/2013/06/12/opinion/deibert-nsa-surveillance/.

disadvantage and they may use alternative domestic services.[38] U.S. cloud computing services are already suffering from this trend because U.S. law enforcement officials do not need a warrant to gain access to much content stored with third parties.[39] In addition, many autocratic regimes may use Section 702 surveillance and PRISM as an excuse for adopting more stringent state controls over the Internet under the guise of national security. This undermines a key U.S. foreign policy goal: to further global Internet freedom.

Recommendation: *PCLOB's findings and recommendations must account for the fundamental human right to privacy enjoyed by people outside the U.S.*

CDT urges PCLOB to view the problems associated with the NSA's broad-sweeping Section 702 surveillance program not only through the eyes of Americans, but from the perspective of the international community as well. In addition to recommending the strengthening of the purpose limitation that governs this surveillance, PCLOB should call for a world-wide dialogue about strengthening the standards for intelligence and criminal surveillance in all countries.

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 NSA's surveillance programs that threaten both. We look forward to further collaboration with you. For more information, please contact CDT's Greg Nojeim, Director, Project on Freedom, Security & Technology, gnojeim@cdt.org; 202/637-9800.

[38] For example, Daniel Castro at the Information Technology and Innovation Forum warns that the companies named in the NSA slides that describe the PRISM program are suffering reputational harm and that "U.S. industries are facing increased threat of a global backlash from customers who may choose to flee to foreign competitors who are perceived, rightly or wrongly, as keeping data safe from government monitoring." Daniel Castro, *The Hill's Congress Blog,* Digital trade in a post-PRISM world, July 24, 2013, http://thehill.com/blogs/congress-blog/technology/312887-digital-trade-in-a-post-prism-world.

[39] *See,* 18 U.S.C. Section 2703.