Stanford Law School

Center for Internet and Society

Crown Quadrangle
559 Nathan Abbott Way
Stanford, CA 94305-8610
Tel 650 723-5205
Fax 650 723-4426
cyberlaw.stanford.edu

Comment on PCLOB-2013-0005-0073
to the Privacy and Civil Liberties Oversight Board
related to the March 19, 2014, hearing regarding surveillance conducted under Section 702 of the Foreign Intelligence Surveillance Act.

By Jennifer Stisa Granick, Director of Civil Liberties, Stanford Center for Internet and Society

April 11, 2014

Dear Members:

I want to thank the Privacy and Civil Liberties Oversight Board (PCLOB) for its public hearings on section 702 of the FISA Amendments Act and for the opportunity to comment regarding those hearings.

I am the Director of Civil Liberties at the Stanford Center for Internet and Society. I practice, speak, write, and teach about computer crime and security, electronic surveillance, and intermediary liability and its relationship to freedom of expression and innovation.

The Stanford Center for Internet and Society (CIS) is a public interest technology law and policy program at Stanford Law School and part of the Law, Science and Technology Program. CIS has been a pioneer in exploring issues at the intersection of law and new technology, examining how their interaction can either promote or harm public goods like free speech, innovation, privacy, public commons, diversity, and scientific inquiry. We conduct ongoing interdisciplinary study, analysis, research and discussion that enable and influence public policy in our focus areas, including government surveillance.

The public is beginning to learn what the NSA's current policies and practices are. But we—and the PCLOB—also need to know whether the rules we have in place are the right ones. The March 19, 2014 PCLOB hearing on section 702 raised and clarified many important issues about surveillance under that provision of law. However, there are additional important issues that the hearing did not fully address.

I hope these questions help the PCLOB to investigate these important matters thoroughly.

1. **Where NSA's internal practices respect privacy or other civil liberties concerns, can these practices be enshrined in public, enforceable statutes rather than codified as secret internal regulation or policy?**

As an overarching matter, it appears that NSA has successfully pushed the Foreign Intelligence Surveillance Court (FISC) for very broad interpretations of its statutory authority to collect information under both section 215 of the Patriot Act and section 702 of the FAA. In accordance with these interpretations, NSA has developed a powerful technological capacity for information collection and storage. Once the agency pulls in this vast amount of information, the Executive branch imposes complex (and differing) limitations on NSA, CIA, and FBI regarding the retention, use and dissemination of the information collected. To some extent, these regulations are overseen by the FISC, which approves formal minimization procedures. However, many of the policies and practices mentioned by intelligence officials at the last hearing are not codified in either law or in the minimization procedures. Rather, they are secret and discretionary. Because they lack robust oversight and the force of law, officials are likely unaccountable for disregarding or abandoning these policies

Many of these internal procedures are reassuring. For example, the declassified section 702 minimization procedures only proscribe procedures for protecting Attorney-Client communications when the communicant is talking to his attorney and under indictment. Yet, at the March 19th hearing, NSA General Counsel Rajesh De said that the NSA takes additional steps to limit collection of attorney client privileged materials even in the civil context. If that policy is material to the PCLOB's and the public's comfort with the collection, there ought to be a rule—publicly enforced, and persistent across personnel and Administration changes. Otherwise, at the very least, the NSA could change the rule—and many others—without anyone knowing.

In other words, where NSA internal policies protect civil liberties and are material in reassuring the PCLOB, these policies should migrate from internal practices to become affirmative, public, enforceable obligations. Can the PCLOB help identify these opportunities?

2. **What categories of 702 certifications have the Attorney General and the Director of National Intelligence obtained, and what are the limitations on the type or breadth of such certifications?**

At the hearing, Brad Weigmann, deputy assistant attorney general in the Justice Department's National Security Division, suggested that the FISC has issued 702 certifications including for "cyberthreats, terrorism, [and] proliferation" investigations.

Section 702, according to the FISC's interpretation, authorizes the NSA to collect communications that are to, from, or even *about* a non-U.S. foreign intelligence

target, so long as these communications are not wholly between U.S. persons. The definition of foreign intelligence information is quite broad, and includes information related to (A) the national defense or the security of the United States; as well as (B) the conduct of the foreign affairs of the United States. The statutory language can be interpreted to allow collection of what we might say about terrorist groups like al Qaeda—or matters of broader interest, like Iran, Germany, Wikileaks, Petrobras, the Institute of Physics at the Hebrew University of Jerusalem, UNICEF, Medicines du Monde, or any other entity that helps the U.S. government "understand economic systems and policies, and monitor anomalous economic activities".

Yet, Mr. Weigmann's testimony suggests that this is not how NSA is using section 702. What are the limits of appropriate 702 targets, and why? Do provisions of section 702 and/or the Fourth Amendment prevent the FISC from issuing certifications for whole countries or other troublingly broad categories of information? Does the government/FISC believe its ability to approve certifications is limited to those for which the purpose behind the surveillance is national security, or can the FISC approve certifications where the goal is foreign intelligence more generally?

As a specific example, can the FISC issue certifications for entire countries? Recent reports by Der Spiegel suggest that the FISC has issued far more than these three certifications, including ones specifying particular countries of interest, like Germany, Jordan, Morocco and others before and after these in the alphabet. The leaked document shows what appear to be court case numbers next to each country name:

For example, if the NSA could get a certification for "Germany" then phone numbers and email addresses for German officials would be selectors. Germans emailing their government, as well as Americans calling relatives overseas, could be subject to 702 collection.

Understanding the categories of certifications is an important window into whether and how regular persons' data gets into NSA databases, and whether and when it is kept. It would also greatly help the public understand how the FISC and the Administration are taking our constitutional rights to privacy into account under a statute that authorizes warrantless surveillance of our foreign communications.

3. How many of the section 702 collected communications are of or concerning U.S. persons?

So far, the public does not know exactly how many American communications NSA collects under section 702 because the agency has refused to provide that information, even in a classified setting.

The public and Congress need a better sense of how much section 702 impacts the communications privacy of Americans and innocent foreigners, however, before it can wisely reauthorize the FISA Amendments Act.

FISA court imposed minimization procedures could give the PCLOB metrics on how section 702 affects Americans. For example, analysts are required under the minimization procedures to identify multi-communication transactions (MCTs) for which the active user is a U.S. person. How many MCTs have analysts found which fit this description? Of course, that doesn't give us a full count of the number of communications within each MCT. But this number, which analysts are required to discover, could give Congress a much clearer idea of the overall effect the 702 program has on U.S. persons' domestic and one-end foreign communications.

Similarly, how many times and about how many different people has NSA disclosed section 702 data to FBI, DEA, IRS or other law enforcement agencies?

As Reuters reported last year, a division of the Drug Enforcement Administration called the Special Operations Division (SOD) funnels information from overseas NSA intercepts, domestic wiretaps, and informants to authorities nationwide to help them launch criminal investigations of Americans. The public currently has no information about the scope and frequency of information sharing between NSA and DEA or any other law enforcement agency. Surely these disclosures are documented and NSA can make a representative count of how many Americans are subject to criminal investigation each year because of 702 collected data.

4. What types of selectors does the NSA use to collect information under approved 702 certifications?

Once the FISC issues 702 certifications, the Attorney General and ODNI issue directives to companies for surveillance assistance. Pursuant to these directives, intelligence agencies provide selectors to service providers or task selectors upstream to collect foreign intelligence information.

NSA officials have defined "selectors" as terms they use to target accounts, and said that selectors are "things like email addresses and telephone numbers", and not keywords like terrorism or "generic names".

As a general rule, actual selectors are a legitimate secret. But the public and PCLOB have a right to know whether the categories of permissible selectors, and the internal NSA processes for approving selectors, is likely to include or exclude collection of regular people's private information.

a. Telephone numbers and email addresses: are they widely known?

Since terrorists seek to hide their activities, average people are less to know a foreign terrorist's email address or telephone number and to include it in their online communications. Limiting selectors to non-public information not widely known—for example a terrorist's phone number—helps screen regular people out of NSA collection. To the contrary, if "Germany" is a legitimate foreign intelligence target approved by the FISC, the email addresses and telephone numbers of German officials are more widely know, and using those selectors could pull into NSA databases German citizens' communications with their government as well as American calls and emails to friends and relatives abroad.

b. "Generic names"

A terrorist's name may not be "generic" but may regularly appear in the public's messages. For example, I could be talking to someone about Obama bin Laden. Names that are uncommon in the United States may be quite common in other countries. Names are often misspelled. And upstream surveillance pulls in communications "about" the foreign intelligence target. Thus, communications surveillance collection based on names is problematic.

c. Other potential selectors

Does NSA use other categories of selectors broader than email addresses or telephone numbers. For example, does NSA use IP addresses, or ranges of IP addresses? Many people can use the same IP address to connect to the Internet, so this category of selector may rope innocent people's data into the NSA coffers.

NSA's use of selectors may be a lot more sophisticated than a single data characteristic. Very simple data search techniques today use a combination of factors to narrow down collection. For example, NSA might use an Internet user's browser language, plus IP address to try to identify people of interest. The question is whether this combination of factors is sufficient to focus the NSA collection on appropriate foreign intelligence matters, while minimizing collection of extraneous information.

Seemingly innocuous and broad pieces of information, like zip code, gender, and data of birth alone do not identify people. However, Dr. Latanya Sweeney's research shows that in combination, these three pieces of information allow researchers to uniquely identify a large percentage of the sample population.[1] Similarly, the Electronic Frontier Foundation finds that people's web browser configurations -- characteristics like installed system fonts and HTTP header options--may be quite unique. Is there an internal process that calculates

[1] https://www.eff.org/deeplinks/2009/09/what-information-personally-identifiable

whether and how unique any NSA selector or combination of selectors are?[2] How does NSA determine if a selector is overbroad?

d. Selectors for persons, or more?

Section 702 authorizes "the targeting of **persons**". However, when private entities scan for cyberthreats, they do not look for particular attackers, or even know who they are. Rather, they look for spam, viruses, attack signatures, and the like. Assuming that in most cases, the government does not know who is behind cyberattacks, is the NSA nevertheless limited to selectors that would uniquely identify particular persons, or is the agency surveilling the Internet backbone for threat signatures, malware and other potential undesireable online conduct more broadly? What are the civil liberties implications of such surveillance?

For example, the recently filed criminal complaint against Dzhokhar Tsarnaev, the surviving suspect in the Boston Marathon Bombing, says that on an unknown date the suspect downloaded a copy of Inspire magazine (an English language online publication of al-Qaeda in the Arabian Peninsula) that contained instructions on how to make pressure cooker bombs.

How did the government learn about this download? One possibility is they found it on D. Tsarnaev's computer. Another possibility is that, in targeting Al-Qaeda, the NSA uses selectors that pull in information whenever anyone downloads articles from the non-U.S. based Inspire. In other words, the NSA could be tracking URLs associated with al-Qaeda, which necessarily means it is tracking peoples' reading.

Knowing the categories of NSA's allowable selectors is critical in understanding the extent to which the agency can and does collect information, including reading history, of regular U.S. persons.

5. Do intelligence agencies treat address books, buddy lists, stored documents, system backups and/or other electronic transmissions between an individual user's personal computer and the servers (i.e. where there is no human being on the received end of the transmission at the ISP) as "communications" for the purposes of minimization?

Under section 702, NSA collects information that contains its selectors from both Internet companies and from the network backbone. This information could include email or instant message communications, as well as computer backups, address books, contact lists, error messages, as well as other data. The thirteen-page section 702 minimization procedures which govern NSA's retention, use, and dissemination of information so collected are now declassified and public.

[2] https://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy

As I have written, the vast majority of those rules refer only to “communications”, and not more generally to collected “information”. Do backups, contact lists, address books, and other data fall outside the definition of “communications”? If so, intelligence agencies may apply the set of minimization rules—which have no protections against retention or use of Americans’ “information”—and call that minimization.

At the recent hearing, NSA officials were asked whether all information they collect under section 702 is minimized. The response was that all US person information is subject to minimization. It is not clear what that answer means, however. It could mean that all Americans’ information is treated as communications and minimized. It could mean that all Americans’ information is run through the minimization procedures, which nevertheless allow NSA to keep, use, and disseminate anything which is non-communications information.

Since it is still unclear what exactly NSA does with Americans' cloud backups, address books, and the like, PCLOB should explore this issue in more detail. Perhaps the question can best be phrased as whether all US person information obtained via section 702 is treated as “communications” for the purposes of minimization?

Given that the CIA and the FBI have different minimization procedures, which are not yet public, the same question applies to those agencies.

6. For what purpose or purposes may the intelligence agencies search 702 collected data for US person selectors?

The full scope of intelligence agencies’ authorization to search 702 collected data for US person selectors remains unclear.

For example, some NSA officials have said that the government can only use US person selectors to pull foreign intelligence information out of the 702 databases. However, at the recent hearing, Director of National Intelligence General Counsel Robert Litt said that “generally speaking”, NSA cannot search collected data with US person selectors “except for foreign intelligence purposes, or when there’s evidence of a crime, or so on and so forth.”

Does NSA search section 702 data using US person selectors for reasons other than foreign intelligence, for example for criminal investigations? If there needs to be a foreign intelligence justification, does foreign intelligence have to be *the* purpose of the search, a significant purpose of the search, or just one of many purposes? What if any restrictions are there on NSA conducting such searches for US persons?

Next, do these same restrictions apply when CIA or FBI seek to access, use or analyze section 702 collected data?

7. **May intelligence agencies search all 702 collected data for US person selectors?**

At the recent PCLOB hearing, NSA General Counsel De said that the agency only conducts searches of collected 702 data using US person identifiers on PRISM data and not on upstream data. However, a recent letter from Director of National Intelligence James Clapper letter does not make that distinction. It is unclear what in either Judge John Bates' 2011 FISC opinion or in the declassified section 702 minimization procedures would prevent US person identifiers from being used to search upstream data as opposed to PRISM data.

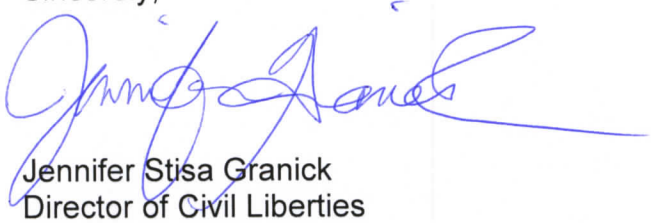
Does NSA or any other intelligence agency search upstream data for US person identifiers? If not, is that an internal policy, or a rule imposed by the FISC, or via minimization procedures?

8. **What is the national security value of authorizing warrantless surveillance of people who are not agents of foreign powers?**

Section 702 by its terms brings regular people under U.S. intelligence agencies' gaze by doing away with the requirement that the target of U.S. based surveillance be an agent of a foreign power. What would be the national security impact of stopping "about the target" collection? How could we measure the national security impact of reverting to the traditional FISA rule that the targets of surveillance be agents of foreign powers? Congress might want to weigh the impact of such a rule change against the business impact of having global customers of U.S. companies know they are more vulnerable to surveillance as a result of section 702.

Again, I want to thank the members of the PCLOB for their public service and for their attention to this critical matter. I hope my contributions assist the Board in conducting its important work.

Sincerely,



Jennifer Stisa Granick
Director of Civil Liberties