Correcting the Record on Section 702:
A Prerequisite for Meaningful Surveillance Reform

Jadzia Butler & Jennifer S. Granick

September 15, 2016

Part One of Three

Correcting the Record on Section 702:
A Prerequisite for Meaningful Surveillance Reform

The legal authority behind the controversial PRISM and Upstream surveillance programs used by the NSA to collect large swaths of private communications from leading Internet companies – Section 702 of the Foreign Intelligence Surveillance Act (FISA) – is scheduled to expire on December 31, 2017. In recent months, Congress began to review these programs to assess whether to renew, reform, or retire section 702. Unfortunately, it appears the debate has already been skewed by misconceptions about the true scope of surveillance conducted under the contentious provision. These misconceptions need to be addressed before they completely derail the unique opportunity at hand to have a well-informed discussion about much-needed reforms – reforms that could stabilize the shaky constitutional ground that current U.S. surveillance practices stand on, and reaffirm the U.S. government's commitment to fundamental human rights.

Specifically, the public debate has not sufficiently acknowledged the broad scope of section 702 collection, the volume of Americans' data collected, or the liberality of the post-collection procedures governing intelligence and law enforcement usage of the data. Hiding behind the counterterrorism justifications for section 702 collection is a broad surveillance program that sucks massive amounts

of private data – a sizeable chunk of which belongs to U.S. persons – into government databases. Once the government has collected this information, it may use it for a variety of purposes that may have nothing to do with foreign intelligence or national security, including criminal investigations. As we'll explore later, when the true scope of the section 702 program is understood, it is readily apparent that the collection of communications content under the program flies in the face of traditional notions of what constitutes a "reasonable" government search. Moreover, collection on this scale is inconsistent with international human rights norms that require surveillance to be necessary and proportionate. In short, the section 702 surveillance program is in desperate need of reform.

Section 702 Is Not a Counterterrorism Statute

Legislators weighing the value of section 702 talk almost exclusively about its use for counterterrorism. For example, the May 10th Senate Judiciary hearing on reauthorizing the FISA Amendments Act opened with references to the terrorist attacks in Paris and San Bernardino, and throughout the discussion senators and panelists emphasized the government's responsibility to keep people safe.[1] The implication was that if Americans' and innocent foreign civilians' private data is warrantlessly captured under section 702, it is only as a necessary byproduct of counterterrorism surveillance.

Despite what many lawmakers appear to believe, counterterrorism and national security are not the only permitted justifications for surveillance under

[1] *Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy and Civil Liberties: Hearing Before the S. Comm. On the Judiciary*, 114th Cong. (May 10, 2016), *available at*: http://www.judiciary.senate.gov/meetings/oversight-and-reauthorization-of-the-fisa-amendments-act-the-balance-between-national-security-privacy-and-civil-liberties.

section 702. Surveillance can occur for any foreign intelligence purpose,[2] including the collection of information about a foreign power or territory that is *related to* "the conduct of the foreign affairs of the United States."[3] Such broadly worded language permits surveillance far beyond that related to counterterrorism. For example, when protesters gather as part of the Arab Spring or to protest a government policy, the reasons for their complaints "relate" to U.S. foreign affairs. Information about other countries' economic policies, which could affect global markets, "relates" to U.S. foreign affairs, as well.[4] In 2015 alone, there were an estimated 94,368 targets under section 702, and the public does not know what fraction of those targets, many of whom communicate with Americans, were actually targeted for counterterrorism-related purposes.[5]

Moreover, foreign intelligence need not even be the *main* purpose of section 702 collection. Collection under section 702 is valid so long as a "significant purpose" of the collection is to obtain foreign intelligence information.[6] The primary purpose of the collection can be for another purpose entirely, such as investigating

---

[2] 50 U.S.C. § 1881a(g)(2)(A)(v).
[3] 50 U.S.C. § 1801(e)(2)(B) (emphasis added). For information concerning U.S. persons, the information must be "necessary to," rather than "relate to." *Id*.
[4] The NSA has been accused of using its powers for economic espionage. For example, documents leaked by Edward Snowden demonstrated that Brazilian oil company Petrobras was one of several targets of the NSA's Blackpearl program. *See* Jonathan Watts, "NSA accused of spying on Brazilian oil company Petrobras," THE GUARDIAN (Sept. 9, 2013), https://www.theguardian.com/world/2013/sep/09/nsa-spying-brazil-oil-petrobras. However, the U.S. draws a policy line between permissible surveillance related to innovation and economics, and impermissible surveillance and information sharing for the purposes of favoring U.S.-based companies. This distinction is often either lost on or disbelieved by other nations. *See* Jack Goldsmith, "The Precise (and Narrow) Limits on U.S. Economic Espionage," LAWFARE (March 23, 2015), https://www.lawfareblog.com/precise-and-narrow-limits-us-economic-espionage.
[5] Office of the Director of National intelligence, "Statistical Transparency Report Regarding Use of National Security Authorities," 5 (April 30, 2016) [hereinafter "ODNI 2015 Statistical Transparency Report"], *available at* https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf.
[6] 50 U.S.C. 1881a(g)(2)(A)(v).

alleged tax evasion. The "significant purpose" loophole could also enable the FBI to use section 702 to direct warrantless surveillance for criminal investigations (although only the NSA can make actual targeting decisions, the FBI is permitted to "nominate" surveillance targets of its own).[7]

Compounding the issue is the fact that decisions about whether or not a potential target is likely to communicate or receive such broadly defined "foreign intelligence information" are made with little guidance or limitation. The NSA's 2009 Targeting Procedures[8] contain a non-exhaustive list of factors that the NSA may consider when assessing whether a target is likely to have foreign intelligence information.[9] These factors include whether or not there is "reason to believe" the target is or has communicated with an individual "associated with" a foreign power or territory.[10] It is unclear what it means to be "associated with" a foreign power or territory when it comes to section 702 surveillance, but such language could be interpreted quite broadly.

Moreover, there is hardly any judicial oversight over section 702 targeting. FISA Court (FISC) judges have very little sway over the targeting procedures

---

[7] *See* Privacy and Civil Liberties Oversight Board (PCLOB), "Report on the Surveillance Programs Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act," 47 (July 2, 2014) [hereinafter "PCLOB Report"].

[8] We do not know precisely how the NSA Targeting Procedures have changed since 2009, because declassified updated procedures are not yet available. *See* PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (current as of July 2014), *available at*: https://www.dni.gov/files/documents/0928/NSA%20Section%20702%20Targeting%20Procedures.pdf.

[9] *See* PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (current as of July 2009) [Hereinafter "NSA Targeting Procedures"], *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716665/exhibit-a.pdf.

[10] *Id*.

themselves – they may only review them to see if they are "reasonably designed" to fit the minimum statutory requirements.[11] In addition, FISC judges do not participate in making individual targeting decisions – such decisions are entirely internal determinations made by the NSA. A predictable by-product of judicial disengagement from targeting decisions is that innocent people may be improperly spied on. The public recently learned that the NSA targeted a peaceful New Zealand pro-democracy activist under the PRISM surveillance program based on erroneous claims by the New Zealand government that the man was plotting violent attacks.[12] Had the NSA been required to provide some form of justification to a judge, the surveillance (in which the agency captured communications of people associated with a Fijian "thumbs up for democracy" campaign and turned them over to the New Zealand government) might not have happened.

Thus, when people talk about section 702 as if the only collection taking place under its auspices is for counterterrorism, that is wrong. Discussing the statute as if foreign intelligence must be the only, or even the primary, driver of its warrantless collection is also wrong. The statute allows warrantless content surveillance for a myriad of other purposes, so long as foreign intelligence collection is a "significant" purpose. Further, section 702 permits a very broad understanding of what type of person or entity is likely to communicate foreign intelligence

---

[11] Overall, the FISC's oversight role is actually quite limited. See 50 U.S.C. § 1881a(i)(3)(A), which states, "the Court *shall* enter an order approving the certification and the use, or continued use" of the collection of data under 702 so long as the statute's requirements are met (emphasis added). The only requirement with respect to the Targeting Procedures is that they be "reasonably designed" to ensure that acquisition is limited to overseas persons and to prevent the intentional acquisition of wholly domestic communications. *See* 50 U.S.C. § 1881a(i)(2)(B).

[12] Ryan Gallagher & Nicky Hager, "In Bungled Spying Operation, NSA Targeted Pro-Democracy Campaigner," THE INTERCEPT (Aug. 14, 2016), https://theintercept.com/2016/08/14/nsa-gcsb-prism-surveillance-fullman-fiji/.

information. Surveillance of conversations of foreigners that may be of foreign intelligence interest is thus neither necessary nor proportionate, as international human rights law requires.[13] The broad scope of targeting under the 702 program should be tremendously worrisome, even for those who do not find the rights of non-U.S. persons particularly compelling. The more foreigners deemed to potentially have foreign intelligence information, the more Americans communicating with those foreigners who may be incidentally spied on, as well. Moreover, in the 2015 *Schrems* decision, the Court of Justice for the European Union invalidated the E.U.-U.S. Safe Harbor agreement, the basis for data transfers between the European Union and the United States, largely because of U.S. surveillance programs such as section 702.[14] This ruling threatens the ongoing flow of data between the U.S. and Europe, potentially creating significant economic costs and legal risk for U.S.-based companies, such as Google and Facebook, that transfer data under the scheme.

Next week, we'll explore how broad the collection of Americans' communications is under Section 702. In part 3, we'll talk about the range of purposes beyond counterterrorism and national security for which section 702 data can be used.

---

[13] U.N. Human Rights Council, *The Right to Privacy in the Digital Age: Rep. of the Office of the U.S. High Comm'r for Human Rights*, U.N. Doc. A/HRC/27/37 (June 30, 2014), *available at*: http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf. *See also* International Principles on the Application of Human Rights to Communications Surveillance, *available at*: https://necessaryandproportionate.org/principles; *and* Case C-362/14, *Maximillian Schrems v. Data Protection Comm'r* .¶ 92 (Oct. 6, 2015), *available at*: http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

[14] *See* Sarah St. Vincent, "Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for U.S. Surveillance Reform," CDT.ORG (Oct. 26, 2015), https://cdt.org/blog/making-privacy-a-reality-the-safe-harbor-judgment-and-its-consequences-for-us-surveillance-reform/.