Correcting the Record on Section 702:
A Prerequisite for Meaningful Surveillance Reform (Part 2)

By Jennifer Granick and Jadzia Butler

Section 702 Programs Gather a Substantial Amount of U.S. Persons' Communications

Section 702 proponents emphasize the FISA statute's requirement that surveillance under the 702 provision only target non-U.S. persons located abroad.[1] They then push the seductive (but false) implication that this requirement means section 702 does not materially affect Americans. For example, during the 2012 FISA reauthorization debate, former House Intelligence Committee Chairman Mike Rogers (R-MI) acknowledged that the law might permit surveillance of Americans, but that this would happen "only very rarely."[2] In 2013, shortly after newspapers revealed details of the PRISM program, Director of National Intelligence James R. Clapper issued a statement reassuring the public that section 702 cannot be used to intentionally target any U.S. citizen or anyone located within the United States.[3] Director Clapper also emphasized that agencies conducting section 702 surveillance must follow procedures meant to minimize the acquisition, retention, and dissemination of incidentally acquired information about U.S. persons.[4]

Nevertheless, a recently declassified FISA Court (FISC) opinion from November 2015 confirmed what many people already suspected – section 702 actually sweeps up "substantial

[1] *See* 50 U.S.C. 1881a(a).
[2] Julian Sanchez, "Confusion in the House: Misunderstanding spying law, and inverting the lessons of 9/11," CATO INST. (Sept. 14, 2012) (citing Rep. Mike Rogers, "FISA Amendments Act Reauthorization Act of 2012 Floor Speech," Sept. 12, 2012), *available at*: http://www.cato.org/blog/confusion-house-misunderstanding-spying-law-inverting-lessons-911.
[3] James R. Clapper, "DNI Statement on Activities Authorized Under Section 702 of FISA," OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE (June 6, 2013), *available at*: https://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa.
[4] *Id*.

quantities" of information concerning U.S. persons.[5] In other words, the surveillance program subjects Americans to extensive, warrantless surveillance. This broad collection of communications may be politically palatable when Americans are talking to terrorists — the implication is that this "incidental" collection is minor and necessary for public safety. However, as explained above, foreign targets are not necessarily terrorism suspects, or wrongdoers of any kind. Section 702 contemplates surveillance targeting bureaucrats, scientists, aid workers – anyone of "foreign intelligence" interest.[6] Because the sanctioned surveillance topics are so broad, a vast number of people, including Americans, routinely have their communications swept up with no national security benefit attached.

First, Americans are surveilled when they talk to foreign targets.[7] The obvious case is international communications, where one of the parties is a target and the other is an American. However, this "incidental collection" is more extensive than one might think because of the very nature of the internet and the many different ways information is exchanged throughout it. For example, internet messages are commonly multi-user communications taking place in chat rooms and on social networks. If even one participant is foreign, communications from all the other people participating may be subject to section 702

[5] [Redacted], Docket [Redacted], at *27 n.25 (FISC Nov. 6, 2015) [hereinafter "Hogan Opinion"], *available at*: https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[6] As David Medine, former chairman of the PCLOB, said during the May 10th Senate Judiciary hearing, "this program targets anyone with foreign intelligence value. It could be a completely innocent businessman or anyone else out of the country who has that information." *See Hearing Before the S. Comm. On the Judiciary*, 114th Cong. (May 10, 2016), *supra* n.1.
[7] *See* PCLOB Report at 6.

collection.[8] In other words, a single target can justify surveillance of tens or hundreds of other people, some of which may be U.S. persons on U.S. soil.

Second, Americans' communications are collected as part of section 702's Upstream collection program. Under the program, the government "tasks" a given selector (such as an email address or phone number) in the stream of internet data flowing through particular network gateways (known as the "internet backbone"). If the stream of internet packets contains the selector, the Upstream program will acquire the entire "internet transaction" containing that selector. Some transactions only include one communication (Single Communications Transactions – SCT's), while others contain multiple discreet communications (Multiple Communications Transactions – MCT's). Because of the way the NSA conducts Upstream collection, if any communication within an SCT or MCT is "to," "from," or even "about"[9] a tasked selector, the entire transaction is collected. The collection of MCT's further removes the nexus between the communicants and the intended target because any communication that is embedded within a transaction that happens to include a communication that so much as *mentions* the targeted selector can get swept up. This includes wholly domestic communications.[10]

---

[8] For example, as the *Washington Post* has reported, if a target enters an online chat room, the NSA may collect the communications and identities of every person who posted in that chat room, as well as every person who simply "lurked" and read what other people wrote. *See* Barton Gellman, Julie Tate & Ashkan Soltani, "In NSA-intercepted data, those not targeted far outnumber the foreigners who are," WASH. POST (Aug. 8, 2013), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

[9] An "about" communication is a communication that merely references a tasked selector. These communications can be gathered under the Upstream program, regardless of the fact that the targeted selector does not belong to one of the actual communicants in the transaction. *See* PCLOB Report at 37. By collecting "about" communications, Upstream collection permits the search and seizure of communications content without a warrant for messages that are not even to or from a person of potential foreign intelligence value.

[10] *See* PCLOB Report at 41.

Changeable Minimization Procedures Allow U.S.-Person Information to be Retained, Disseminated, and Used

Congress anticipated that Americans' communications would get swept up through warrantless section 702 surveillance, so they required the adoption of "minimization procedures" as a way to control the retention, dissemination, and use of nonpublic, non-consenting U.S.-person information.[11] The statute requires the procedures to be consistent with the government's need to "obtain, produce, and disseminate" foreign intelligence information,[12] and to permit the retention and dissemination of evidence of any crime.[13] As a result, there are still many ways in which communications of or about innocent Americans can not only be collected under section 702, but can also remain in government databases for several years at a time and be used for a variety of purposes unrelated to national security or counterterrorism.

In response to recommendations made by the Privacy and Civil Liberties Oversight Board (PCLOB), the ODNI has made an effort to declassify the minimization procedures used by intelligence agencies as part of their section 702 surveillance practices. Most recently, in August 2016, the 2015 minimization procedures for the NSA, the CIA, the FBI, and the NCTC were partially declassified. Although declassifying the minimization procedures is a welcome step in the right direction, we still do not know when the rules apply and when the intelligence agencies may disregard them. For example, the 2015 minimization procedures for the NSA, the CIA, and the FBI state that "[n]othing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific

[11] 50 U.S.C. § 1801(h)(1).
[12] *Id*.
[13] 50 U.S.C. § 1801(h)(3).

constitutional, judicial or legislative mandates."[14] The apparent ability of agencies to deviate from the minimization procedures based on unspecified "mandates" undermines the anemic privacy safeguards those procedures contain. The FISC cannot ensure that the procedures meet either statutory or constitutional requirements in the face of such a vague exception. FISC Judge Thomas F. Hogan was aware of this problem when he nevertheless approved the NSA and the CIA procedures in November 2015.[15] Without fully explaining his conclusion, Judge Hogan concluded the vague language was not as problematic as it seemed, referring to informal conversations in which NSA and CIA officials said they planned to only use this exception to the minimization procedures sparingly.[16]

Beyond this worrisome language that appears to permit agencies to disregard their minimization procedures when they decide that doing so comports with some unspecified "mandate," there are additional flaws to the most recently declassified procedures that allow Americans' communications to be retained, searched, and used by a range of government agencies without a warrant or other judicial oversight. First, Americans' communications are generally fair game for retention, use, and dissemination if one participant at the other end of the communication is outside the United States. Such communications are deemed "foreign

---

[14] *See* MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 1 (2015) [hereinafter "NSA 2015 Minimization Procedures"], *available at*: https://www.dni.gov/files/documents/2015NSAMinimizationProcedures_Redacted.pdf; MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 6(g) (2015) [hereinafter "CIA 2015 Minimization Procedures"], *available at* https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf; MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § I.G (2015) [hereinafter "FBI 2015 Minimization Procedures"], *available at*: https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf.

[15] *See* Hogan Opinion at 22.

[16] *Id.* at 23.

communications" despite the fact that at least part of the communication involves a U.S. person.[17] Defenders of the section 702 program may point out that during such "incidental" collection, the foreign end of the communication has likely been identified as a target of interest for surveillance. As explained above, however, it can be alarmingly easy to become such a target under the section 702 statute and the policy guidelines that go with it. Moreover, in all other contexts Americans cannot be subject to incidental collection in the first place unless an investigator has obtained a search warrant or Title III interception order based on probable cause from a judge – a critical oversight mechanism that is absent in the section 702 context.[18]

Once these "foreign" communications get swept up, they can be retained in one or more databases at the NSA, the CIA, and the FBI for a number of years. They can remain in the NSA's database, for example, between two to five years, depending on whether they were gathered via the Upstream or PRISM collection program.[19] They may be retained longer under a variety of circumstances, such as when they are encrypted or may be used to help decrypt other encrypted communications.[20] Given the growing proportion of communications that are encrypted by default, this is one of the most significant loopholes to the retention limitations.[21]

---

[17] *See* NSA 2015 Minimization Procedures at § 1(e).
[18] *See, e.g.* 18 U.S.C. § 2518(3)(a) (requiring a judicial probable cause finding for a Title III wiretap order); 50 U.S.C. § 1805(a)(2) (requiring a judicial probable cause finding for a traditional FISA surveillance order); Berger v. New York, 388 U.S. 41 (1967) (invalidating a New York state law that permitted wiretaps without a probable cause finding by a judge).
[19] NSA 2015 Minimization Procedures at § 6(a)(1)(b).
[20] *Id.* at § 6(a)(1)(a); CIA 2015 Minimization Procedures at 3.c; FBI 2015 Minimization Procedures at III.G.5.
[21] *See, e.g.*, Cade Metz, "Forget Apple vs. the FBI: WhatsApp Just Switched On Encryption for a Billion People," WIRED (April 5, 2016), http://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

In addition, although the NSA may only pass U.S.-person information on to other government entities if the identity of the U.S. person is concealed, there are several exceptions to this rule – such as when the communication or information is "reasonably believed to contain evidence that a crime has been, is being, or is about to be committed."[22] Moreover, whether or not irrelevant U.S.-person information must be minimized largely depends on whether or not the communicant is "known" to be a U.S. person. The minimization procedures contain a presumption that people outside the U.S. or whose location is unknown are "foreign" until there is evidence demonstrating otherwise.[23] This presumption undermines assurances that U.S.-person information that does not meet the requirements for retention will be destroyed "upon recognition," since such assurances will only apply when that information is "known" to belong to or concern U.S. persons.[24] In practice, the chances of the agencies actually determining that a domestic communication is not the communication of a foreigner are slim, both because it is technologically difficult to determine for certain whether or not a communication belongs to or is about a U.S. person, as well as because agencies do not scrutinize each and every communication to make such a determination.[25]

Even if a communication is of or about a U.S. person and irrelevant to foreign intelligence or crime, the NSA minimization procedures only require destruction "at the earliest practicable point" before the retention limit when such communications are "clearly" not relevant to the authorized purpose of collection (such as the acquisition of foreign intelligence

[22] NSA 2015 Minimization Procedures at § 6(b)(8).
[23] *Id.* at § 2(k)(2): "A person known to be currently outside the U.S., or whose location is unknown, will not be treated as a U.S. person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a U.S. person." *See also* FBI 2015 Minimization Procedures at § I.D.
[24] *Id.* at § 3(c)(1).
[25] PCLOB Report at 128.

information) or evidence of a crime.[26] During the PCLOB's public hearing on section 702, the NSA's then-General Counsel admitted that it is often "difficult" to determine the foreign intelligence value of a particular piece of information at a given time,[27] and the PCLOB concluded that, in reality, the "destroyed upon recognition" requirement rarely happens.[28]

Finally, despite some improvements to the minimization procedures since the Edward Snowden leaks, there are still significant loopholes to the minimization procedures' purging requirements that allow communications that took place entirely within the United States to be retained, searched, and disseminated. For example the NSA's procedures require that all domestic communications (including, if applicable, the entire internet transaction in which such communications were contained) be destroyed upon recognition.[29] The NSA director, however, may waive this requirement on a communication-by-communication basis when he determines that one side of the domestic communication was properly targeted under section 702 and at least one of several circumstances apply, such as when the communication is "reasonably believed" to contain significant foreign intelligence information, evidence of a crime, or to be information that can be used for cryptanalytic purposes.[30] The CIA and the FBI 2015 minimization procedures contain similar exceptions, but they do not require that one side of

[26] NSA 2015 Minimization Procedures at § 3(b)(1).
[27] PCLOB PUBLIC HEARING REGARDING THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 46 (Mar. 19, 2014), *available at* https://www.pclob.gov/library/20140319-Transcript.pdf.
[28] PCLOB Report at 129.
[29] *See* NSA 2015 Minimization Procedures at §5. *But see* MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED, § 5 (2011) (allowing the retention of domestic communications upon reasonable belief that they contain foreign intelligence information or evidence of a crime), *available at*: https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.
[30] NSA 2015 Minimization Procedures at § 5(1)-(2).

the communication belong to a properly targeted individual.[31] It is troubling that there are so many situations in which communications between people on U.S. soil may be retained and used as part of a surveillance program purportedly geared towards foreign intelligence and national security. The fact that a very senior official at the intelligence agencies must approve of the retention on a case-by-case basis should help, but increased transparency in this area would help reassure the American public that this exception to the purging requirement is not being overused.

[31] CIA 2015 Minimization Procedures at § 8; FBI 2015 Minimization Procedures at § III.A.