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

Jadzia Butler & Jennifer S. Granick

September 2016

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 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

[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.

[2] 50 U.S.C. § 1881a(g)(2)(A)(v).

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 alleged tax evasion. The "significant purpose" loophole could also enable the FBI to use section 702 to direct warrantless

[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).

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 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

---

[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*.

[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

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 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

---

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/.

[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*

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.

END PART 1

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.[15] They then push the seductive (but false) implication that this requirement means section 702 does not materially

---

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/.

[15] *See* 50 U.S.C. 1881a(a).

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."[16] 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.[17] 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.[18]

Nevertheless, a recently declassified FISA Court (FISC) opinion from November 2015 confirmed what many people already suspected – section 702 actually sweeps up "substantial quantities" of information concerning U.S. persons.[19] 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 –

[16] 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.
[17] 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.
[18] *Id*.
[19] [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.

anyone of "foreign intelligence" interest.[20] 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.[21] 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 collection.[22] 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"

---

[20] 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.

[21] *See* PCLOB Report at 6.

[22] 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.

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"[23] 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.[24]

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.[25] The statute requires the procedures to be consistent with the government's need to "obtain, produce, and disseminate" foreign intelligence information,[26] and to permit the retention and dissemination of evidence of any crime.[27] As a result, there are still many ways in which communications of or about innocent Americans can

[23] 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.
[24] *See* PCLOB Report at 41.
[25] 50 U.S.C. § 1801(h)(1).
[26] *Id*.
[27] 50 U.S.C. § 1801(h)(3).

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 constitutional, judicial or legislative mandates."[28] 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

[28] *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.

and the CIA procedures in November 2015.[29] 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.[30]

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 communications" despite the fact that at least part of the communication involves a U.S. person.[31] 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

[29] *See* Hogan Opinion at 22.
[30] *Id.* at 23.
[31] *See* NSA 2015 Minimization Procedures at § 1(e).

probable cause from a judge – a critical oversight mechanism that is absent in the section 702 context.[32]

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.[33] 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.[34] Given the growing proportion of communications that are encrypted by default, this is one of the most significant loopholes to the retention limitations.[35]

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."[36] 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"

---

[32] *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).
[33] NSA 2015 Minimization Procedures at § 6(a)(1)(b).
[34] *Id.* at § 6(a)(1)(a); CIA 2015 Minimization Procedures at 3.c; FBI 2015 Minimization Procedures at III.G.5.
[35] *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/.
[36] NSA 2015 Minimization Procedures at § 6(b)(8).

until there is evidence demonstrating otherwise.[37] 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.[38] 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.[39]

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 information) or evidence of a crime.[40] 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,[41] and the PCLOB concluded that, in reality, the "destroyed upon recognition" requirement rarely happens.[42]

---

[37] *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.

[38] *Id.* at § 3(c)(1).

[39] PCLOB Report at 128.

[40] NSA 2015 Minimization Procedures at § 3(b)(1).

[41] 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.

[42] PCLOB Report at 129.

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.[43] 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.[44] The CIA and the FBI 2015 minimization procedures contain similar exceptions, but they do not require that one side of the communication belong to a properly targeted individual.[45] 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

[43] *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.

[44] NSA 2015 Minimization Procedures at § 5(1)-(2).

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

would help reassure the American public that this exception to the purging requirement is not being overused.

Warrantlessly Acquired 702 information Can Be Searched and Used for Non-Foreign Intelligence Purposes

The government can, and regularly does, search through its massive databases of content and metadata gathered under section 702 for information about U.S. persons. Such searches are often referred to as the "backdoor search loophole," because they enable the government to access information that would otherwise be unavailable without a warrant or similar probable cause finding. The NSA and the CIA minimization procedures now require analysts to create a "statement of facts showing that a query is reasonably likely to return foreign intelligence information"[46] before searching section 702 data for U.S.-person information, but the procedures do not require that foreign intelligence be the *purpose* of conducting the search. Moreover, this restriction does not pertain to the FBI, whose agents can query 702-acquired data for U.S.-person information as part of routine criminal investigations.[47]

[46] A new policy announced by the administration in February 2015 required a "written statement" of facts. *See* "New Privacy Protections for Information Collected Under Section 702," IC ON THE RECORD (Feb. 3, 2015), https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties. The newly-declassified 2015 minimization procedures (which were approved in July 2015) merely require a "statement of facts," without specifying that a written version is required. *See* NSA 2015 Minimization Procedures § 3(b)(5); CIA 2015 Minimization Procedures § 4. However, in order to comply with the DOJ and ODNI's oversight requirements, the NSA must submit a list of all U.S.-person identifiers approved to be used to query section 702 data, along with information detailing why those identifiers are reasonably likely to return foreign intelligence information. The CIA must submit a list of every section 702 query using a U.S.-person identifier, as well as a "contemporaneously written" justification regarding why those identifiers were reasonably likely to return foreign intelligence information. *See* "Release of a Summary of DOJ and ODNI Oversight of Section 702," IC ON THE RECORD 3-4 (released Aug. 11, 2016), *available at* https://icontherecord.tumblr.com/post/148796781888/release-of-a-summary-of-doj-and-odni-oversight-of.

[47] FBI 2015 Minimization Procedures at § III.D.

The FBI can even search section 702 data for U.S.-person identifiers in order to *initiate* an investigation – without a suspicion of wrongdoing, never mind probable cause.[48]

Even unauthorized FBI agents can conduct warrantless and suspicionless fishing expeditions through section 702 data for criminal conduct and thereby gain access to private information about Americans. According to the FBI's minimization procedures, the FBI does not consider a search a "query" if the agent conducting the search does not immediately see responsive data containing U.S.-person information – either because they are not authorized to access section 702-acquired data or because no section 702-acquired data was responsive to their query.[49] Unfortunately, the inability to see 702-acquired information immediately after a query does not prevent unauthorized agents from easily gaining access to it: upon notification that some results from their query contain section 702 information, the procedures allow unauthorized agents to simply ask an authorized person to give them access once that authorized person determines the information "reasonably appears" to be foreign intelligence or evidence of a crime.[50] Worse, if it is unclear to the authorized person whether or not the 702 information may contain foreign intelligence or evidence of a crime, the unauthorized agent can view the information and make that determination *himself*.[51]

With such a huge repository of data, government agents have the capacity to learn whether individuals have engaged in particularly "sensitive" activities, which the FBI's minimization procedures define as including, among other things, religious activities, political

[48] *Id.* at n.3 ("Examples of such queries include, but are not limited to . . . queries conducted by FBI personnel in making an initial decision to open an assessment concerning . . . the prevention of or protection against a Federal crime.").
[49] FBI 2015 Minimization Procedures at § III.D.
[50] Hogan opinion at *29. This provision appears in footnote four of the FBI 2015 Minimization Procedures, but that footnote remains classified.
[51] *Id.*

activities, activities involving the press or other media, sexual activities, and medical, psychiatric, or psychotherapeutic activities.[52] If the sensitive information returned "reasonably appears" to be foreign intelligence information or evidence of a crime, that information may be retained, processed, and disseminated in the same manner as all other "non-sensitive" information.[53]

The public has no idea how often the FBI conducts backdoor searches because the FBI will not report this data.[54] However, the latest Statistical Transparency Report from the Office of the Director of National Intelligence shows that the backdoor search loophole is being used by the NSA and the CIA more than ever before: last year, there were 4,672 acknowledged backdoor search terms concerning a "known" U.S.-person – a 223% increase since 2013. [55]

In 2015, largely in response to the PCLOB's criticisms of the section 702 programs, the Office of the Director of National Intelligence announced that it would limit the introduction of section 702 information as evidence against U.S. persons to the prosecution of "serious" crimes.[56] However, this policy was not officially adopted into the FBI's 2015 minimization procedures, which means that the policy may change at any time and without the Attorney General's approval or FISC oversight. In addition, ODNI General Counsel Robert Litt's explanation of what constitutes a "serious" crime indicates that the government may interpret this term broadly. Along with a few somewhat more specific serious crimes such as human

[52] FBI 2015 Minimization Procedures at § III.C.2.
[53] *Id*.
[54] The FBI is excluded from the querying reporting requirement of the USA Freedom Act. *See* 50 U.S.C. § 1873(d)(2)(A).
[55] *Compare* ODNI 2015 Statistical Transparency Report at 5 *with* PCLOB Report at 57-58. That number does not include the number of FBI queries.
[56] *See* "ODNI's Signals Intelligence Reform 2015 Anniversary Report," IC ON THE RECORD, https://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

trafficking and "incapacitation or destruction of critical infrastructure," ODNI defines "serious crimes" to include cases "related to national security" and "transnational crimes."[57] Moreover, even if section 702 information cannot be used as evidence in court against a U.S. person for certain crimes, law enforcement can still use the information to find other evidence that *can* be used in court. In 2013, *Reuters* revealed that the U.S. Drug Enforcement Administration has engaged in a technique known as "parallel construction," in which they used intelligence-gathered data to launch criminal investigations.[58] Once they found enough information, they used traditional investigatory tools and legal processes to create a new discovery trail for the data, thereby obscuring the fact that foreign intelligence surveillance was the true source of the evidence.[59]

Thus, section 702 surveillance can be abused in ways that create an end-run around the Fourth Amendment. The vast scope of collection under Section 702 means that troves of sensitive information belonging to or concerning U.S. persons is warrantlessly gathered without any connection to crime or national security threats. This information is subsequently available to a wide variety of government actors for a variety of purposes, including suspicionless searches meant to ferret out criminal activity.

Conclusion: The Overbroad Scope of Section 702's Warrantless Collection Endangers Privacy and Civil Liberties Without Necessarily Contributing to National Security

[57] "ODNI General Counsel Robert Litt Speaks on Intelligence Surveillance Reform at the Brookings Institute," IC ON THE RECORD (Feb. 4, 2015), *available at*: http://icontherecord.tumblr.com/post/110632851413/odni-general-counsel-robert -litts-as-prepared.
[58] John Shiffman and Kristina Cooke, "Exclusive: U.S. directs agents to cover up program used to investigate Americans," REUTERS (Aug. 5, 2013), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805. *See also* U.S. Department of Justice Office of the Inspector General Report to Congress on Implementation of Section 1001 of the USA PATRIOT Act (Sept. 2015) (noting that "[t]he OIG is examining the DEA's use of administrative subpoenas to obtain broad collections of data or information. The review will address the . . . use of 'parallel construction' or other techniques to protect the confidentiality of these programs.").
[59] *Id.*

Once the scope of section 702 collection is truly understood, it is clear that communications gathered under its authority do not only belong to the terrorists hiding in caves who wish to do us harm. As the statute and the guidelines that go with it are written, section 702-acquired data could belong to scientists, protestors, advocates, journalists, diplomats, students, and other everyday civilians. Given the broad scope of section 702 collection, coupled with the fact that collected data may be kept for several years and searched without probable cause or even factual predicate, the surveillance statute comes with grave privacy and civil liberties concerns. Lawmakers considering the reauthorization of section 702 must understand that such privacy and civil liberties concerns are not merely a necessary by-product of national security efforts. Rather, they are an unnecessary symptom of a statute that has metastasized well beyond its purported goal. This must be resolved before section 702 surveillance is allowed to continue past its expiration date.