ISSUE BRIEF: SECTION 702 AND THE NEED FOR REASONABLE USE RESTRICTIONS

THE CONSTITUTION PROJECT

Safeguarding Liberty, Justice & the Rule of Law

Law Enforcement Use of Foreign Intelligence Surveillance Generally

In recent years—driven by technological advance and a heightened focus on counterterrorism—foreign intelligence surveillance has expanded dramatically. At the same time, the government removed "the Wall" (which stove piped information at various intelligence agencies) to support unprecedented information sharing. As a result, a vast amount private communications collected without a warrant pursuant to foreign intelligence authorities (notably Section 702 of the Foreign Intelligence Surveillance Act (FISA)) freely flow to law enforcement agencies, which can access and use them—again without a warrant—for law enforcement purposes completely unrelated to national security.

Ending the practice of stove piping and removing the Wall made sense towards the specific end of allowing intelligence agencies to properly understand and combat national security threats. But today's use of intelligence surveillance stretches far beyond that goal. The demise of the Wall led not only to the proper *sharing* of national security information between agencies, but also to a troublingly unrestricted *use* of military and intelligence agencies' power for domestic law enforcement.

We can reasonably limit law enforcement use of foreign intelligence surveillance without recreating the Wall. We need to establish a new middle-ground between the Wall and the status-quo; a "Chain Link Fence" that allows national security information to pass unobstructed between agencies, but blocks the full merger of domestic law enforcement with warrantless military and intelligence surveillance. This Chain Link Fence policy would not obstruct the necessary sharing of national security information with those who need it, but it would appropriately separate intelligence programs from the realm of domestic law enforcement.

Significant Problems With Law Enforcement Use of Information Obtained Via Sec. 702

Section 702 of FISA is an especially problematic expansion of foreign intelligence surveillance into a domestic law enforcement power. Section 702 permits surveillance absent any court authorization, and in the process monitors a significant number of Americans. This surveillance is authorized for broadly defined "foreign intelligence purposes," but it can be used for domestic law enforcement completely unrelated to national security. Existing restrictions on law enforcement uses are insufficient, and contain major loopholes.

Law enforcement can use Section 702 to initiate or aid investigations of minor crimes. The NSA can retain and disseminate Americans' communications that may contain *any* evidence of *any* crime.[1] A recently declassified FISA Court opinion revealed that the FBI can use Section 702 data to open or support investigations of any federal crime, including nonviolent offenses.[2] According to the FISA Court appointed Special Advocate, "There is no requirement that the matter be a serious one, nor that it have any relation to national security...[T]hese practices do not comply with....the Fourth Amendment."[3]

The FBI is encouraged to "poke around" Americans' emails absent any suspicion of wrongdoing. According to then-Privacy and Civil Liberties Oversight Board Chairman David Medine, even when "the FBI has *absolutely no suspicion of wrongdoing* … they're just sort of entitled to poke around [in Americans' communications obtained via Section 702] and see if something is going on."[4] The FBI's own Minimization Guidelines state that it is an "encouraged practice" for FBI personnel to search Section 702 data "in making an initial decision to open an assessment" of domestic criminal activity.[5]

---

[1] See, NSA 702 Minimization Guidelines, available at http://tinyurl.com/NSA702MinimizationRules.

[2] *November 2015 FISA Court Opinion*, available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

[3] *Id*.

[4] *See*, Senate Judiciary Committee Hearing, *Oversight and Reauthorization of the FISA Amendments Act* (May 10, 2016) (emphasis added).

[5] *See*, Jake Laperruque, Just Security, *Revelations From the Newly Declassified FISC Opinion on Section 702* (April 27, 2016), *available at* https://www.justsecurity.org/30776/revelations-newly-declassified-fisc-opinion-section-702/.

Existing limits on evidentiary use of Section 702 data are inadequate. In 2015, the Office of the Director of National Intelligence (ODNI) placed a limit on law enforcement use of Section 702 data, restricting use of such data as evidence in court to eight categories of crimes.[6] This limitation is inadequate in two respects: First, because it is not enshrined in statute or even in the FBI Minimization Guidelines, the restrictions could be removed secretly and unilaterally by ODNI at any time. Second, the eight categories of crimes need to be narrowed and better defined.

Further limiting "evidentiary" use of Section 702 data is necessary but not sufficient. Generally, information derived from warrantless surveillance is considered "fruit of the poisonous tree," and use of such surveillance by law enforcement in investigations is prohibited. The ODNI evidentiary use limit does not restrict such investigative use, creating a "fruit of the poisonous tree" loophole: law enforcement may still use Americans' communications collected via Section 702 to open or support investigations of *any* crime, so long as the information is not introduced as evidence in court proceedings.

Law enforcement use of foreign intelligence information is limited in other key areas. Presidential Policy Directive 28 limits use of data obtained via bulk collection under another foreign intelligence authority, Executive Order 12333, to six categories;[7] no law enforcement uses outside of those six categories is permitted. A similar restriction could prevent Section 702—which like EO 12333 is a foreign intelligence tool that lacks the judicial oversight required for domestic surveillance—from being co-opted for law enforcement.

Reasonable use restrictions would not excessively inhibit law enforcement. According to the FBI it is "extremely unlikely" that a query conducted in investigation of a non-national security crime would return 702 data,[8] thus the impact of use restrictions on law enforcement operations would be minimal, especially if some exceptions exist.

Reform Proposal Regarding Law Enforcement Use of Section 702 Data

As a general rule, law enforcement should be *required* to obtain a warrant before using Americans' private communications, and *prohibited* from using 702-derrived information that was obtained without a warrant. We recognize, though, that there may be appropriate, narrow exceptions to this rule. As such, we recommend amending Section 702 to restrict law enforcement uses of Section 702 to certain crimes. The 2015 ODNI use restrictions could serve as a baseline for such reforms; we recommend codifying this list with certain key changes:

1) *Include only specifically enumerated offenses*: The current ODNI rule does not define certain categories of exempt crimes, and also contains a non-exclusive exception for "criminal proceedings related to national security." While national security offenses such as terrorism and espionage could be reasonably exempt, the breadth of exceptions should be based on specifically enumerated offenses to provide clarity and prevent overreach and inconsistent application.
2) *Close the "fruit of the poisonous tree" loophole*: Limiting evidentiary use but permitting investigative use continues to allow foreign intelligence surveillance, which is *not* conducted pursuant to tradition Fourth Amendment safeguards, to circumvent constitutional limits on domestic surveillance. While this loophole is in place, law enforcement can still use Section 702 information to target any American absent suspicion of wrongdoing.
3) *Narrow the list of permitted uses*: While the ODNI evidentiary use rule is generally limited to serious threats to life and national security, some currently permissible uses are beyond the foreign intelligence scope of Section 702 and do not relate to imminent threats. Congress should limit such uses.

---

[6] Specifically, crimes involving 1) death, 2) kidnapping, 3) substantial bodily harm, 4) conduct that constitutes a criminal offense that is a specified offense against a minor as defined in 42 USC 16911, 5) incapacitation or destruction of critical infrastructure as defined in 42 USC 5195c(e), 6) cybersecurity, 7) transnational crimes, and 8) human trafficking. Additionally use for "criminal proceedings related to national security" is permitted. See, https://icontherecord.tumblr.com/post/110099240063/video-odni-general-counsel-robert-litt-speaks-on.

[7] Specifically, such data can only be used for the purposes of detecting and countering: (1) espionage; (2) terrorism; (3) proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats. See, Presidential Policy Directive 28, Sec. 2, available at https://www.eff.org/files/2014/09/04/2014sigint.mem_.ppd_.rel_.pdf.

[8] *See*, The Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report-2.pdf, at 59-60.