ISSUE BRIEF: Reforming FISA Section 702

THE CONSTITUTION PROJECT
Safeguarding Liberty, Justice & the Rule of Law

Section 702 of FISA creates serious privacy and due process problems, and unnecessarily harms U.S. business interests. The law must be reformed before it sunsets at the end of 2017. This brief recommends how to do so while retaining Section 702's security value. Please contact Jake Laperruque (jlaperruque@constitutionproject.org; 202-580-6921) with any question or for additional information.

Background:

The 1978 Foreign Intelligence Surveillance Act ("FISA") created rules governing surveillance for foreign intelligence purposes, including a requirement that the government obtain individualized warrants from the FISA Court. After the 9/11 attacks, the government sought to rapidly increase surveillance of terrorist targets. The Bush Administration initially created the President's Surveillance Program, which authorized broad surveillance within the U.S. of *international* communications, without FISA Court approval. After the program was disclosed, Congress added Section 702 to FISA,[1] which permits warrantless targeting and monitoring—for foreign intelligence purposes—of *any* foreigner outside the U.S.

Congress intended Section 702 to be focused on and limited to national security. However, the explosion of global communications over the last decade—which resulted in more and more Americans' communications getting caught in Section 702's web—has created serious problems that Congress did not account for. First, Congress failed to guard against this warrantless national security tool being co-opted for domestic law enforcement purposes, in violation of the Fourth Amendment. Second, Congress did not limit Section 702 surveillance to suspected wrongdoers, a decision that increasingly harms American tech and communications businesses globally.

Section 702 surveillance goes far beyond suspected wrongdoers, and improperly impacts Americans:

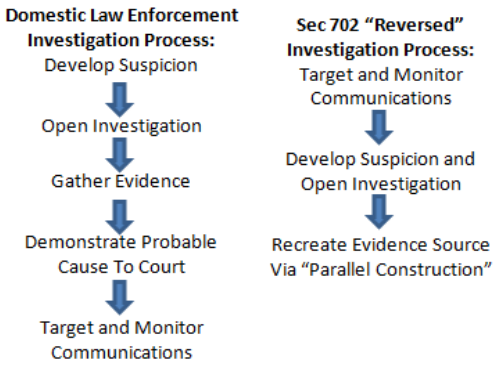
Section 702 permits surveillance of individuals in no way connected to suspected wrongdoing. The law authorizes targeting *any* foreigner located abroad for foreign intelligence purposes, which is defined broadly to include "information with respect to a foreign power or foreign territory that relates to the conduct of the foreign affairs of the United States."[2] This could permit surveillance of individuals on the basis of commonplace activities such as protesting outside a U.S. embassy, supporting a human rights group, or writing about international relations or global economics.

Casting such a wide net also endangers Americans, whose communications with wholly innocent individuals abroad can be captured "incidentally." Americans have long been subject to some degree of incidental collection through domestic surveillance by law enforcement, but *only* when they are communicating with someone suspected of criminal wrongdoing, as determined by a court. Requiring judicial approval for domestic surveillance also narrows the scope of incidental collection by limiting the means through which the surveillance can occur.[3] Section 702 lacks those protections. Americans merely communicating with someone abroad who is politically active, engaged in advocacy, or involved in research are within 702's reach.[4] Americans are also vulnerable to invasive surveillance tools like the NSA's "Upstream" program, which for years improperly collected tens of thousands of wholly domestic communications before the FISA Court was made aware that NSA surveillance methods went beyond authorized bounds.[5]

	Is incidental collection limited to:	
	Individuals communicating with suspected wrongdoers?	*Surveillance that received judicial authorization and corresponding limits?*
Domestic Incidental Collection, pursuant to the Wiretap Act	YES	YES
Incidental Collection, pursuant to Section 702 of FISA	NO	NO

[1] 50 U.S.C. 1881a
[2] 50 U.S.C. 1801(e)(2).
[3] Judicial authorization limits the scope of specific surveillance activities; orders authorized by the Wiretap Act - and all domestic incidental collection resulting from it - must describe and set limits on what communications facilities will be used, and how long surveillance will last. 18 U.S.C. 2518(4).
[4] *See*, Jake Laperruque, The Center for Democracy and Technology, *Why Average Internet Users Should Demand Significant Section 702 Reform* (July 22, 2014), *available at* https://cdt.org/blog/why-average-internet-users-should-demand-significant-section-702-reform/.
[5] *Bat0e\s October 2011 Opinion*, *available at* https://www.eff.org/files/filenode/fisc_opinion_-_unconstitutional_surveillance_0.pdf.

Section 702 undermines Americans' privacy and due process rights through the "Backdoor Search Loophole" and lack of use limits:



Section 702 was designed to target foreigners for national security purposes, but it created an end-run around the Fourth Amendment for law enforcement investigating and prosecuting low-level crimes. The "backdoor search loophole" allows the FBI to search for specific Americans' communications absent any suspicion of wrongdoing. The FBI can then use Section 702 data to open or support *any* federal criminal investigation.[6] This reverses the domestic criminal process, whereby law enforcement must demonstrate probable cause of a crime *before* targeting and monitoring communications. 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."[7] 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.[8] 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."[9]

Section 702 is unnecessarily endangering American communication and tech businesses globally:

Because Section 702 permits such a broad range of targets, foreign customers are increasingly avoiding American services that could be subject to Section 702 orders. American businesses have already felt the impact.[10] Furthermore, unless reformed, Section 702 is likely to cause the dissolution of the U.S.-EU safe harbor agreement for commercial exchange and use of data, which would have a catastrophic impact on American business.[11]

Six reforms that protect Americans' rights and interests and preserve Section 702's national security value:

1) ***Close the Backdoor Search Loophole:*** The government should be required to obtain a warrant prior to querying for Americans' communications, as was already required in similar contexts.[12] Carefully defined and limited emergency exceptions can be built in to accommodate the need for speed in cases of an imminent threat.
2) ***Include Reasonable Use Limits:*** Section 702 data should only be used for foreign intelligence, national security, and counterterrorism purposes. Domestic law enforcement should be prohibited from using Section 702 to investigate low-level and nonviolent crimes.
3) ***Refine the Purpose for Targeting:*** Targeting should be limited to Section 702's purpose: national security. Broader targeting rules put innocent foreigners at risk of surveillance, jeopardize the privacy of Americans with whom they communicate, and needlessly harm American communication and tech companies globally.
4) ***Prevent Inaccurate Surveillance Methods:*** The government should *only* be permitted to collect communications *to and from* Section 702 targets; currently the "Upstream" program scans and sometimes collects communications that do not include any surveillance targets.
5) ***Ensure Due Process Rights Are Protected:*** Defendants must be given notice when evidence derived from Section 702 is used, as is constitutionally required.
6) ***Increase Transparency:*** The government should increase transparency so Americans know more about how the law affects them, which will increase confidence in the Intelligence Community without revealing sources and methods.

---

[6] *November 2015 FISA Court Opinion*, available at https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.
[7] *See*, Senate Judiciary Committee Hearing, *Oversight and Reauthorization of the FISA Amendments Act* (May 10, 2016) (emphasis added).
[8] *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/.
[9] *Id*.
[10] *See*, Danielle Kehl et al, The Open Technology Institute, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity* (July 2014), *available at* https://na-production.s3.amazonaws.com/documents/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity.pdf.
[11] *See*, Faiza Patel, Just Security, *Safe Harbor and Reforming Section 702* (October 22, 2015), *available at* https://www.justsecurity.org/27009/safe-harbor-reforming-section-702/.
[12] For example, the now debunked bulk telephony metadata database required FISA Court authorization for queries after January 17, 2014, without inhibiting intelligence community essential capabilities.