THE SENATE INTELLIGENCE COMMITTEE 702 BILL IS A DOMESTIC SPYING BILL

Richard Burr has released his draft Section 702 bill.

Contrary to what you're reading about it not "reforming" 702, the SSCI bill makes dramatic changes to 702. Effectively, it makes 702 a domestic spying program.

The SSCI expands the kinds of criminal prosecutions with which it can use Section 702 data

It does so in Section 5, in what is cynically called "End Use Restriction," but which is in reality a vast expansion of the uses to which Section 702 data may be used (affirmatively codifying, effectively, a move the IC made in 2015). It permits the use of 702 data in any criminal proceeding that "Affects, involves, or is related to" the national security of the United States (which will include proceedings used to flip informants on top of whatever terrorism, proliferation, or espionage and hacking crimes that would more directly fall under national security) or involves,

- Death
- Kidnapping
- Serious bodily injury
- Specified offense against a minor

- Incapacitation or destruction of critical infrastructure (critical infrastructure can include even campgrounds!)
- Cybersecurity, including violations of CFAA
- Transnational crime, including transnational narcotics trafficking
- Human trafficking (which, especially dissociated from transnational crime, is often used as a ploy to prosecute prostitution; the government also includes assisting undocumented migration to be human trafficking)

This effectively gives affirmative approval to the list of crimes for which the IC can use 702 information laid out by Bob Litt in 2015 (in the wake of the 2014 approval).

Importantly, the bill *does not permit* judicial review on whether the determination that something "affects, involves, or is related to" national security. Meaning Attorney General Jeff Sessions could decide tomorrow that it can collect the Tor traffic of BLM or BDS activists, and no judge can rule that's an inappropriate use of a foreign intelligence program.

"So what?" you might ask, this is a foreign surveillance program. So what if they find evidence of child porn in the course of spying on designated foreign targets, and in the process turn it over to the FBI?

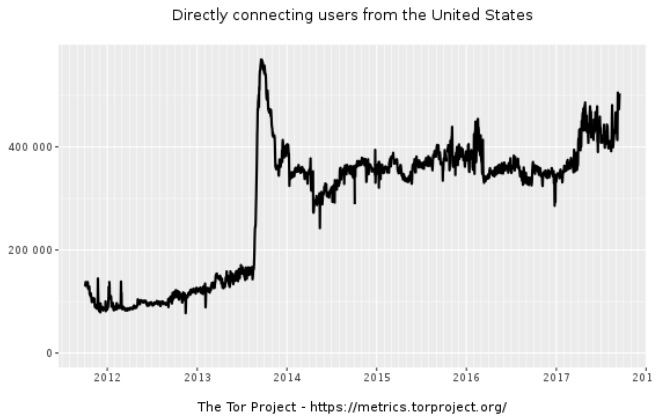
The reason this is a domestic spying program is because of two obscure parts of 702 precedent.

The 2014 exception permits NSA to collect Tor traffic — including the traffic of 430,000 Americans

First, there's the 2014 exception.

In 2014, the FISC approved an exception to the rule that the NSA must detask from a facility when it discovers that a US person was using it. I laid out the case that the facilities in question were VPNs (collected in the same way PRISM would be) and Tor (probably collected via upstream collection). I suggested then that it was informed speculation, but it was more than that: the 2014 exception is about Tor (though I haven't been able to confirm the technical details of it).

NSA is collecting Tor traffic, including the traffic of the 430,000 Americans each day who use Tor.



One way to understand how NSA gets away with this is to consider how the use of upstream surveillance with cybersecurity works. As was reported in 2015, NSA can use upstream for cybersecurity purposes, but only if that use is tied to known indicators of compromise of a foreign government hacking group.

On December 29 of last year, the Intelligence Community released a Joint Analysis Report on

the hack of the DNC that was considered — for cybersecurity purposes — an utter shitshow. Most confusing at the time was why the IC labeled 367 Tor exit nodes as Russian state hacker indicators of compromise.

But once you realize the NSA can collect on indicators of compromise that it has associated with a nation-state hacking group, and once you realize NSA can collect on Tor traffic under that 2014 exception, then it all begins to make sense. By declaring those nodes indicators of compromise of Russian state hackers, NSA got the ability to collect off of them.

NSA's minimization procedures permit it to retain domestic communications that are evidence of a crime

The FISC approved the 2014 exception based on the understanding that NSA would purge any domestic communications collected via the exception in post-tasking process. But NSA's minimization procedures permit the retention of domestic communications if the communication was properly targeted (under targeting procedures that include the 2014 exception) and the communication 1) includes significant foreign intelligence information, 2) the communication includes technical database information (which includes the use of encryption), 3) contains information pertaining to an imminent threat of serious harm to life or property OR,

> Such domestic communication does not contain foreign intelligence information but is reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed. Such domestic communication may be disseminated (including United States person identities) to appropriate law

> enforcement authorities, in accordance with 50 U.S.C. § 1806(b) and 1825(c), Executive Order No 12333, and, where applicable, the crimes reporting procedures set out in the August 1995 "Memorandum of Understanding: Reporting of Information Concerning Federal Crimes," or any successor document.

So they get the data via the 2014 exception permitting NSA to collect from Tor (and VPNs). And they keep it and hand it off to FBI via the exception on NSA's destruction requirements.

In other words, what Richard Burr's bill does is affirmatively approve the use of Section 702 to collect Tor traffic and use it to prosecute a range of crimes, some of them potentially quite minor.