

# IN ADVANCE OF USA FREEDOM AND CISA FIGHTS, PCLOB PRETENDS SECTION 702 DOESN'T HAVE A CYBER FUNCTION

In a piece for Salon, I note some of the weird silences in yesterday's PCLOB report, from things like the failure to give defendants notice (which I discussed yesterday) to the false claim that Targeting Procedures haven't been released (they have been – by Edward Snowden). One of the most troubling silences, however, pertains to cybersecurity.

That's especially true in one area where PCLOB inexplicably remained entirely silent. PCLOB noted in its report that, because Congress limited its mandate to counterterrorism programs, it focused primarily on those uses of Section 702. That meant a number of PCLOB's discussions – particularly regarding "incidental collections" of Americans sucked up under Section 702 – minimized the degree to which Americans who corresponded with completely innocent foreigners could be in a government database. That said, PCLOB did admit there were other uses, and it discussed the government's use of Section 702 to pursue weapons proliferators.

Yet PCLOB remained silent about a use of Section 702 that both Director of National Intelligence James Clapper's office, in its very first [information sheet](#) on Section 702 released in June 2013, and [multiple government witnesses at PCLOB's own hearing on this topic in](#)

March, discussed: cybersecurity. Not only should that have been discussed because Congress is preparing to debate cybersecurity legislation that would be modeled on Section 702. But the use of Section 702 for cybersecurity presents a number of unique, and potentially more significant, privacy concerns.

And PCLOB just dodged that issue entirely, even though Section 702's use for cybersecurity is unclassified.

In the transcript of the March PCLOB hearing on Section 702 uses, the word "cyber" shows up 12 times. Four of those references come from DOJ's Deputy Assistant Attorney General Brad Wiegmann's description of the kinds of foreign intelligence uses targeted under Section 702. (The other references came from Information Technology Industry Council President Dean Garfield.)

MR. WIEGMANN: You task a selector. So you're identifying, that's when you take that selector to the company and say this one's been approved. You've concluded that it is, does belong to a non-U.S. person overseas, a terrorist, or a proliferator, or a cyber person, right, whoever it is, and then we go to the company and get the information.

[snip]

It's aimed at only those people who are foreign intelligence targets and you have reason to believe that going up on that account that I mentioned, bad guy at Google.com is going to give you back information, information that is foreign intelligence, like on cyber threats, on terrorists, on proliferation, whatever it might be.

[snip]

So in other words, if I need to, if it's Joe Smith and his name is necessary if I'm passing it to that foreign government and it's key that they understand that it's Joe Smith because that's relevant to understanding what the threat is, or what the information is, let's say he's a cyber, malicious cyber hacker or whatever, and it was key to know the information, then you might pass Joe Smith's name.

Yesterday's report, however, doesn't mention "cyber" a single time. Indeed, it seems to go out of its way to avoid mentioning it.

As discussed elsewhere in this Report, the Board believes that the Section 702 program significantly aids the government's efforts to prevent terrorism, as well as to combat weapons proliferation and gather foreign intelligence for other purposes.

[snip]

The Section 702 program, for instance, is also used for surveillance aimed at countering the efforts of proliferators of weapons of mass destruction.<sup>473</sup> Given that these other foreign intelligence purposes of the program are not strictly within the Board's mandate, we have not scrutinized the effectiveness of Section 702 in contributing to those other purposes with the same rigor that we have applied in assessing the program's contribution to counterterrorism. Nevertheless, we have come to learn how the program is used for these other purposes, including, for example, specific ways in which it has been used to combat weapons proliferation and the degree to which the program supports the government's efforts to gather foreign intelligence for the benefit of policymakers.

Its footnote to that last section cites DOJ's 2012 report to SSCI on the uses of Section 702 (which doesn't mention cyber) rather than the information sheet released in June 2013, which does.

I find PCLOB's silence about the use of Section 702 to pursue cyber targets particularly interesting for several reasons.

First, because cyber targets pose unique privacy threats – in part because cyberattackers are more likely to hide their location and exploit the communications of entirely innocent people, meaning Section 702's claimed targeting limits offer no protection to Americans. Additionally, targeting (as Wiegmann describes it) a "malicious cyber hacker" goes beyond any traditional definition of foreign agent; it is telling he didn't use a Chinese military hacker as his example instead! Indeed, while proliferation (along with foreign governments, the other presumed certification) is solidly within FISA Amendment Act's definition of foreign intelligence, cybersecurity is not. In its discussion of back door searches, PCLOB admits there are concerns raised by back door searches that are heightened (or perhaps more sensitive, because they involve affluent white people) outside the counterterrorism context, that's especially true for cybersecurity targeting.

Consider, too, the likelihood that cyber collection is among the categories of about collection that PCLOB obliquely mentions but doesn't describe due to classification.

Although we cannot discuss the details in an unclassified public report, the moniker "about" collection describes a number of distinct scenarios, which the government has in the past characterized as different "categories" of "about" collection. These categories are not predetermined limits that confine what the government acquires; rather, they are merely ways of describing the

different forms of communications that are neither to nor from a tasked selector but nevertheless are collected because they contain the selector somewhere within them.

At the beginning of the report, PCLOB repeated the government's claim this is primarily about emails; here in the guts of it, it obliquely references other categories of collection, without really considering whether these categories present different privacy concerns.

Remember, too, that the original, good version of USA Freedom Act remains before the Senate Judiciary Committee. That bill would disallow the use of upstream 702 for any use but counterterrorism and counterproliferation. Did PCLOB ignore this use of Section 702 just to avoid alerting Senators who haven't been briefed on it that it exists?

Finally, I also find PCLOB's silence about NSA's admitted use of Section 702 to pursue cyberattackers curious given that, after Congress largely ditched ideas to involve PCLOB in various NSA oversight – such as providing it a role in the FISA Advocate position – Dianne Feinstein's Cyber Information Sharing Act all of a sudden has found a use for PCLOB again (serving a function, I should add, that arguably replaces FISC review).

(1) BIENNIAL REPORT FROM PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD.—Not later than 1 year after the date of the enactment of this Act and not less frequently than once every 2 years thereafter, the Privacy and Civil Liberties Oversight Board shall submit to Congress and the President a report providing—

(A) an assessment of the privacy and civil liberties impact of the type of activities carried out under this Act; and

(B) an assessment of the sufficiency of the policies, procedures, and guidelines established pursuant to section 5 in addressing privacy and civil liberties concerns.

Feinstein introduced this bill on June 17, several weeks after PCLOB briefed her staffers on their report (they briefed Congressional committee aides on June 2, and the White House on June 17 – see just after 9:00).

A renewed openness to expanding PCLOB's role may be entirely unmotivated, or it may stem from PCLOB's chastened analysis of the legal issues surrounding Section 702.

But I do find it interesting that PCLOB uttered, literally, not one word about the topic that, if DiFi's bill passes, would expand their mandate.