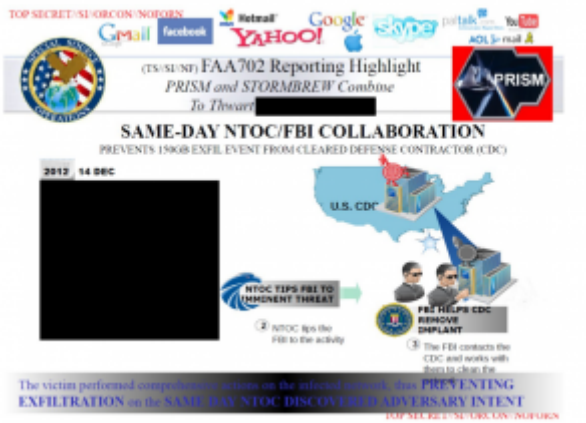
LEAHY-SENSENBRENNER WOULD SHUT THE SECTION 702 CYBERSECURITY LOOPHOLE



I'm going to have a few posts on the Leahy-Sensenbrenner bill, which is the most likely way we'll be able to rein in NSA spying. In addition to several sections stopping bulk collection, it has a section on collection of US person data under FISA Amendments Act (I'll return to the back-door loophole later).

But I'm particularly interested in what it does with upstream collection. It basically adds a paragraph to section d of Section 702 that limits upstream collection to two uses: international terrorism or WMD proliferation.

> (C) limit the acquisition of the contents of any communication to those communications—
>
> (i) to which any party is a target of the acquisition; or
>
> (ii) that contain an account identifier of a target of an acquisition, only if such communications are acquired to protect against international terrorism or the international proliferation of weapons of mass destruction.;

And adds a definition for "account identifier" limiting it to identifiers of people.

> (1) ACCOUNT IDENTIFIER.—The term 'account identifier' means a telephone or instrument number, other subscriber number, email address, or username used to uniquely identify an account.

I believe the effect of this is to prevent NSA from using Section 702 to conduct cyberdefense in the US.

As I have noted, there are reasons to believe that NSA uses Section 702 for just 3 kinds of targets:

- International terrorism
- WMD proliferation
- Cybersecurity

There are many reasons to believe one primary use of Section 702 for cybersecurity involves upstream collection targeted on actual pieces of code (that is, the identifier for a cyberattack, rather than the identifier of a user). As an example, the slide above, which I discuss in more detail here, explains that one of the biggest Section 702 successes involves preventing an attacker from exfiltrating 150 Gigs of data from a defense contractor. The success involved both PRISM and STORMBREW, the latter of which is upstream collection in the US.

In other words, the government has been conducting upstream collection within the US to search for malicious code (I'm not sure how they determine whether the code originated in a foreign country though given that they refuse to count domestic communications collected via upstream collection, I doubt they care).

So what these two sections of Leahy-Sensenbrenner would do is 1) limit the use of upstream collection to terrorists and proliferators, thereby prohibiting its use for

cybersecurity, and 2) define “account identifier” to exclude something like malicious code.

There’s one more interesting aspect of this fix. Unlike many other sections of the bill, it doesn’t go into effect right away.

> EFFECTIVE DATE.—The amendments made by subsections (a) and (b) shall take effect on the date that is 180 days after the date of the enactment of this Act.

The bill gives the Executive 6 months to find an alternative to this use of Section 702 — presumably, to pass a cybersecurity bill explicitly labeled as such.

Keith Alexander and others have long talked about the need to scan domestic traffic to protect against cyberattacks. But it appears — especially given the 6 month effective date on these changes — they’re already doing that, all in the name of foreign intelligence.