

IN OCTOBER 2013, PATRICK LEAHY AND JIM SENSENBRENNER ROLLED OUT A BILL THAT WOULD HAVE ENDED UPSTREAM CYBER COLLECTION

Back in October 2013, Jim Sensenbrenner and Patrick Leahy released the original, far better, version of the USA Freedom Act. As I noted in November 2013, it included a provision that would limit upstream collection to international terrorism and international proliferation of WMD uses.

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.

At the time, I noted that this would give the NSA 6 months to shut down the use of upstream collection to collect cyber signatures.

Jonathan Mayer's comments on the NYT/PP story today reveals why that would be important to do (this is a point I've been making for years): because if you're collecting signatures of cyber attacks, you're collecting victim data, as well, a problem that would only get worse under the cyberinformation sharing bills before Congress.

This understanding of the NSA's domestic cybersecurity authority leads to, in my view, a more persuasive set of privacy objections. Information sharing legislation would create a concerning surveillance dividend for the agency.



Because this flow of information is indirect, it prevents businesses from acting as privacy gatekeepers. Even if firms carefully screen personal information out of their threat reports, the NSA can nevertheless intercept that information on the Internet backbone.

Furthermore, this flow of information greatly magnifies the scale of privacy impact associated with information sharing. Here's an entirely realistic

scenario: imagine that a business detects a handful of bots on its network. The business reports a signature to DHS, who hands it off to the NSA. The NSA, in turn, scans backbone traffic using that signature; it collects exfiltrated data from tens of thousands of bots. The agency can then use and share that data.¹² What began as a tiny report is magnified to Internet scale.

But, instead of giving NSA 6 months to close this loophole, we instead passed USA F-ReDux, which does nothing to rein domestic spying in the name of cybersecurity.

Leahy released a remarkable statement in response to today's story that doesn't reveal whether he knew of this practice (someone knew to forbid it in their original bill!), but insisting he'll fight for more limits on surveillance and transparency.

Today's report that the NSA has expanded its warrantless surveillance of Internet traffic underscores the critical importance of placing reasonable and commonsense limits on government surveillance in order to protect the privacy of Americans. Congress took an important step in this direction this week by passing the USA FREEDOM Act, but I have always believed and said that more reforms are needed. Congress should have an open, transparent and honest debate about how to protect both our national security and our privacy. As Congress continues to work on surveillance and cybersecurity legislation, I will continue to fight for more reforms, more transparency, and more accountability – particularly on issues related to the privacy of Americans' personal communications.

Remember: on Tuesday, Richard Burr vehemently denied we had secret law. And while this application of FISA wasn't entirely secret – I figured it out pretty quickly, but a great great many people doubted me, as per usual – even Leahy is faced with a situation where he can't admit he knew about a practice he already tried to shut down once.