

AS SNOWDEN LEAK ANNIVERSARY APPROACHES, INTELLIGENCE COMMUNITY PREPARES TO DECLARE VICTORY

As June 5 approaches – and with it the one year anniversary of the first reporting on Edward Snowden’s leaks – the privacy community is calling supporters to redouble efforts to improve the NSA “reform bill,” which I call the USA Freedumber Act, in the Senate.

I explained here why the Senate is unlikely to improve USA Freedumber in any meaningful way. The votes just aren’t there – not even in the Senate Judiciary Committee.

Ominously, Dianne Feinstein just scheduled an NSA hearing for Thursday afternoon, when most of the privacy community will be out rallying the troops.

Unless the surveillance community finds some way to defeat USA Freedumber, the intelligence community will soon be toasting themselves that they used the cover of Edward Snowden’s disclosures to expand surveillance. The “Edward Snowden Put the NSA in Your Smartphone Act,” they might call it.

To prevent that, the privacy community needs to find a way to defeat USA Freedumber. It’s not enough, in my opinion, to point to the judicial review codified by USA Freedumber to accede to letting this pass. Not only doesn’t USA Freedumber end what most normal people call, “bulk collection,” but it expands collection in a number of ways.

That’s true, in part, because of the way the bill defines “bulk collection.” USA

Freedumber only considers something “bulk collection” if it collects all of some kind of data (so, all phone data in the US). If NSA limits collection at all – selecting to collect all the phone records from Area Code 202, for example – it no longer qualifies as bulk collection under the Intel Community definition used in the bill, no matter how broadly they’re collecting.

Here’s a post where I lay that out.

To make things worse, the last version of the House bill changed the term “selection term” to make it very broad: including “entities,” “addresses,” and “devices” among the things that count as a single target, all of which invite mass targeting. I was always skeptical about “specific selection term” serving as the limiting factor in the bill; key language about how the FISC currently understands “selection term” remains classified. But I do know that Zoe Lofgren and others in the House kept saying that under the current definition of the bill the government could collect all records in, say, my Area Code 202 example. And if that’s possible, it means the phone dragnet under this “reform” may be little more targeted than upstream Section 702 collection currently is, which has telecoms sniff through up to 75% of US Internet traffic.

But it’s not *just* that the bill doesn’t deliver what its boosters claim it does.

There are 4 other ways that the bill makes the status quo worse, as I show in this post:

- The move to telecoms codifies changes in the chaining process that will almost certainly expand the universe of data being analyzed – potentially significantly
- In three ways, the

bill would permit the use of phone chaining for purposes beyond counterterrorism, which isn't currently permitted

- The bill weakens the minimization procedures on upstream Section 702 collection imposed by FISC Judge John Bates in 2011, making it easier for the government to collect and keep domestic content domestically
- The bill moves the authority to set minimization procedures for Pen Registers from FISC to the Attorney General (and weakens them significantly), thus eliminating the tool John Bates used to shut down illegal content-as-metadata collection

In my opinion, these changes mean the NSA will be able to do much of what they were doing in 2009, before what were then called abuses – but under this bill would be legalized – were discovered. That, plus they're likely to expand the dragnet beyond terrorism targets.

For a year, privacy advocates have believed we'd get reform in response to Snowden's leaks. For too long, advocates treated HR 3361 as positive reform.

But unless we defeat USA Freedom, the Intelligence Community will have used the event of Snowden's leaks as an opportunity to expand the dragnet.