NSA BIDS TO EXPAND SPYING IN GUISE OF "FIXING" PHONE DRAGNET

Dutch Ruppersberger has provided Siobhan Gorman with details of his plan to "fix" the dragnet — including repeating the laughable claim that the "dragnet" (which she again doesn't distinguish as solely the Section 215 data that makes up a small part of the larger dragnet) doesn't include cell data.

Only, predictably, it's not a "fix" of the phone dragnet at all, except insofar as NSA appears to be bidding to use it to do all the things they want to do with domestic dragnets but haven't been able to do legally. Rather, it appears to be an attempt to outsource to telecoms some of the things the NSA hasn't been able to do legally since 2009.

For example, there's the alert system that Reggie Walton shut down in 2009.

As I reported back in February, the NSA reportedly has never succeeded in replacing that alert system, either for technical or legal reasons or both.

> NSA reportedly can't get its automated chaining program to work. In the motion to amend, footnote 12 — which modifies part of some entirely redacted paragraphs describing its new automated alert approved back in 2012 — reads:
>
> > The Court understands that to date NSA has not implemented, and for the duration of this authorization will not as a technical matter be in a position to implement, the automated query process authorized by prior orders of

> > this Court for analytical purposes. Accordingly, this amendment to the Primary Order authorizes the use of this automated query process for development and testing purposes only. No query results from such testing shall be made available for analytic purposes. Use of this automated query process for analytical purposes requires further order of this Court.

PCLOB describes this automated alert this way.

> > In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.68 The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store."

It has been 15 months since FISC approved this alert, but NSA still can't get it working.

I suspect this is the root of the stories claiming NSA can only access 30% of US phone records.

As described by WSJ, this automated system will

be built into the orders NSA provides telecoms; once a selector has been provided to the telecoms, they will keep automatically alerting on it.

> Under the new bill, a phone company would search its databases for a phone number under an individual "directive" it would receive from the government. It would send the NSA a list of numbers called from that phone number, and possibly lists of phone numbers those numbers had called. **A directive also could order a phone company to search its database for such calls as future records come in**. [my emphasis]

This would, presumably, mean NSA still ends up with a corporate store, a collection of people against whom the NSA has absolutely not a shred of non-contact evidence, against whom they can use all their analytical toys, including searching of content.

Note, too, that this program uses the word "directive," not query. Directive comes from the PRISM program, where the NSA gives providers generalized descriptions and from there have broad leeway to add new selectors. Until I hear differently, I'll assume the same is true here: that this actually involves less individualized review before engaging in 2 degrees of Osama bin Laden.

The legislation seems ripe for inclusion of querying of Internet data (another area where the NSA could never do what it wanted to legally after 2009), given that it ties this program to "banning" (US collection of, but Gorman doesn't say that either, maintaining her consistency in totally ignoring that EO 12333 collection makes up the greater part of bulk programs) Internet bulk data collection.

> The bill from Intelligence Committee Chairman Mike Rogers (R., Mich.) and his Democratic counterpart, Rep. C.A.

> "Dutch" Ruppersberger (D., Md.), would ban so-called bulk collection of phone, email and **Internet** records by the government, according to congressional aides familiar with the negotiations. [my emphasis]

Call me crazy, but I'm betting there's a way they'll spin this to add in Internet chaining with this "fix."

Note, too, Gorman makes no mention of location data, in spite of having tied that to her claims that NSA only collects 20% of data. Particularly given that AT&T's Hemisphere program provides location data, we should assume this program could too, which would present a very broad expansion on the status quo.

And finally, note that neither the passage I quoted above on directives to providers, nor this passage specifies what kind of investigations this would be tied to (though they are honest that they want to do away with the fig leaf of this being tied to investigations at all).

> The House intelligence committee bill doesn't require a request be part of an ongoing investigation, Mr. Ruppersberger said, because intelligence probes aim to uncover what should be investigated, not what already is under investigation.

Again, the word "directive" in the PRISM context also provides the government the ability to secretly pass new areas of queries — having expanded at least from counterterrorism to counterproliferation and cybersecurity uses. So absent some very restrictive language, I would assume that's what would happen here: NSA would pass it in the name of terrorism, but then use it primarily for cybersecurity and counterintelligence, which the NSA considers bigger threats these days.

And that last suspicion? That's precisely what

Keith Alexander said he planned to do with this "fix," presumably during the period when he was crafting this "fix" with NSA's local Congressman: throw civil libertarians a sop but getting instead an expansion of his cybersecurity authorities.

Update: Here's Spencer on HPSCI, confirming it's as shitty as I expected.

And here's Charlie Savage on Obama's alternative.

It would:

- Keep Section 215 in place, though perhaps with limits on whether it can be used in this narrow application
- Enact the same alert-based system and feed into the corporate store, just as the HPSCI proposal would
- Include judicial review like they have now (presumably including automatic approval for FISA targets)

Obama's is far better than HPSCI (though this seems to be part of a bad cop-good cop plan, and the devil remains in the details). But there are still some very serious concerns.