A BRIEF HISTORY OF THE PATRIOT REAUTHORIZATION DEBATE

I wanted to provide some background of how we got to this week's PATRIOT Reauthorization debate to explain what I believe the surveillance boosters are really aiming for. Rather than a response to Edward Snowden, I think it is more useful to consider "reform" as an Intelligence Community effort to recreate functionalities they had and then lost in 2009.

2009 violations require NSA to start treating PATRIOT data like PATRIOT data and shut down automated functions

That history starts in 2009, when NSA was still operating under the system they had established under Stellar Wind while pretending to abide by FISC rules.

At the beginning of 2009, the NSA had probably close to full coverage of phone records in the US, and coverage on the most important Internet circuits as well. Contrary to the explicit orders of the FISC, NSA was treating all this data as EO 12333 data, not PATRIOT data.

On the Internet side, it was acquiring data that it considered Dialing, Routing, Addressing, and Signaling information but which also constituted content (and which violated the category limits Colleen Kollar-Kotelly had first imposed).

On the phone side, NSA was not only treating PATRIOT data according to NSA's more general minimization procedures as opposed to those dictated by the FISC. But in violation of those minimization procedures, NSA was submitting

phone dragnet data to all the automated procedures it submitted EO 12333 data to, which included automated searches and automatic chaining on other identifiers believed to belong to the same user (the latter of which NSA calls "correlations"). Either these procedures consisted of — or the data was also treated to — pattern analysis, chaining users on patterns rather than calls made. Of key importance, one point of having all the data in the country was to be able to run this pattern analysis. Until 2008 (and really until 2009) they were sharing the results of this data in real time.

Having both types of data allowed the NSA to chain across both telephony and Internet data (obtained under a range of authorities) in the same query, which would give them a pretty comprehensive picture of all the communications a target was engaging in, regardless of medium.

I believe this bucolic state is where the surveillance hawks want us to return to. Indeed, to a large extent that's what Richard Burr's bill does (with a lot of obstructive measures to make sure this process never gets exposed again).

But when DOJ disclosed the phone violations to FISC in early 2009, they shut down all those automatic processes. And Judge Reggie Walton took over 6 months before he'd even let NSA have full ability to query the data.

Then, probably in October 2009, DOJ finally confessed to FISC that every single record NSA had collected under the Internet dragnet for five years violated Kollar-Kotelly's category rules. Walton probably shut down the dragnet on October 30, 2009, and it remained shut down until around July 2010.

At this point, not only didn't NSA have domestic coverage that included Internet and phone, but the phone dragnet was a lot less useful than all the other phone data NSA collected because NSA couldn't use its nifty automatic tools on it.

Attempts to restore the pre-2009 state

We know that NSA convinced John Bates to not only turn the Internet dragnet back on around July 2010 (though it took a while before they actually turned it on), but to expand collection to some or all circuits in the US. He permitted that by interpreting anything that might be Dialing, Routing, Addressing, and Signaling (DRAS) to be metadata, regardless of whether it also was content, and by pointing back to the phone dragnet to justify the extension of the Internet dragnet. Bates' fix was short-lived, however, because by 2011, NSA shut down that dragnet. I wildarseguess that may partly because DOJ knew it was still collecting content, and when Bates told NSA if it knew it was collecting content with upstream collection, it would be illegal (NSA destroyed the Internet dragnet data at the same time it decided to start destroying its illegal upstream data). I also think there may have been a problem with Bates' redefinition of DRAS, because Richard Burr explicitly adopted Bates' definition in his bill, which would have given Bates' 2010 opinion congressional sanction. As far as we know, NSA has been coping without the domestic Internet dragnet by collecting on US person Internet data overseas, as well as off PRISM targets.

Remember, any residual problems the Internet dragnet had may have affected NSA's ability to collect any IP-based calls or at least messaging.

Meanwhile, NSA was trying to replace the automated functions it had up until 2009, and on November 8, 2012, the NSA finally authorized a way to do that. But over the next year plus, NSA never managed to turn it on.

The phone records gap

Meanwhile, the phone dragnet was collecting less and less of the data out there. My current theory is that the gap arose because of two

things involving Verizon. First, in 2009, part or all of Verizon dropped its contract with the FBI to provide enhanced call records first set up in 2002. This meant it no longer had all its data collected in a way that was useful to FBI that it could use to provide CDRs (though Verizon had already changed the way it complied with phone records in 2007, which had, by itself, created some technical issues). In addition, I suspect that as Verizon moved to 4G technology it didn't keep the same kind of records for 4G calls that transited its backbone (which is where the records come from, not from customer bills). The problems with the Internet dragnet may have exacerbated this (and in any case, the phone dragnet orders only ask for telephony metadata, not IP metadata).

Once you lose cell calls transiting Verizon's backbone, you've got a big hole in the system.

At the same time, more and more people (and, disproportionately, terrorist targets) were relying more and more on IP-based communications — Skype, especially, but also texting and other VOIP calls. And while AT&T gets some of what crosses its backbone (and had and still has a contract for that enhanced call record service with the FBI, which means it will be accessible), a lot of that would not be available as telephony. Again, any limits on Internet collection may also impact IP based calls and messaging.

Edward Snowden provides a convenient excuse

Which brings you to where the dragnets were in 2013, when Edward Snowden alerted us to their presence. The domestic PATRIOT-authorized Internet dragnet had been shut down (and with it, potentially, Internet-based calls and messaging). The phone dragnet still operated, but there were significant gaps in what the telecoms would or could turn over (though I suspect NSA still has full coverage of data that transits AT&T's backbone). And that data

couldn't be subjected to all the nifty kinds of analysis NSA liked to subject call data to. Plus, complying with the FISC-imposed minimization procedures meant NSA could only share query results in limited situations and even then with some bureaucratic limits. Finally, it could only be used for counterterrorism programs, and such data analysis had become a critical part of all of NSA's analysis, even including US collection.

And this is where I suspect all those stories about NSA already considering, in 2009 and in 2013, shutting down the dragnet. As both Ken Dilanian stories on this make clear, DOJ believed they could not achieve the same search results without a new law passed by Congress. Bob Litt has said the same publicly. Which makes it clear these are not plain old phone records.

So while Edward Snowden was a huge pain in the ass for the IC, he also provided the impetus to make a decision on the phone dragnet. Obama made a big show of listening to his Presidential Review Group and PCLOB, both of which said to get rid of it (the latter of which said it was not authorized by Section 215). But — as I noted at the time — moving to providers would fix some of their problems.

In their ideal world, here's what we know the IC would like:

- Full coverage on both telephony and IP-based calls and messaging and — ideally — other kinds of Internet communications
- Ability to share promiscuously
- Ability to use all NSA's analytical tools on raw data (the data mandates are about requiring some kind of analytical work from

providers)
- Permission to use the "call" function for all intelligence purposes
- Ability to federate queries with data collected under other authorities

And the IC wants this while retaining Section 215's use of bulky collections that can be cross-referenced with other data, especially the other Internet collection it conducts using Section 215, which makes up a majority of Section 215 orders.

Those 5 categories are how I've been analyzing the various solutions (which is one of about 10 reasons I'm so certain that Mitch McConnell would never want straight reauthorization, because there's nothing that straight reauthorization would have ratified that would have fixed the existing problems with the dragnet), while keeping in mind that as currently constructed, the Internet 215 collection is far more important to the IC than the phone dragnet.

How the bills stack up

USA F-ReDux, as currently incarnated, would vastly expand data sharing, because data would come in through FBI (as PRISM data does) and FBI metadata rules are very permissive. And it would give collection on telephony and IP-based calls (probably not from all entities, but probably from Apple, Google, and Microsoft). It would *not* permit use for all intelligence purposes. And it is unclear how many of NSA's analytical tools they'd be able to use (I believe they'd have access to the "correlations" function directly, because providers would have access internally to customers' other accounts, but with the House report, other kinds of analysis should be prohibited, though who knows what AT&T and Microsoft would do with immunity).

The House report clearly envisions federated queries, but they would be awkward to integrate with the outsourced collection.

Burr's bill, on the other hand, would expand provider based querying to all intelligence uses. But even before querying might — maybe — probably wouldn't — move to providers in 2 years, Burr's bill would have *immediately* permitted NSA to obtain all the things they'd need to return to the 2009 bucolic era where US collected data had the same treatment as EO 12333 collected data. And Burr's bill would probably permit federated queries with all other NSA data. This is why, I think, he adopted EO 12333 minimization procedures, which are far more restrictive than what will happen when data comes in via FBI, because since it will continue to come in in bulk, it needs to have an NSA minimization procedure. Burr's bill would also sneak the Section 215 Internet collection back into NSL production, making that data more promiscuously available as well.

In other words, this is why so many hawks in the House are happy to have USA F-ReDux: because it is vastly better than the status quo. But it's also why so many hawks in the Senate are unsatisfied with it: because it doesn't let the IC do the other things — some of the analytical work and easy federated queries — that they'd like, across all intelligence functions. (Ironically, that means even while they're squawking about ISIS, the capabilities they'd really like under Burr's bill involve entirely other kinds of targets.)

A lot of the debate about a phone dragnet fix has focused on other aspects of the bill — on transparency and reporting and so on. And while I think those things do matter (the IC clearly wants to minimize those extras, and had gutted many of them even in last year's bill), what really matters are those 5 functionalities.