THE REASON OBAMA CAPITULATED ON THE (PHONE) DRAGNET

This will be a bit of a contrary take on what I believe to be the reasons for President Obama's capitulation on the dragnet, announcing support today for a plan to outsource the first query in the dragnetting process to the telecoms.

It goes back to the claims — rolled out in February — that the NSA has only been getting 20 to 30% of the call data in the US. Those reports were always silent or sketchy on several items:

- The claims were always silent that they applied only to Section 215, and did not account for the vast amount of data, including US person cell data, collected under EO 12333.
- The claims were sketchy about the timing of the claim, especially in light of known collection of cell data in 2010 and 2011, showing that at that point NSA had no legal restrictions on accepting such data.
- The claims were silent about why, in both sworn court declarations and statements to Congress, Administration officials said the collection (sometimes modified by Section 215,

> often, especially in court declarations, not) was comprehensive.

Here's what I think lies behind those claims.

We know that as recently as September 1, 2011, the NSA believed it had the legal authority to collect cell location data under Section 215, because they were doing just that. Congress apparently did not respond well to learning, belatedly, that the government was collecting location data in a secret interpretation of a secret interpretation. Nevertheless, it appears the government still believed it had that authority — though was reevaluating it — on January 31, 2012, when Ron Wyden asked James Clapper about it — invoking the "secret law" we know to be Section 215 — during his yearly grilling of Clapper in the Global Threat hearing.

> > Wyden: Director Clapper, as you know the Supreme Court ruled last week that it was unconstitutional for federal agents to attach a GPS tracking device to an individual's car and monitor their movements 24/7 without a warrant. Because the Chair was being very gracious, I want to do this briefly. Can you tell me as of now what you believe this means for the intelligence community, number 1, and 2, would you be willing to commit this morning to giving me an unclassified response with respect to what you believe the law authorizes. This goes to the point that you and I have talked, Sir, about in the past, the question of secret law, I strongly feel that the laws and their interpretations must be public. And then of course the important work that all of

> > you're doing we very often have to keep that classified in order to protect secrets and the well-being of your capable staff. So just two parts, 1, what you think the law means as of now, and will you commit to giving me an unclassified answer on the point of what you believe the law actually authorizes.
>
> Clapper: Sir, the judgment rendered was, as you stated, was in a law enforcement context. We are now examining, and the lawyers are, what are the potential implications for intelligence, you know, foreign or domestic. So, that reading is of great interest to us. And I'm sure we can share it with you. [looks around for confirmation] One more point I need to make, though. In all of this, we will—we have and will continue to abide by the Fourth Amendment. [my emphasis]

Unsurprisingly, as far as I know, Clapper never gave Wyden an unclassified answer.

Nevertheless, since then the government has come to believe it cannot accept cell data under Section 215. Perhaps in 2012 as part of the review Clapper said was ongoing, the government decided the Jones decision made their collection of the cell location of every cell phone in the US illegal or at least problematic. Maybe, in one of the 7 Primary orders DOJ is still withholding from 2011 to 2013, the FISC decided Jones made it illegal to accept data that included cell location. It may be that a February 24, 2013 FISC opinion — not a primary order but one that significantly reinterpreted Section 215 — did so. Certainly, by July 19, 2013, when Claire Eagan prohibited it explicitly

in a primary order, it became illegal for the government to accept cell location data.

That much is clear, though: until at least 2011, DOJ believed accepting cell location under Section 215 was legal. At least by July 19, 2013, FISC made it clear that would not be legal.

That, I believe, is where the problems accepting cell phone data as part of Section 215 come from (though this doesn't affect EO 12333 data at all, and NSA surely still gets much of what it wants via EO 12333). Theresa Shea has explicitly said in sworn declarations that the NSA only gets existing business records. As William Ockham and Mindrayge have helped me understand, unless a telecom makes it own daily record of all the calls carried on its network — which we know AT&T does in the Hemisphere program, funded by the White House Drug Czar — then the business ecords the phone company will have are its SS7 routing records. And that's going to include cell phone records. And those include location data for cell phones.

Now, it may be that the telecoms chose not to scan out this information for the government. It may be that after the program got exposed they chose to do the bare minimum, and the cell restrictions allowed them to limit what they turned over (something similar may have happened with VOIP calls carried across their networks). It may be that Verizon and even AT&T chose to only provide that kind of data via EO 12333 program that, because they are voluntary, get paid at a much higher rate. In any case, I have very little doubt that NSA got the phone records from Verizon, just not via Section 215.

But I'm increasingly sure the conflict between Section 215's limit to existing business record and the limits imposed on Section 215 via whatever means was the source of the "problem" that led NSA to only get 30% of phone records [via the Section 215 program, which is different than saying they only got 30% of all records from US calls].

And a key feature of both the President's sketchy program…

- the companies would be compelled by court order to provide technical assistance to ensure that the records can be queried and that results are transmitted to the government in a usable format and in a timely manner.

And the RuppRoge Fake Fix…

> (h)(1)(A) immediately provide the Government with records, whether existing or created in the future, in the format specified by the Government
>
> [snip]
>
> (h)(2) The Government may provide any information, facilities, or assistance necessary to aid an electronic communications service provider in complying with a directive issued pursuant to paragraph (1).

Is that the government gets to dictate what format they get records in here, which they couldn't do under Section 215. That means, among other things, they can dictate that the telecoms strip out any location data before it gets to NSA, meaning NSA would remain compliant with whatever secret orders have made the collection of cell location in bulk illegal.

Remember, too, that both of these programs will have an alert feature. In spite of getting an alert system to replace the one deemed illegal in 2009 approved on November 8 2012, the government has not yet gotten that alert function working for what are described as technical reasons.

> 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.

It's possible that, simply doing the alert on exclusively legally authorized data (as opposed to data mixing EO 12333 and FISC data) solves the technical problems that had stymied NSA from rolling out the alert system they have been trying to replace for 5 years. It's possible that because NSA was getting its comprehensive coverage of US calls via different authorities, it could not comply with the FISC's legal limits on the alert system. But we know there will be an alert function if either of these bills are passed.

The point is, here, too, outsourcing the initial query process solves a legal-technical problem the government has been struggling with for years.

The Obama plan is an improvement over the status quo (though I do have grave concerns about its applicability in non-terrorist contexts, and my concerns about what the government does with the data of tens to hundreds of thousands of innocent Americans remain).

But don't be fooled. Obama's doing this as much because it's the easiest way to solve legal and technical problems that have long existed because the government chose to apply a law that was entirely inapt to the function they wanted

to use it for.

Shockers! A more privacy protective solution also happens to provide the best technical and legal solution to the problem at hand.

Update: Forgot to add that, assuming I'm right, this will be a pressure point that Members of Congress will know about but we won't get to talk about. That is, a significant subset of Congress will know that unless they do something drastic, like threatening legal penalties or specifically defunding any dragnetting, the Executive will continue to do this one way or another, whether it's under a hybrid of Section 215 and EO 12333 collection, or under this new program. That is, it will be a selling point to people like Adam Schiff (who advocated taking the call records out of government hands but who has also backed these proposals) that this could bring all US intelligence collection under the oversight of the FISC (it won't, really, especially without a very strong exclusivity provision that prohibits using other means, which the Administration will refuse because it would make a lot of what it does overseas illegal). This is the same tension that won the support of moderates during the FISA Amendments Act, a hope to resolve real separation of powers concerns with an imperfect law. So long as the Leahy-Sensenbrenner supporters remain firm on their demands for more reforms, we may be able to make this a less imperfect law. But understand that some members of Congress will view passing this law as a way to impose oversight over a practice (the EO 12333 collection of US phone records) that has none.

Update: Verizon has released this telling statement.

> This week Congressmen Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD) released the "End Bulk Collection Act of 2014", which would end bulk collection of data related to electronic communications. The White House also announced that it is proposing an approach to end bulk

> collection. We applaud these proposals to end Section 215 bulk collection, but feel that it is critical to get the details of this important effort right. So at this early point in the process, we propose this basic principle that should guide the effort: the reformed collection process should not require companies to store data for longer than, or in formats that differ from, what they already do for business purposes. If Verizon receives a valid request for business records, we will respond in a timely way, but companies should not be required to create, analyze or retain records for reasons other than business purposes. [my emphasis]

It's telling, first of all, because Verizon still doesn't want to have to fuss with anything but their business records. That says it has been unwilling to do so, in the past, which, in my schema, totally explains why the government couldn't get Verizon cell records using Section 215. (I have wondered whether this was a newfound complaint, since they got exposed whereas AT&T did not; and even in spite of Randal Milch's denial, I still do wonder whether the Verizon-Vodaphone split hasn't freed them of some data compliance obligations.)

Just as importantly, Verizon doesn't want to analyze any of this data. As I have pointed out, someone is going to have to do high volume number analysis, because otherwise the number of US person records turned over will be inappropriately large but small enough it will be a significant privacy violation to do it at that point (for some things, it requires access to the raw data).

I'm unclear whether the RuppRuge Fake Fix plan of offering assistance (that is, having NSA onsite) fixes this, because NSA could do this analysis at Verizon.