DEVIN NUNES THINKS CONGRESS NEEDS MORE CLASSIFIED BRIEFINGS TO UNDERSTAND PHONE DRAGNET

In an article describing the current state of play on the Section 215 sunset, WaPo quotes Devin Nunes claiming that the poor maligned phone dragnet is just misunderstood. So he plans on having more briefings (curiously, just for the Republican caucus).

> "NSA programs, including the bulk telephone metadata program, are crucial anti-terror and foreign intelligence tools that should be reauthorized," said Rep. Devin Nunes (R-Calif.), chairman of the House Intelligence Committee.
>
> He told reporters on Tuesday that he felt the program has been misunderstood and that he would hold classified briefings for the GOP caucus.

I don't mean to mock Nunes. After all, I've been saying for well over a year that the public assessments of the phone dragnet don't actually measure how the government really uses it (below the rule I've copied the part of this post that describes other ways we know they use it). And that was before the phone dragnet orders replaced "contact chaining" with "connection chaining" over a year ago, which presumably adds a correlating function to the mix (that is, the government also uses the phone dragnet to identify a

person's multiple phone-based identities, potentially including smart phone identities).

But I do think it worth noting two things.

First, Nunes' decision to tell Republicans more, coming relatively soon after he took over the House Intelligence Chair from Mike Rogers, suggests that Mike Rogers was never fully forthcoming — not even in the secret briefings he gave in lieu of passing on Executive Branch explanations of the phone dragnet — about what it did.

But Nunes' response is *not* to require the government to itself explain publicly what it's really doing with the phone dragnet. But instead to hold classified briefings that often serve as a means to buy silence from those who attend.

In any case, that story you've been told for almost two years about how the phone dragnet identifies who is two degrees away from Osama bin Laden? Unsurprisingly, it's nowhere near the full story.

[A]ssessments of the phone dragnet […] don't even take the IC at its word in its other, quieter admissions of how it uses the dragnet (notably, in none of Stone's five posts on the dragnet does he mention any of these — one, two, three, four,five — raising questions whether he ever learned or considered them). These uses include:

- Corporate store
- "Data integrity" analysis
- Informants
- Index

Corporate store: As the minimization procedures and a few FISC documents make clear, once the NSA has run a query, the results of that query are placed in a "corporate store," a database of all previous query results.

ACLU's Patrick Toomey has described this in depth, but the key takeaways are once data gets into the corporate store, NSA can use "the full range of SIGINT analytic tradecraft" on it, and none of that activity is audited.

NSA would have you believe very few Americans' data gets into that corporate store, but even if the NSA treats queries it says it does, it could well be in the millions. Worse, if NSA doesn't do what they say they do in removing high volume numbers like telemarketers, pizza joints, and cell voice mail numbers, literally everyone could be in the corporate store. As far as I've seen, the metrics measuring the phone dragnet only involve tips going out to FBI and not the gross number of Americans' data going into the corporate store and therefore subject to "the full range of analytic tradecraft," so we (and probably even the FISC) don't know how many Americans get sucked into it. Worse, we don't know what's included in "the full range of SIGINT analytic tradecraft" (see this post for some of what they do with Internet metadata), but we should assume it includes the data mining the government says it's not doing on the database itself.

The government doesn't datamine phone records in the main dragnet database, but they're legally permitted to datamine anyone's phone records who has come within 3 degrees of separation from someone suspected of having ties to terrorism.

"Data integrity" analysis: As noted, the NSA claims that before analysts start doing more formal queries of the phone dragnet data, "data integrity" analysts standardize it and do something (it's unclear whether they delete or just suppress) "high volume numbers." They also — and the details on this are even sketchier — use this live data to develop algorithms. This has the possibility of significantly changing the dragnet and what it does; at the very least, it risks eliminating precisely the numbers that might be most valuable (as in the Boston Marathon case, where a pizza joint plays a

central role in the Tsarnaev brothers' activities). The auditing on this activity has varied over time, but Dianne Feinstein's bill would eliminate it by statute. Without such oversight, data integrity analysts have in the past, moved chunks of data, disaggregated them from any identifying (collection date and source) information, and done … we don't know what with it. So one question about the data integrity analyst position is how narrowly scoped the high volume numbers are (if it's not narrow, then everyone's in the corporate store); an even bigger is what they do with the data in often unaudited behavior before it's place into the main database.

Informants: Then there's the very specific, admitted use of the dragnet that no one besides me (as far as I know) has spoken about: to find potential informants. From thevery start of the FISC-approved program, the government maintained the dragnet "may help to discover individuals willing to become FBI assets," and given that the government repeated that claim 3 years later, it does seem to have been used to find informants.

This is an example of a use that would support "connecting the dots" (as the program's defenders all claim it does) but that could ruin the lives of people who have no tie to actual terrorists (aside from speaking on the phone to someone one or two degrees away from a suspected terror affiliate). The government has in the past told FISCR it might use FISA data to find evidence of other crimes — even rape — to coerce people to become informants, and in some cases, metadata (especially that in the corporate store, enhanced by "the full range of analytic tradecraft") could pinpoint not just potential criminals, but people whose visa violations and extramarital affairs might make them amenable to narcing on the people in their mosque (with the additional side effect of building distrust within a worship community). There's not all that much oversight over FBI's use of informants in any case (aside from permitting us to learn

that they're letting their informants commit more and more crimes), so it's pretty safe to assume no one is tracking the efficacy of the informants recruited using the powerful tools of the phone dragnet.

Index: Finally, there's the NSA's use of this metadata as a Dewey Decimal System (to useJames Clapper's description) to pull already-collected content off the shelf to listen to — a use even alluded to in the NSA's declarations in suits trying to shut down the dragnet.

> Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

Don't get me wrong. Given how poorly the NSA has addressed its longterm failure to hire enough translators in target languages, I can understand how much easier it must be to pick what to read based on metadata analysis (though see my concerns, above, about whether the NSA's assessment techniques are valid). But when the NSA says, "non-US persons" here, what they mean

is “content collected by targeting non-US persons,” which includes a great deal of content of US persons.

Which is another way of saying the dragnet serves as an excuse to read US person content.