THE RUPPROGE FAKE DRAGNET FIX, AS INTRODUCED: DOES IT INCLUDE KEITH ALEXANDER'S QUID PRO QUO?

This post is going to be a general review on the contents of the actual records collection part of the RuppRoge Fake Dragnet Fix, which starts on page 15, though I confess I'm particularly interested in what other uses — besides the phone dragnet — it will be put to.

First, note that this bill applies to "electronic communication service providers," not telecoms. In addition, it uses neither the language of Toll Records from National Security Letters nor Dialing, Addressing, Routing, or Signalling from Pen Registers. Instead, it uses "records created as a result of communications of an individual or facility." Also remember that FISC has, in the past, interpreted "facility" to mean "entire telecom switch." This language might permit a lot of things, but I suspect that one of them is another attempt to end run content collection restrictions on Internet metadata — the same problem behind the hospital confrontation and the Internet dragnet shutdown in 2009. I look forward to legal analysis on whether this successfully provides an out.

The facility language is also troubling in association with the foreign power language of the bill (which already is a vast expansion beyond the terrorism-only targeting of the phone dragnet). Because you could have a telecom switch in contact with a suspected agent of a foreign power and still get a great deal of data, much of it on innocent people. The limitation (at b1B) to querying with "specific

identifiers or selection terms' then becomes far less meaningful.

Then add two details from section h, covering the directives the government gives the providers. The government requires the data in the format they want. Section 215 required existing business records, which may have provided providers a way to be obstinate about how they delivered the data (and this may have led to the government's problems with the cell phone data). But it also says this (in the paragraph providing for compensation I wrote about here):

> The Government may provide any information, facilities, or assistance necessary to aid an electronic communications service provider in complying with a directive

Remember, one month ago, Keith Alexander said he'd be willing to trade a phone dragnet fix for what amounts to the ability to partner with industry on cybersecurity. The limits on this bill to electronic communication service providers means it's not precisely what Alexander wanted (I understand him to want that kind of broad partnership across industries). Still, the endorsement of the government basically going to camp out at a provider makes me wonder if there isn't some of that. Note, that also may answer my question about when and where NSA would conduct the pizza joint analysis, which would mean there'd still be NSA techs (or contractors) rifling through raw data, but they'd be doing it at the telecoms' location.

The First Amendment restriction appears more limited than it is in the Section 215 context, though I suspect RuppRoge simply reflects the reality of what NSA is doing now. Both say you can't investigate an American solely for First Amendment views, but RuppRoge says you can't get the information for an investigation of an American. Given that RuppRoge eliminates any

requirement that this collection be tied to an investigation, it would make it very easy to query a US person selector based on First Amendment issues in the guise of collecting information for another reason. But again, I suspect that's what the NSA is doing in practice in any case.

Note, too, that RuppRoge borrows the "significant purpose" language from FISA, meaning the government can have a domestic law enforcement goal to getting these records.

RuppRoge then lays out an elaborate certification/directive system that is (as I guessed) modeled on the FISA Amendments Act, but written to be even more Byzantine in the bill. It works the same, though: the Attorney General and the Director of National Intelligence submit broad certifications to the FISC, which reviews whether they comply with the general requirements in the bill. It can also get emergency orders (though for some reason here, as elsewhere, RuppRoge have decided to invent new words from the standard ones), though the language is less about emergency and more about timely acquisition of data. Ultimately, there is judicial review, after the fact, except that like FAA, the review is programmatic, not identifier specific. Significantly, the records the government has to keep only need to comply with selection procedures (which are the new name for targeting procedures) "at the time the directive was issued," which would seem to eliminate any need to detask over a year if you discover the target isn't actually in contact with an agent of a foreign power. Also, in the clause permitting the FISC to order data be destroyed if the directives were improper, the description talks about halting production of "records," but destruction of "information." That might be more protective (including the destruction of reports based on data) or it might not (requiring only the finished reports be destroyed). Interestingly, this section includes no language affirmatively permitting alert systems, though RuppRoge have made it

clear that's what they intend with the year long certifications. In addition, those year long certifications might be used in conjunction with a year long PRISM order to first search a provider for metadata, then immediately task on content (which would be useful in a cybersecurity context).

The bill also changed the language of minimization procedures, which they call "civil liberties and privacy protection procedures." Interestingly, the procedures differ from the standard in Section 215, including both a generalized privacy protection and one limiting receipt and dissmenation of "records associated with a specific person." These might actually be more protective than those in Section 215, or they might not, given that the identifying information (at b1D) excludes things like phone number or email which clearly identify a specific person, but get no protection (this identifying information hearkens back, at least in part, to debates about whether the dragnet minimization procedures complied with requirement for them in law on this point). In other words, it may provide people more protection, but given the NSA's claim that they can't get identify from a phone number, they likely don't consider that data to be protected at all.

I can't help believing much of this bill was written with cases like Lavabit and the presumed Credo NSL challenges in mind, as it uses language disdainful of legal challenges.

> If the judge determines that such petition consists of claims, defenses, or other legal contentions that are not warranted by existing law or consists of a frivolous argument for extending, modifying, or reversing existing law or for establishing new law, the judge shall immediately deny such petition and affirm the directive or any part of the directive that is the subject of the such petition and order the recipient to

> comply with the directive or any part of it.

This seems to completely rule out any constitutional challenge to this law from providers. Though the bill even allows for emergency acquisition while FISC is reviewing a certification, suggesting RuppRoge don’t want the FISC to make any through either. So if this bill were to pass, you can be sure it will remain in place indefinitely.