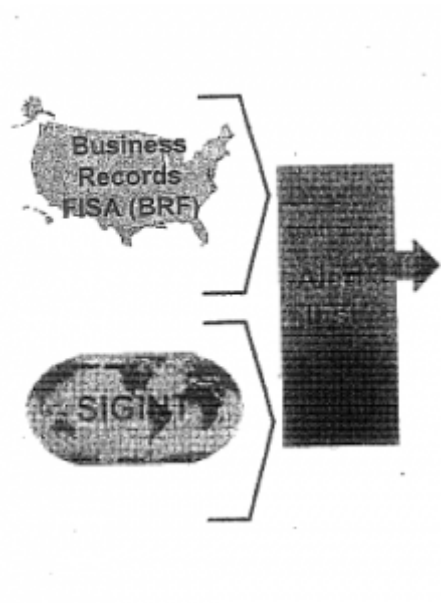
MARCO RUBIO EXPLAINS THE DRAGNET



A penny dropped for me, earlier this week, when Marco Rubio revealed that authorities are asking "a large number of companies" for "phone records." Then, yesterday, he made it clear that these companies don't fall under FCC's definition of "phone" companies, because they're not subject to that regulator's 18 month retention requirement.

His comments clear up a few things that have been uncertain since February 2014, when some credulous reporters started reporting that the Section 215 phone dragnet — though they didn't know enough to call it that — got only 20 to 30% of "all US calls."

The claim came not long after Judge Richard Leon had declared the 215 phone dragnet to be unconstitutional. It also came just as the President's Review Group (scoped to include all of the government's surveillance) and PCLOB (scoped to include only the 215 phone dragnet) were recommending the government come up with a better approach to the phone dragnet.

The report clearly did several things. First, it provided a way for the government to try to undermine the standing claim of other plaintiffs challenging the phone dragnet, by leaving the possibility their records were among the claimed 70% that was not collected. It gave a public excuse the Intelligence Community could use to explain why PRG and PCLOB showed the dragnet to

be mostly useless. And it laid the ground work to use “reform” to fix the problems that had, at least since 2009, made the phone dragnet largely useless.

It did not, however, admit the truth about what the 215 phone dragnet really was: just a small part of the far vaster dragnet. The dragnet as a whole aspires to capture a complete record of communications and other metadata indicating relationships (with a focus on locales of concern) that would, in turn, offer the ability to visualize the networks of the world, and not just for terrorism. At first, when the Bush Administration moved the Internet (in 2004) and phone (in 2006) dragnets under FISC authority, NSA ignored FISC’s more stringent rules and instead treated all the data with much more lax EO 12333 rules(see this post for some historical background). When FISC forced the NSA to start following the rules in 2009, however, it meant NSA could no longer do as much with the data collected in the US. So from that point forward, it became even more of a gap-filler than it had been, offering a thinner network map of the US, one the NSA could not subject to as many kinds of analysis. As part of the reforms imposed in 2009, NSA had to start tracking where it got any piece of data and what authority’s rules it had to follow; in response, NSA trained analysts to try to use EO 12333 collected data for their queries, so as to apply the more permissive rules.

That, by itself, makes it clear that EO 12333 and Section 215 (and PRTT) data was significantly redundant. For every international phone call (or at least those to countries of terrorism interest, as the PATRIOT authorities were supposed to be restricted to terrorism and Iran), there might be two or more copies of any given phone call, one collected from a provider domestically, and one collected via a range of means overseas (in fact, the phone dragnet orders make it clear the same providers were also providing international collection not subject to 215). If you don’t believe me on

this point, Mike Lee spelled it out last week. Not only might NSA get additional data with the international call — such as location data — but it could subject that data to more interesting analysis, such as co-location. Thus, once the distinction between EO 12333 and PATRIOT data became formalized in 2009 (years after it should have been) the PATRIOT data served primarily to get a thinner network map of the data they could only collect domestically.

Because the government didn't want to admit they had a dragnet, they never tried to legislate fixes for it such that it would be more comprehensive in terms of reach or more permissive in terms of analysis.

So that's a big part of why four beat journalists got that leak in February 2014, at virtually the same time President Obama decided to replace the 215 phone dragnet with something else.

The problem was, the government never admitted the extent of what they wanted to do with the dragnet. It wasn't just telephony-carried voice calls they wanted to map, it was all communications a person might make from their phone, which increasingly means a smart phone. It wasn't just call-chaining they wanted to do, it was connection chaining, linking identities, potentially using far more intrusive technological analysis.

Some of that was clear with the initial IC effort at "reform." Significantly, it didn't ask for Call Detail Records, understood to include either phone or Internet or both, but instead "records created as a result of communications of an individual or facility." That language would have permitted the government to get backbone providers to collect all addressing records, regardless if it counted as content. The bill also permitted the use of such tools for all purposes, not just counterterrorism. In effect, this bill would have completed the dragnet, permitting the IC to conduct EO 12333 collection and analysis on records collected in

the US, for any “intelligence” purpose.

But there was enough support for real reform, demonstrated most vividly in the votes on Amash-Conyers in July 2013, that whatever got passed had to look like real reform, so that effort was killed.

So we got the USA F-ReDux model, swapping more targeted collection (of communications, but not other kinds of records, which can still be collected in bulk) for the ability to require providers to hand over the data in usable form. This meant the government could get what it wanted, but it might have to work really hard to do so, as the communications provider market is so fragmented.

The GOP recognized, at least in the weeks before the passage of the bill, that this would be the case. I believe that Richard Burr’s claimed “mistake” in claiming there was an Internet dragnet was instead an effort to create legislative intent supporting an Internet dragnet. After that failed, Burr introduced a last minute bill using John Bates’ Dialing, Routing, Addressing, and Signaling language, meaning it would enable the government to bulk collect packet communications off switches again, along with EO 12333 minimization rules. That failed (in part because of Mitch McConnell’s parliamentary screw ups).

But now the IC is left with a law that does *what it said* it wanted (plus some, as it definitely gets non-telephony “phone” “calls”), rather than one that does *what it wanted*, which was to re-establish the full dragnet it had in the US at various times in the past.

I would expect they won’t stop trying for the latter, though.

Indeed, I suspect that’s the real reason Marco Rubio has been permitted to keep complaining about the dragnet’s shortcomings.