SECTION 215'S MULTIPLE PROGRAMS AND WHERE THEY MIGHT HIDE AFTER JUNE 1

In an column explicitly limited to the phone dragnet, Conor Friedersdorf pointed to a post I wrote about Section 215 generally and suggested I thought the phone dragnet was about to get hidden under a new authority.

> Marcy Wheeler is suspicious that the Obama Administration is planning to continue the dragnet under different authorities.

But my post was about more that just the phone dragnet. It was about two things: First, the way that, rather than go "cold turkey" after it ended the Internet dragnet in 2011 as the AP had claimed, NSA had instead already started doing the same kind of collection using other authorities that — while they didn't collect all US traffic — had more permissive rules for the tracking they were doing. That's an instructive narrative for the phone dragnet amid discussions it might lapse, because it's quite possible that the Intelligence Community will move to doing far less controlled tracking, albeit on fewer Americans, under a new approach.

In addition, I noted that there are already signs that the IC is doing what Keith Alexander said he could live with a year ago: ending the phone dragnet in exchange for cybersecurity information sharing. I raised that in light of increasing evidence that the majority of Section 215 orders are used for things related to cybersecurity (though possibly obtained by FBI, not NSA). If that's correct, Alexander's comment would make sense, because it would reflect that it is working cybersecurity investigations under

protections — most notably, FISC-supervised minimization — all involved would rather get rid of.

Those two strands are important, taken together, for the debate about Section 215 expiration, because Section 215 is far more than the dragnet. And the singular focus of everyone — from the press to activists and definitely fostered by NatSec types leaking — on the phone dragnet as Section 215 sunset approaches makes it more likely the government will pull off some kind of shell game, moving the surveillances they care most about (that is, *not* the phone dragnet) under some new shell while using other authorities to accomplish what they need to sustain some kind of phone contact and connection chaining.

So in an effort to bring more nuance to the debate about Section 215 sunset, here is my best guess — and it is a guess — about what they're doing with Section 215 and what other authorities they might be able to use to do the same collection.

Here are the known numbers on how Section 215 orders break out based on annual reports and this timeline.

Year	Total 215 Orders	Modified	Phone Dragnet
2006	43	4	3
2007	17*		4
2008	13	0	5
2009	21	9	6
2010	96	43	4
2011	205	176	Est. 5
2012	212	200	Est. 4
2013	178	141	Est. 4
2014	Est. 180	NA	5

*Initially, DOJ did not report 11 of these orders.

The Phone Dragnet

Since its transfer under Section 215 in 2006, the phone dragnet has generally made up 4 or 5 orders a year (Reggie Walton imposed shorter renewal periods in 2009 as he was working through the problems in the program). 2009 is the one known year where many of the modified orders — which generally involve imposed

minimization procedures — were phone dragnet orders.

We know that the government believes that if Section 215 were to sunset, it would still have authority to do the dragnet. Indeed, it not only has a still-active Jack Goldsmith memo from 2004 saying it can do the dragnet without any law, it sort of waved it around just before the USA Freedom Act debate last year as if to remind those paying attention that they didn't necessarily think they needed USAF (in spite of comments from people like Bob Litt that they do need a new law to do what they'd like to do).

But that depends on telecoms being willing to turn over the dragnet data voluntarily. While we have every reason to believe AT&T does that, the government's inability to obligate Verizon to turn over phone records in the form it wants them is probably part of the explanation for claims the current dragnet is not getting all the cell records of Americans.

A number of people — including, in part, Ron Wyden and other SSCI skeptics in a letter written last June — think the government could use FISA's PRTT authority (which does not sunset) to replace Section 215, and while they certainly could get phone records using it, if they could use PRTT to get what it wants, they probably would have been doing so going back to 2006 (the difference in authority is that PRTT gets actual activity placed, whereas 215 can only get records maintained (and Verizon isn't maintaining the records the government would like it to, and PRTT could not get 2 hops).

For calls based off a foreign RAS, the government could use PRISM to obtain the data, with the added benefit that using PRISM would include all the smart phone data — things like address books, video messaging, and location — that the government surely increasingly relies on. Using PRISM to collect Internet metadata is one of two ways the government replaced the PRTT Internet dragnet. The government couldn't get 2 hops and couldn't chain off of Americans,

however.

I also suspect that telecoms' embrace of supercookies may provide other options to get the smart phone data they're probably increasingly interested in.

For data collected offshore, the government could use SPCMA, the other authority the government appears to have replaced the PRTT Internet dragnet with. We know that at least one of the location data programs NSA has tested out works with SPCMA, so that would offer the benefit of including location data in the dragnet. If cell phone location data is what has prevented the government from doing what they want to do with the existing phone dragnet, SPCMA's ability to incorporate location would be a real plus for NSA, to the extent that this data is available (and cell phone likely has more offshore availability than land line).

The government could obtain individualized data using NSLs — and it continues to get not just "community of interest" (that is, at least one hop) from AT&T, but also 7 other things that go beyond ECPA that FBI doesn't want us to know about. But using NSLs may suffer from a similar problem to the current dragnet, that providers only have to provide as much as ECPA requires. Thus, there, too, other providers are probably unwilling to provide as much data as AT&T.

Telecoms might be willing to provide data the government is currently getting under 215 under CISA and CISA collection won't be tied in any way to ECPA definitions, though its application is a different topic, cybersecurity (plus leaks and IP theft) rather than terrorism. So one question I have is whether, because of the immunity and extended secrecy provisions of CISA, telecoms would be willing to stretch that?

Other Dragnets

In addition to the phone dragnet, FBI and other IC agencies seem to operate other dragnets under

Section 215. It's probably a decent guess that the 8-13 other 215 orders prior to 2009 were for such things. NYT and WSJ reported on a Western Union dragnet that would probably amount to 4-5 orders a year. Other items discussed involve hotel dragnets and explosives precursor dragnets, the latter of which would have been expanded after the 2009 Najibullah Zazi investigation. In other words, there might be up to 5 dragnets, each representing 4-5 orders a year (assuming they work on the same 90-day renewal cycle), so a total of around 22 of the roughly 175 orders a year that aren't the phone dragnet (the higher numbers for 2006 are known to be combination orders both obtaining subscription data for PRTT orders and location data with a PRTT order; those uses stopped in part with the passage of PATRIOT reauthorization in 2006 and in part with FISC's response to magistrate rulings on location data from that year).

Some of these dragnets could be obtained, in more limited fashion, with NSLs (NSLs currently require reporting on how many US persons are targeted, so we will know if they move larger dragnets to NSLs). Alternately, the FBI may be willing to do these under grand jury subpoenas or other orders, given the way they admitted they had done a Macy's Frago Elite pressure cooker dragnet after the Boston Marathon attack. The three biggest restrictions on this usage would be timeliness (some NSLs might not be quick enough), the need to have a grand jury involved for some subpoenas, and data retention, but those are all probably manageable hurdles.

The Internet content

Finally, there is the Internet content — which we know makes up for a majority of Section 215 orders — that moved to that production from NSLs starting in 2009. It's probably a conservative bet that over 100 of current dragnet orders are for this kind of content. And we know the modification numbers for 2009 through 2011 — and therefore, probably still — are tied to

minimization procedure requirements imposed by the FISC.

A recent court document from a Nicholas Merrill lawsuit suggests this production likely includes URL and data flow requests. And the FBI has recently claimed —for what that's worth — that they rely on Section 215 for cybersecurity investigations.

Now, for some reason, the government has always declined to revise ECPA to restore their ability to use NSLs to obtain this collection, which I suspect is because they don't want the public to know how extensive the collection is (which is why they're still gagging Merrill, 11 years after he got an NSL).

But the data here strongly suggests that going from NSL production to Section 215 production has not only involved more cumbersome application processes, but also added a minimization requirement.

And I guarantee you, FBI or NSA or whoever is doing this must hate that new requirement. Under NSLs, they could just horde data, as we know both love to do, the FBI even more so than the NSA. Under 215s, judges made them minimize it.

As I noted above, *this* is why I think Keith Alexander was willing to do a CISA for 215 swap. While CISA would require weak sauce Attorney General derived "privacy guidelines," those would almost certainly be more lenient than what FISC orders, and wouldn't come with a reporting requirement. Moreover, whereas at least for the phone dragnet, FISC has imposed very strict usage requirements (demanding that a counterterrorism dragnet be used only for counterterrorism purposes), CISA has unbelievably broad application once that data gets collected — not even requiring that terrorist usages be tied to international terrorism, which would seem to be a violation of the *Keith* Supreme Court precedent).

All of this is to suggest that for cybersecurity, IP theft, and leak

investigations, CISA would offer FBI their ideal collection approach. It would certainly make sense that Alexander (or now, Admiral Mike Rogers and Jim Comey) would be willing to swap a phone dragnet they could largely achieve the same paltry results for using other authorities if they in exchange got to access cybersecurity data in a far, far more permissive way. That'd be a no-brainer.

There's just one limitation on this formula, potentially a big one. CISA does not include any obligation. Providers may share data, but there is nothing in the bill to obligate them to do so. And to the extent that providers no longer provide this data under NSLs, it suggests they may have fought such permissive obligation in the past. It would seem that those same providers would be unwilling to share it willingly.

But my thoughts on CISA's voluntary nature are for another post.

One final thought. If the government is contemplating some or all of this, then it represents an effort — one we saw in all versions of dragnet reform to greater (RuppRoge) or lesser degrees (USAF) — to bypass FISC. The government and its overseers clearly seem to think FISC-ordered minimization procedures are too restrictive, and so are increasingly (and have been, since 2009) attempting to replace the role played by an utterly dysfunctional secret court with one entirely within the Executive.

This is the reason why Section 215 sunset can't be treated in a vacuum: because, to the extent that the government could do this in other authorities, it would largely involve bypassing what few restrictions exist on this spying. Sunsetting Section 215 would be great, but only if we could at the same time prevent the government from doing similar work with even fewer controls.