THE REASONS TO SHUT DOWN THE (DOMESTIC) INTERNET DRAGNET: PURPOSE AND DISSEMINATION LIMITS, CORRELATIONS, AND FUNCTIONALITY

Charlie Savage has a story that confirms (he linked some of my earlier reporting) something I've long argued: NSA was willing to shut down the Internet dragnet in 2011 because it could do what it wanted using other authorities. In it, Savage points to an NSA IG Report on its purge of the PRTT data that he obtained via FOIA. The document includes four reasons the government shut the program down, just one of which was declassified (I'll explain what is probably one of the still-classified reasons probably in a later post). It states that SPCMA and Section 702 can fulfill the requirements that the Internet dragnet was designed to meet. The government had made (and I had noted) a similar statement in a different FOIA for PRTT materials in 2014, though this passage makes it even more clear that SPCMA — DOD's self-authorization to conduct analysis including US persons on data collected overseas — is what made the switch possible.

It's actually clear there are several reasons why the current plan is *better* for the government than the previous dragnet, in ways that are instructive for the phone dragnet, both retrospectively for the USA F-ReDux debate and prospectively as hawks like Tom Cotton and Jeb Bush and Richard Burr try to resuscitate an expanded phone dragnet. Those are:

- Purpose and dissemination limits

- Correlations
- Functionality

Purpose and dissemination limits

Both the domestic Internet and phone dragnet limited their use to counterterrorism. While I believe the Internet dragnet limits were not as stringent as the phone ones (at least in pre 2009 shutdown incarnation), they both required that the information only be disseminated for a counterterrorism purpose. The phone dragnet, at least, required someone sign off that's why information from the dragnet was being disseminated.

Admittedly, when the FISC approved the use of the phone dragnet to target Iran, it was effectively authorizing its use for a counterproliferation purpose. But the government's stated admissions — which are almost certainly not true — in the Shantia Hassanshahi case suggest the government would still pretend it was not using the phone dragnet for counterproliferation purposes. The government now claims it busted Iranian-American Hassanshahi for proliferating with Iran using a DEA database rather than the NSA one that technically would have permitted *the search* but not the dissemination, and yesterday Judge Rudolph Contreras ruled that was all kosher.

But as I noted in this SPCMA piece, the only requirement for accessing EO 12333 data to track Americans is a foreign intelligence purpose.

> Additionally, in what would have been true from the start but was made clear in the roll-out, NSA could use this contact chaining for any foreign intelligence purpose. Unlike the PATRIOT-authorized dragnets, it wasn't limited to al Qaeda and Iranian targets. NSA required only a valid foreign intelligence justification for using this data for analysis.

> The primary new responsibility is the requirement:
>
> - *to enter a foreign intelligence (FI) justification for making a query or starting a chain,[emphasis original]*
>
> Now, I don't know whether or not NSA rolled out this program because of problems with the phone and Internet dragnets. But one source of the phone dragnet problems, at least, is that NSA integrated the PATRIOT-collected data with the EO 12333 collected data and applied the protections for the latter authorities to both (particularly with regards to dissemination). NSA basically just dumped the PATRIOT-authorized data in with EO 12333 data and treated it as such. Rolling out SPCMA would allow NSA to use US person data in a dragnet that met the less-restrictive minimization procedures.

That means the government can do chaining under SPCMA for terrorism, counterproliferation, Chinese spying, cyber, or counter-narcotic purposes, among others. I would bet quite a lot of money that when the government "shut down" the DEA dragnet in 2013, they made access rules to SPCMA chaining still more liberal, which is great for the DEA because SPCMA did far more than the DEA dragnet anyway.

So one thing that happened with the Internet dragnet is that it had initial limits on purpose and who could access it. Along the way, NSA cheated those open, by arguing that people in different function areas (like drug trafficking and hacking) might need to help out on

counterterrorism. By the end, though, NSA surely realized it loved this dragnet approach and wanted to apply it to all NSA's functional areas. A key part of the FISC's decision that such dragnets were appropriate is the special need posed by counterterrorism; while I think they might well buy off on drug trafficking and counterproliferation and hacking and Chinese spying as other special needs, they had not done so before.

The other thing that happened is that, starting in 2008, the government started putting FBI in a more central role in this process, meaning FBI's promiscuous sharing rules would apply to anything FBI touched first. That came with two benefits. First, the FBI can do back door searches on 702 data (NSA's ability to do so is much more limited), and it does so even at the assessment level. This basically puts data collected under the guise of foreign intelligence at the fingertips of FBI Agents even when they're just searching for informants or doing other pre-investigative things.

In addition, the minimization procedures permit the FBI (and CIA) to copy entire metadata databases.

> FBI can "transfer some or all such metadata to other FBI electronic and data storage systems," which seems to broaden access to it still further.
>
> > Users authorized to access FBI electronic and data storage systems that contain "metadata" may query such systems to find, extract, and analyze "metadata" pertaining to communications. The FBI may also use such metadata to analyze communications and may upload or transfer some or all such metadata to other FBI electronic and data storage systems for authorized foreign intelligence or law enforcement purposes.

> In this same passage, the definition of metadata is curious.
>
> > For purposes of these procedures, “metadata” is dialing, routing, addressing, or signaling information associated with a communication, but does not include information concerning the substance, purport, or meaning of the communication.
>
> I assume this uses the very broad definition John Bates rubber stamped in 2010, which included some kinds of content. Furthermore, the SMPs elsewhere tell us they’re pulling photographs (and, presumably, videos and the like). All those will also have metadata which, so long as it is not the meaning of a communication, presumably could be tracked as well (and I’m very curious whether FBI treats location data as metadata as well).

Whereas under the old Internet dragnet the data had to stay at NSA, this basically lets FBI copy entire swaths of metadata and integrate it into their existing databases. And, as noted, the definition of metadata may well be broader than even the broadened categories approved by John Bates in 2010 when he restarted the dragnet.

So one big improvement between the old domestic Internet dragnet and SPCMA (and 702 to a lesser degree, and I of course, improvement from a dragnet-loving perspective) is that the government can use it for any foreign intelligence purpose.

At several times during the USA F-ReDux debate, surveillance hawks tried to use the “reform” to expand the acceptable uses of the dragnet. I believe controls on the new system will be looser (especially with regards to emergency

searches), but it is, ostensibly at least, limited to counterterrorism.

One way USA F-ReDux will be far more liberal, however, is in dissemination. It's quite clear that the data returned from queries will go (at least) to FBI, as well as NSA, which means FBI will serve as a means to disseminate it promiscuously from there.

Correlations

Another thing replacing the Internet dragnet with 702 access does it provide another way to correlate multiple identities, which is critically important when you're trying to map networks and track all the communication happening within one. Under 702, the government can obtain not just Internet "call records" and the content of that Internet communication from providers, but also the kinds of thing they would obtain with a subpoena (and probably far more). As I've shown, here are the kinds of things you'd almost certainly get from Google (because that's what you get with a few subpoenas) under 702 that you'd have to correlate using algorithms under the old Internet dragnet.

- a primary gmail account
- two secondary gmail accounts
- a second name tied to one of those gmail accounts
- a backup email (Yahoo) address
- a backup phone (unknown provider) account
- Google phone number
- Google SMS number
- a primary login IP
- 4 other IP logins they were tracking
- 3 credit card accounts

- Respectively 40, 5, and 11 Google services tied to the primary and two secondary Google accounts, much of which would be treated as separate, correlated identifiers

Every single one of these data points provides a potentially new identity that the government can track on, whereas the old dragnet might only provide an email and IP address associated with one communication. The NSA has a great deal of ability to correlate those individual identifiers, but — as I suspect the Paris attack probably shows — that process can be thwarted somewhat by very good operational security (and by using providers, like Telegram, that won't be as accessible to NSA collection).

This is an area where the new phone dragnet will be significantly better than the existing phone dragnet, which returns IMSI, IMEI, phone number, and a few other identifiers. But under the new system, providers will be asked to identify "connected" identities, which has some limits, but will nonetheless pull some of the same kind of data that would come back in a subpoena.

Functionality

While replacing the domestic Internet dragnet with SPCMA provides additional data with which to do correlations, much of that might fall under the category of additional functionality. There are two obvious things that distinguish the old Internet dragnet from what NSA can do under SPCMA, though really the possibilities are endless.

The first of those is content scraping. As the Intercept recently described in a piece on the breathtaking extent of metadata collection, the NSA (and GCHQ) will scrape content for metadata, in addition to collecting metadata directly in transit. This will get you to different kinds of

connection data. And particularly in the wake of John Bates' October 3, 2011 opinion on upstream collection, doing so as part of a domestic dragnet would be prohibitive.

In addition, it's clear that at least some of the experimental implementations on geolocation incorporated SPCMA data.

> I'm particularly interested that one of NSA's pilot co-traveler programs, CHALKFUN, works with SPCMA.
>
> > Chalkfun's Co-Travel analytic computes the date, time, and network location of a mobile phone over a given time period, and then looks for other mobile phones that were seen in the same network locations around a one hour time window. When a selector was seen at the same location (e.g., VLR) during the time window, the algorithm will reduce processing time by choosing a few events to match over the time period. Chalkfun is SPCMA enabled1.
>
> > 1 (S//SI//REL) SPCMA enables the analytic to chain "from," "through," or "to" communications metadata fields without regard to the nationality or location of the communicants, and users may view those same communications metadata fields in an unmasked form. [my emphasis]
>
> Now, aside from what this says about the dragnet database generally (because this makes it clear there is location data in the EO 12333 data available under SPCMA, though that was already clear), it makes it clear there is a way to geolocate US

> persons — because the entire point of SPCMA is to be able to analyze data including US persons, without even any limits on their location (meaning they could be in the US).

That means, in addition to tracking who emails and talks with whom, SPCMA has permitted (and probably still does) permit NSA to track who is traveling with whom using location data.

Finally, one thing we know SPCMA allows is tracking on cookies. I'm of mixed opinion on whether the domestic Internet ever permitted this, but tracking cookies is not only nice for understanding someone's browsing history, it's probably critical for tracking who is hanging out in Internet forums, which is obviously key (or at least used to be) to tracking aspiring terrorists.

Most of these things shouldn't be available via the new phone dragnet — indeed, the House explicitly prohibited not just the return of location data, but the use of it by providers to do analysis to find new identifiers (though that is something AT&T does now under Hemisphere). But I would suspect NSA either already plans or will decide to use things like Supercookies in the years ahead, and that's clearly something Verizon, at least, does keep in the course of doing business.

All of which is to say it's not just that the domestic Internet dragnet wasn't all that useful in its current form (which is also true of the phone dragnet in its current form now), it's also that the alternatives provided far more than the domestic Internet did.

Jim Comey recently said he expects to get more information under the new dragnet — and the apparent addition of another provider already suggests that the government will get more kinds of data (including all cell calls) from more kinds of providers (including VOIP). But there are also probably some functionalities that will

work far better under the new system. When the hawks say they want a return of the dragnet, they actually want both things: mandates on providers to obtain richer data, but also the inclusion of all Americans.