HOW INTERNET DRAGNETTERY GOT WAY MORE PERMISSIVE UNDER PRISM

I'm finally working through the minimization procedures released earlier this month as part of the blitz claiming that the Intelligence Community has made big changes in the year since President Obama's surveillance speech. Here's my first working thread, on FBI's Section 702 minimization procedures (SMPs).

The SMPs provide one sense of why the NSA shut down the Internet dragnet in 2011. As a court filing last year made clear, one of the places the Internet metadata analysis moved to was Section 702. And FBI's SMPs show that collecting and analyzing metadata via PRISM would be far more permissive in a number of ways than doing it under the rules laid out under the PRTT orders.

The first reason is obvious: whereas the PRTT dragnet could only be used for terrorism purposes, FBI can pull metadata from foreign selectors identified for any number of reasons: there are counterterrorism and counterproliferation certificates, as well as a foreign government one that appears to get used very broadly, including to cover hackers, which the government seems to treat as a counterintelligence function.

Moreover, FBI can disseminate metadata results far more broadly. It can disseminate USP data for all foreign intelligence information, which would include counterterrorism, counterproliferation, and (assuming they're treating hacking as a clandestine intelligence activity) hackers. And it can disseminate such metadata analysis to state, local, tribal, and other agencies. There's only protection for USP identities if FBI pulled it for foreign power

purposes (that is, who's chatting with Angela Merkel).

Those receiving the data would be told there are SMPs, but they wouldn't require any training to receive such query results.

And that's all before you consider that 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).

Using PRISM data, it would be far, far easier to "correlate" multiple identities, so as to show (for example) all the people chained off of one person's multiple Google identities, because the providers know these (note, too, this seems to have been something the government started asking Yahoo for months after Protect America Act started).

Then there's retention. While some of the key numbers are redacted, the base retention level for FBI 702 data is 5 years, and for data deemed to have a foreign intelligence purpose it is longer — perhaps as long as the 20 and 30 year retention for FBI records (plus 5 years on the front end). So whereas the NSA had to throw out the underlying data after 4.5 and, for a period, 5 years, they can keep underlying data far longer at the FBI.

Finally, there's tracking. It appears the FBI doesn't have to track the metadata queries it makes at all.

> The FBI shall identify FISA-acquired information in its storage systems, other than those used solely for link analysis of metadata, that has been reviewed and meets those standards.2
>
> 2 Although the FBI need not mark metadata as meeting the retention standards or as having been disseminated, the FBI must still assess whether the metadata meets the requirements for dissemination pursuant to Section V prior to actually disseminating the information.

Indeed, this may be the real problem for FBI's counting of back door searches — that they don't require the tracking of metadata queries at all.

And I think it's possible (though I'm less sure about this) the curious language I noted in USA Freedom Act exempting communications metadata from cloud providers may also hide what isn't already protected under back door searches,

basically not counting this metadata collection as such.

So whereas under the PRTT program the NSA tracked every single metadata query, using PRISM data there'd be almost no tracking at all.

There are, I think, just two limits in using PRISM to do Internet dragnettery (but remember, some of this almost certainly moved overseas under SPCMA as well, which wouldn't have these particular limits). First, depending on how a provider retains their data (and how long a user retains her own communications), the FBI might not have access to 5 years of communications data when it first started tracking someone (though it seems NSA primarily needed 2 years, and given how long people keep email, there'd often be far more than 5 years available).

And finally — and this is a significant one — there's the requirement that the government only target people overseas. So unless FBI is permitted to pull two or three degrees of communication off of targets (and they might be!), it would harder, though not impossible, to show internal communication patterns.

Still, I can see how they'd find the PRTT dragnet to have performance limits. Because, for the purpose of tracking those with ties to known overseas threats, pulling metadata from PRISM would be far permissive if you did it at FBI.