BACK DOOR SEARCHES: ONE OF TWO REPLACEMENTS FOR THE INTERNET DRAGNET?

I said the other day, most of NSA's Civil Liberties and Privacy Office comment to the Privacy and Civil Liberties Oversight Board on Section 702 was disappointing boilerplate, less descriptive than numerous other statements already in the public record.

In the passage on back door searches I looked at, however, there was one new detail that is very suggestive. It said NSA does more back door searches on metadata than on content under Section 702.

> NSA distinguishes between queries of communications content and communications metadata. NSA analysts must provide justification and receive additional approval before a content query using a U.S. person identifier can occur. To date, NSA analysts have queried Section 702 content with U.S. person identifiers less frequently than Section 702 metadata.

Consider what this means. NSA collects content from a selector — say, all the Hotmail communications of ScaryAQAPTerrorist. That content of course includes metadata (setting aside the question of whether this is legally metadata or content for the moment): the emails and IPs of people who were in communication with that scary terrorist.

The NSA is saying that the greater part of their back door searches on US person identifiers — say, searching on the email, "TroubledTeenager@gmail.com" — is just for

metadata.

Given the timing, it seems that they're using back door searches as one of two known replacements for the PRTT Internet dragnet shut down around October 30, 2009, turned on again between July and October 2010, then shut down for good in 2011 (the other being the SPCMA contact chaining of EO 12333 collected data through US person identifiers).

Recall that NSA and CIA first asked for these back door searches in April 2011. That was somewhere between 6 to 9 months after John Bates had permitted NSA to turn the Internet dragnet back on in 2010 under sharply restricted terms. NSA was still implementing their rules for using back door searches in early 2012, just months after NSA had shut down the (domestic) Internet dragnet once and for all.

And then NSA started using 702 collection for a very similar function: to identify whether suspicious identifiers were in contact with known suspicious people.

There are many parts of this practice that are far preferable to the old Internet dragnet.

For starters, it has the benefit of being legal, which the Internet dragnet never was!

Congress and the FISC have authorized NSA to collect this data from the actual service providers targeting on overseas targets. Rather than collecting content-as-metadata from the telecoms — which no matter how hard they tried, NSA couldn't make both legal and effective — NSA collected the data from Yahoo and Microsoft and Google. Since the data was collected as content, it solves the content-as-metadata problem.

And this approach should limit the number of innocent Americans whose records are implicated. While everyone in contact with ScaryAQAPTerrorist will potentially be identified via a backdoor search, that's still less intrusive than having every Americans' contacts collected (though if we can believe the

NSA's public statements, the Internet dragnet always collected on fewer people than the phone dragnet).

That said, the fact that the NSA is presumably using this as a replacement may lead it to task on much broader selectors than they otherwise might have: all of Yemen, perhaps, rather than just certain provinces, which would have largely the same effect as the old Internet dragnet did.

In addition, this seems to reverse the structure of the old dragnet (or rather, replicate some of the problems of the alert system that set off the phone dragnet problems in 2009). It seems an analyst might test a US person identifier — remember, the analyst doesn't even need reasonable articulable suspicion to do a back door search — against the collected metadata of scary terrorist types, to see if the US person is a baddie. And I bet you a quarter this is automated, so that identifiers that come up in, say, a phone dragnet search are then run against all the baddies to see if they also email at the press of a button. And at that point, you're just one more internal approval step away from getting the US person content.

In short, this would seem to encourage a kind of wild goose chase, to use Internet metadata of overseas contact to judge whether a particular American is suspicious. These searches have a far lower standard than the phone and Internet dragnets did (as far as we know, neither the original collection nor the back door search ever require an assertion of RAS). And the FISC is far less involved; John Bates has admitted he doesn't know how or how often NSA is using this.

But it is, as far as we know, legal.