THE CORPORATE STORE: WHERE NSA GOES TO SHOP YOUR CONTENT AND YOUR LIFESTYLE

I'm increasingly convinced that for seven months, we've been distracted by a shiny object, the phone dragnet, the database recording all or almost all of the phone-based relationships in the US over the last five years. We were never wrong to discuss the dangers of the dragnet. It is the equivalent of a nuclear bomb, just waiting to go off. But I'm quite certain the NatSec establishment decided in the days after Edward Snowden's leaks to intensify focus on the actual construction of the dragnet — the collection of phone records and the limits on access to the initial database (what they call the collection store) of them — to distract us away from the true family jewels.

A shiny object.

All that time, I increasingly believe, we should have been talking about the corporate store, the database where queries from the collection store are kept for an undisclosed (and possibly indefinite) period of time. Once records get put in that database, I've noted repeatedly, they are subject to "the full range of [NSA's] analytic tradecraft."

We don't know precisely when that tradecraft gets applied or to how many of the phone identifiers collected in any given query. But we know that tradecraft includes matching individuals' various communication identifiers (which can include phone number, handset identifier, email address, IP address, cookies from various websites) — a process the NSA suggests may not be all that accurate, but whatever! Once NSA links all those identities, NSA can pull together both network maps and additional lifestyle information.

> The agency was authorized to conduct "large-scale graph analysis on very large sets of communications metadata without having to check foreignness" of every e-mail address, phone number or other identifier, the document said.
>
> [snip]
>
> The agency can augment the communications data with material from public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data, according to the documents. They do not indicate any restrictions on the use of such "enrichment" data, and several former senior Obama administration officials said the agency drew on it for both Americans and foreigners.

That analysis might even include tracking a person's online sex habits, if the government deems you a "radicalizer" for opposing unchecked US power, even if you're a US person.

Such profiles are not the only thing included in NSA's "full range of analytic tradecraft."

We also know — because James Clapper told us this very early on in this process — the metadata helps the NSA pick and locate which content to read. The head of NSA's Signals Intelligence Division, Theresa Shea, said this more plainly in court filings last year.

> Section 215 bulk telephony metadata complements other counterterrorist-related collection sources by serving as a significant enabler for NSA intelligence analysis. It assists the NSA in applying limited linguistic resources available to the counterterrorism mission against links

> that have the highest probability of connection to terrorist targets. Put another way, while Section 215 does not contain content, analysis of the Section 215 metadata can help the NSA prioritize for content analysis communications of non-U.S. persons which it acquires under other authorities. Such persons are of heightened interest if they are in a communication network with persons located in the U.S. Thus, Section 215 metadata can provide the means for steering and applying content analysis so that the U.S. Government gains the best possible understanding of terrorist target actions and intentions. [my emphasis]

The NSA prioritizes reading the content that involves US persons. And the NSA finds it, and decides what to read, using the queries that get dumped into the corporate store (presumably, they do some analytical tradecraft to narrow down which particular conversations involving US persons they want to read).

And there are several different kinds of content this might involve: content (phone or Internet) of a specific targeted individual — perhaps the identifier NSA conducted the RAS query with in the first place — already sitting on some NSA server, Internet and in some cases phone content the NSA can go get from providers after having decided it might be interesting, or content the NSA collects in bulk from upstream collections that was never targeted at a particular user.

The NSA is not only permitted to access all of this to see what Americans are saying, but in all but the domestically collected upstream content, it can go access the content by searching on the US person identifier, not the foreign interlocutor, without establishing even Reasonable Articulable Suspicion that it pertains to terrorism (though the analyst does have to claim it serves foreign intelligence purpose). That's important because lots of this

content-collection is not tied to a specific terrorist suspect (it can be tied to a geographical area, for example), so the NSA can hypothetically get to US person content without ever having reason to believe it has any tie to terrorism.

In other words, all the things NSA's defenders have been insisting the dragnet doesn't do — it doesn't provide content, it doesn't allow unaudited searches, NSA doesn't know identities, NSA doesn't data mine it, NSA doesn't develop dossiers on it, even James Clapper's claim that NSA doesn't voyeuristically troll through people's porn habits — every single one is potentially true for the results of queries run three hops off an identifier with just Reasonable Articulable Suspicion of some tie to terrorism (or Iran). Everything the defenders say the phone dragnet is not, the corporate store is.

All the phone contacts of all the phone contacts of all the phone contacts of someone subjected to the equivalent of a digital stop-and-frisk are potentially subject to all the things NSA's defenders assure us the dragnet is not subject to.

Don't get me wrong: I'm not saying some of this analysis isn't appropriate with actual terrorist suspects.

But that's not what the corporate store is. It is — PCLOB estimates — up to 120 million phone users (the actual number of people would be smaller because of burner phones, and a significant number would be foreign numbers), the overwhelming majority of which are completely innocent of anything but being up to 3 degrees away from a guy who got digitally stop-and-frisked.

Yet those potentially millions of Americans get no effective protection once they're in the corporate store. As the PCLOB elaborates,

> Once contained in the corporate store, analysts may further examine these

> records without the need for any new reasonable articulable suspicion determination.
>
> [snip]
>
> Furthermore, under the rules approved by the FISA court, NSA personnel may then search any phone number, including the phone number of a U.S. person, against the corporate store — as long as the agency has a valid foreign intelligence purpose in doing so — without regard to whether there is "reasonable articulable suspicion" about that number. 589 Unlike with respect to the initial RAS query, the FISA court's orders specifically exempt the NSA from maintaining an audit trail when analysts access records in the corporate store. 590

There are just a few protections. The analysts accessing the corporate store need to have undergone training and must claim a foreign intelligence (but not exclusively counterterrorism) purpose. And normally, if NSA wants to circulate the US person data outside of the NSA, a high level official must certify that,

> the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.

Again, that doesn't require the US person have any tie to counterterrorism, just that it be "related to" counterterrorism, which FISC has already deemed even the larger collection store to be by default. (The Executive Branch can also search the corporate store for exculpatory or inculpatory information, which, given that no defendant has succeeded in getting a search for the former, probably means it is only used for

the latter — and note, this is not, apparently, limited to counterterrorism purposes, and as of right now the Executive is also permitted to do back door searches of content for criminal evidence unrelated to terrorism, though Obama has vaguely promised to change that while stopping short of a warrant.)

And no one, aside from PCLOB's estimate of up to 120 million (which may or may not have been reviewed when PCLOB let the IC review some of their process descriptions), is talking about how many Americans are in the corporate store. Geoffrey Stone has said NSA only "touched" 6,000 people in 2012, though that may mean only 6,000 of a much larger number of people who got placed in the corporate store were subjected to further NSA processing. We can assume the numbers were far higher until 2009, when there were over 17,000 on a RAS list. Furthermore, I'm very curious to see whether such numbers spike for 2013, given claims that NSA used the dragnet for "peace of mind" after the Boston Marathon attack, launched by young men who interacted via mobile phone with a huge number of totally innocent US person contacts. Will half of Cambridge, MA be subject to the full range of NSA's tradecraft because we used the dragnet to get peace of mind after the Boston Marathon attack?

Moreover, as discussed last month, the NSA can alter the intake into the corporate store via choices made by data integrity analysts — the other part of the process largely exempted from oversight, and with a few inclusions could cause the bulk of American call records to end up in the corporate store.

Obama said the dragnet "does not involve the NSA examining the phone records of ordinary Americans." But in doing so, he was implying that the millions of Americans whose records may have made it into the corporate store are not ordinary, and therefore not entitled to the kind of due process enshrined in the Constitution.