THE PURPOSE(S) OF THE DRAGNET, REVISITED

As I noted the other day, one basis Judge Richard Leon used to find that the dragnet was likely unconstitutional was that it wasn't all that useful. But I was particularly interested in the evidence he points to to establish that (see page 61 of his ruling), because it and the underlying basis for it reveal far more about how the government uses the dragnet than we've seen.

Leon points to the three cases in which the phone dragnet was supposed to be useful, which he gets from the declaration of FBI Acting Assistant Director Robert Holley. Holley claims the dragnet was useful in the Khalid Ouazzani, David Headley, and Najibullah Zazi cases (though Holley does not mention Ouazzani by name), using the following language.

> In January 2009, using authorized collection under Section 702 of the Foreign Intelligence Surveillance Act to monitor the communications of an extremist overseas with ties to al-Qa'ida, NSA discovered a connection with an individual based in Kansas City. NSA tipped the information to the FBI, which during the course of its investigation discovered that there had been a plot in its early stages to attack the New York Stock Exchange. After further investigation, NSA queried the telephony metadata to ensure that all potential connections were identified, which assisted the FBI in running down leads.
>
> [snip]
>
> At the time of his arrest, Headley and his colleagues, at the behest of al-Qa'ida, were plotting to attack the Danish newspaper that published cartoons depicting the Prophet Mohammed. Headley

> was later charged with support for terrorism based on his involvement in the planning and reconnaissance for the 2008 hotel attack in Mumbai. Collection against foreign terrorists and telephony metadata analysis were utilized in tandem with FBI law enforcement authorities to establish Headley's foreign ties and them in context with his U.S. based planning efforts.
>
> [snip]
>
> NSA received Zazi's telephone number from the FBI and ran it against the Section 215 telephony metadata, identifying and passing additional leads back to the FBI for investigation. One of these leads revealed a previously unknown number for co-conspirator Adis Medunjanin and corroborated his connection to Zazi as well as to other U.S.-based extremists.

First, note what's missing? Any mention of Basaaly Moalin, the **only** defendant for which the government claims the phone dragnet was critical to his identification. Holley may have left Moalin out because of the timing: DOJ submitted his declaration on November 12, the day before the hearing on Moalin's bid for a new trial and two days before Jeffrey Miller's ruling rejecting that. Did DOJ think they might lose that argument, and so left it out out of fear it would make them more likely to lose this one (Leon does acknowledge Miller's ruling in his own). Or was the case just so dated they chose not to mention it?

Whatever the reason, they're left describing three cases in which even Keith Alexander admits the dragnet was at best only helpful.

But note the other thing: Up until now, the government has only described how the dragnet was useful in the Zazi case. While in its

propaganda about 54 plots or maybe just terrorist events thwarted, it has implicitly suggested that only those with a US-nexus could involve the dragnet, I know of no other instance where they made it clear that they sort of used it in the Headley and Ouazzani cases (I'm going to check the declarations in the parallel suits later).

In both cases, it appears, the government only used it after the fact (which is how they used it in the Boston Marathon attack, which bizarrely also goes unmentioned).

They found the claimed NYSE plot (which wasn't really a plot), and only later consulted the dragnet. They arrested Headley (DEA's informant, remember), and then used the dragnet to put this US informant's foreign ties in context.

That at least suggests the possibility that, as the challenge of getting the dragnet reauthorized in 2009, FBI started having its Agents consult the dragnet in any case involving Section 702.

Note one more thing about the language Holley uses: while he describes the telephony metadata consulted in the Zazi case Section 215 data, he calls the others simply telephony metadata. Given what we now know about the way that all metadata collections are accessible from the same interface and NSA analysts are encouraged to use EO 12333 collections when they'll return the same results as a Section 215 query, this raises the distinct possibility that the Ouazzani and Headley queries weren't even technically Section 215 queries. (There are vague hints in other documents that the NSA's "data integrity analysts" may remove informants from the dragnet — which they might do to keep FBI and other federal Agents out of the dragnet — which I may return to later.)

Which means it's not only possible they're doing queries after the fact to be able to say they used the dragnet, but they're technically doing queries of a different dragnet.

I find that slippery language of particular interest given the advantages Holley says the dragnet offers. First, he says the dragnet offers advantages over other possible means of chaining.

> The NSA bulk collection program at issue here presents distinct advantages. The contact chaining capabilities offered by the program exceed the chaining that is performed on data collected pursuant to other means, including traditional means of case-by case intelligence gathering targeted at individual telephone numbers such as subpoena, warrant, national security letter, pen-register and trap-and-trace (PR/TT) devices, or more narrowly defined orders under Section 215.

He lays out what may be just some of the other possibilities (I find it of particular interest that he includes "more narrowly defined orders under Section 215," which suggests they may replicate Section 215 collection for non-counterterrorism uses). But his list doesn't necessarily exclude EO 12333 collected dragnet (which would be broader because it included foreign to foreign contacts, but more narrow because it would not be comprehensive for US contacts).

Holley then points to the the "agility" with which NSA can do second-order chaining (again raising questions why they didn't include Moalin, who was found on a second hop) and the ability to identify chains across multiple providers

> This is so in at least two important respects, namely, the NSA's querying and analysis of the aggregated bulk telephony metadata under this program. First, the agility of querying the metadata collected by NSA under this program allows for more immediate contact chaining, which is significant

> in time-sensitive situations of suspects' communications with known or as-yet unknown co-conspirators. For example, if investigators find a new telephone number when an agent of one of the identified international terrorist organizations is captured, and the Government issues a national security letter for the call details for that particular number, it would only be able to obtain the first tier of telephone number and contacts and, in rare instances, if the second tier of contacts if the FBI separately demonstrates the relevance of the second-generation information to the national security investigation. At least with respect to the vast majority of national security letters issued, new national security letters would have to be issued for telephone numbers identified in the first tier, in order to find an additional tier of contacts. The delay inherent in issuing new national security letters would necessarily mean losing valuable time.
>
> Second, aggregating the NSA telephony metadata from different telecommunications providers enhances and expedites the ability to identify chains of communications across multiple providers. Furthermore, NSA disseminations provided to the FBI from this program may include NSA's analysis informed by its unique capabilities.

This last paragraph is particularly interesting. The reference to "NSA's analysis informed by its unique capabilities" likely refers to stuff the NSA can do once it has deposited queries into the corporate store (all the more so given the reference in the Headley description to "**Collection against foreign terrorists and telephony metadata analysis** were utilized in tandem with FBI law enforcement authorities"),

which far exceed simple chaining.

Which brings me to the declaration of Theresa Shea, the Director of NSA's Signals Intelligence Directorate.

Her declaration is patently dishonest in parts: it doesn't mention the use of dragnet information to identify informants (as opposed to potential terrorists); it doesn't disclose all the violations in 2009 and pretends Congress got timely notice of violations; it doesn't describe the ease with which NSA accesses US person content via back door access; it doesn't admit that NSA lumps and chains phone metadata in with Internet metadata.

But her declaration does provide this description of how NSA uses the dragnet to decide which communications to prioritize.

> 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]

She implies this is used solely with non-US persons, but the example of Moalin, not to mention everything we know about minimization procedures, suggests they use it to read the incidentally collected content of US persons in communication with foreigners, and (in his case) then use that content to establish probable cause to get his content directly.

Now, we've known the government does this for months; both James Clapper and Edward Snowden described using the metadata to find which communications to read (and General Alexander used the same library metaphor Clapper did in last week's SJC hearing).

But this is as close as the government has come to officially admitting that the metadata does, in fact, lead directly to accessing content, that since they collect "everything" — both metadata and content — from at least selected targets, a metadata connection amounts to accessing content.

If that's right, though, it means any US persons whose contacts are deposited into the corporate store are likely to have their contents read (and we know NSA doesn't require Reasonable Articulable Suspicion to do that). The NSA and FBI together got very close to admitting that a system that needs only RAS to initiate intrusive contact chaining serves as the justification — literally "the key" — to access US person content without further RAS. Which would be a remarkably different Fourth Amendment equation than even billions of pen registers, which is what the government wants to pretend this is.

But that's not all. Holley's declaration provides hints about some other ways this contact chaining is used. As I've been predicting for months and months, Holley suggests this data goes into things like No Fly and State and Treasury Terrorist designations — designations that are almost impossible to challenge in court.

> Counter-terrorism investigations serve

> important purposes beyond the ambit of routine criminal inquiries and prosecution, which ordinarily focus retrospectively on specific crimes that have already occurred and the persons known or suspected to have committed them. The key purpose of terrorism investigations, in contrast, to prevent terrorist attacks before they occur. Terrorism investigations also provide the basis for, and inform decisions concerning other measures needed to protect the national security, including: **excluding or removing persons involved in terrorism from the United States; freezing assets of organization that engage in or support terrorism**; securing targets of terrorism; providing threat information and warnings to other federal, state, local, and private agencies and entities; diplomatic or military actions; and actions by other intelligence agencies to counter international terrorism threats. [my emphasis]

While Holley doesn't connect this passage directly with the dragnet, it appears in a declaration about the dragnet. Which means, rather unsurprisingly, that the government may be basing due process free infringements on certain basic privileges — like flying and banking — on the contact chaining including every single American.

Judge Leon only looked at the unconvincing explanations of how the dragnet tied to the three cases presented by the FBI to rule this was probably unconstitutional (he also cited ProPublica's debunking of such claims). He didn't look at any of the far more ominous language in the declarations before him, which hint at — but ultimately stop short of clarity or candor — potentially far greater constitutional problems with the dragnet. Let's hope one of the other judges reviewing these

suits asks for more clarity.