# SUCKY ASSESSMENTS OF THE PHONE DRAGNET REVEAL HOW MUCH THEY'RE KEEPING "SECRET"

The assessments of the phone dragnet suck.

I don't mean the assessments of the phone dragnet show the program sucks, though that may well be the case. I mean the assessments of the phone dragnet I've seen do a very poor job of assessing the value of it. Which serves to show how much of the larger dragnet remains, if not secret, still largely undiscussed.

To see what I mean, consider this post, from Just Security's Ryan Goodman.

**Insiders disagree about the phone dragnet value with outsiders**

The strongest part of his post compares the seemingly contradictory assessments of the phone dragnet by two different members of the NSA Review Group. University of Chicago Professor Geoffrey Stone and Deputy Director of CIA Mike Morell.

Stone, based on what he learned from public sources and from the briefings the Group received, believes the program did not prevent any terrorist attacks. Morell, whose former agency receives Tippers from the program and even had direct access to query results until 2009 just like the FBI does and did (though no one talks about that) insists it has helped prevent terrorist attacks.

Goodman also notes that the Gang of Four immediately defended the phone dragnet after the Review Group released its results (actually, they object to more than the phone dragnet recommendation but don't say what other recommendations they object to), but doesn't

note the terms they use to do so:

> However, a number of recommendations in the report should not be adopted by Congress, starting with those based on the misleading conclusion that the NSA's metadata program is 'not essential to preventing attacks.' **Intelligence programs do not operate in isolation** and terrorist attacks are not disrupted by the work of any one person or program. The NSA's metadata program is a valuable analytical tool that assists intelligence personnel in their efforts to efficiently 'connect the dots' on emerging or current terrorist threats directed against Americans in the United States. **The necessity of this program cannot be measured merely by the number of terrorist attacks disrupted, but must also take into account the extent to which it contributes to the overall efforts** of intelligence professionals to quickly respond to, and prevent, rapidly emerging terrorist threats. [my emphasis]

In other words, Goodman presents evidence that the Gang of Four and a former top CIA official believe there are other reasons the phone dragnet is valuable, while someone relying on limited briefings evaluates the program based on its failure to stop any attack.

That ought to make Goodman ask what Morell and Dianne Feinstein know (or think they know) that Stone does not. It ought to make him engage seriously with their claim that **the phone dragnet is doing something else** beyond providing the single clues to prevent terrorist attacks.

One they're not willing to talk about explicitly.

**Assessments and the terrorist attack thwarted metric**

Instead, Goodman assesses the phone dragnet

solely on the basis of the public excuse offered over and over and over since the Guardian first published the Verizon order in June: to see which Americans are in contact with (alleged) terrorist associates so as to prevent an attack.

Goodman lectures program critics that identifying funders or members of terrorist groups might help find terrorists, too, and "peace of mind" might help dedicate resources most productively.

> The key objective of course is to stop terrorist attacks against the US homeland and vital US interests abroad. An important distinction, however, is whether the intelligence generated by the program is:
>
> (a) "direct": timely information to foil a specific attack; or
>
> (b) "indirect": information that enables the government to degrade a terrorist group or decrease the general likelihood of attacks
>
> **Examples of the latter might include information on individuals who have joined or are funding a terrorist organization**. Intelligence could help to identify and successfully prosecute such individuals, and hence disable them and deter others. The important point is that both types of information aid the overall goal of stopping terrorist attacks. That point appears to have been lost on some critics of the program. When the government cites the latter information yields, critics often consider such situations irrelevant or little to do with stopping attacks.

But Goodman imagines only those affirmatively supporting terrorism would help the government prevent terrorism, which is not necessarily the case.

**Does the NSA's network analysis even pick the right calls?**

One thing missing from such assessments are the failures. Why didn't, for example, Faisal Shahzad's planning with the Pakistani Taliban identify him and his *hawala* before the attack? There are plausible explanations: he used good enough operational security such that he had no communications that could have included in the dragnets, his TTP phone and Internet contacts were not among the services sucked up, the turmoil in the phone and (especially) Internet dragnet in 2009 and 2010 led to gaps in the collection. Then there's a far more serious one: that the methods NSA use to identify numbers of interest may not work, and may instead only be identifying those whose doings with terror affiliates are relatively innocent, meaning they don't use operational security (though note the US-based phone dragnets would use more sophisticated analysis only after data gets put in the corporate store, whereas data collected overseas might be immediately subject to it).

And for those who, like Goodman, place great stock in the dragnet's "peace of mind" metric, they need to assess not just the privacy invasion that might result, but the resources required to investigate all possible leads — which could have been upwards of 36,000 people in the Boston Marathon case.

That is, unless we have evidence that NSA's means of picking the interesting phone contacts from the uninteresting ones works (and given the numbers involved, we probably don't have that), then the dragnet may be as much a time suck as it is a key tool.

**What about the other purposes the Intelligence Community has (quietly) admitted?**

The other problem with assessments of the phone dragnet is they don't even take the IC at its word in its other, quieter admissions of how it uses the dragnet (notably, in none of Stone's five posts on the dragnet does he mention any of

these — one, two, three, four, five — raising questions whether he ever learned or considered them). These uses include:

- Corporate store
- "Data integrity" analysis
- Informants
- Index

Corporate store: As the minimization procedures and a few FISC documents make clear, once the NSA has run a query, the results of that query are placed in a "corporate store," a database of all previous query results.

ACLU's Patrick Toomey has described this in depth, but the key takeaways are once data gets into the corporate store, NSA can use "the full range of SIGINT analytic tradecraft" on it, and none of that activity is audited.

NSA would have you believe very few Americans' data gets into that corporate store, but even if the NSA treats queries it says it does, it could well be in the millions. Worse, if NSA doesn't do what they say they do in removing high volume numbers like telemarketers, pizza joints, and cell voice mail numbers, literally everyone could be in the corporate store. As far as I've seen, the metrics measuring the phone dragnet only involve tips **going out** to FBI and not the gross number of Americans' data going into the corporate store and therefore subject to "the full range of analytic tradecraft," so we (and probably even the FISC) don't know how many Americans get sucked into it. Worse, we don't know what's included in "the full range of SIGINT analytic tradecraft" (see this post for some of what they do with Internet metadata), but we should assume it includes the data mining the government says it's not doing on the database itself.

The government doesn't datamine phone records in the main dragnet database, but they're legally permitted to datamine anyone's phone records who has come within 3 degrees of separation from

someone suspected of having ties to terrorism.

"Data integrity" analysis: As noted, the NSA claims that before analysts start doing more formal queries of the phone dragnet data, "data integrity" analysts standardize it and do something (it's unclear whether they delete or just suppress) "high volume numbers." They also — and the details on this are even sketchier — use this live data to develop algorithms. This has the possibility of significantly changing the dragnet and what it does; at the very least, it risks eliminating precisely the numbers that might be most valuable (as in the Boston Marathon case, where a pizza joint plays a central role in the Tsarnaev brothers' activities). The auditing on this activity has varied over time, but Dianne Feinstein's bill would eliminate it by statute. Without such oversight, data integrity analysts have in the past, moved chunks of data, disaggregated them from any identifying (collection date and source) information, and done … we don't know what with it. So one question about the data integrity analyst position is how narrowly scoped the high volume numbers are (if it's not narrow, then everyone's in the corporate store); an even bigger is what they do with the data in often unaudited behavior before it's place into the main database.

Informants: Then there's the very specific, admitted use of the dragnet that no one besides me (as far as I know) has spoken about: to find potential informants. From the very start of the FISC-approved program, the government maintained the dragnet "may help to discover individuals willing to become FBI assets," and given that the government repeated that claim 3 years later, it does seem to have been used to find informants.

This is an example of a use that would support "connecting the dots" (as the program's defenders all claim it does) but that could ruin the lives of people who have no tie to actual terrorists (aside from speaking on the phone to

someone one or two degrees away from a suspected terror affiliate). The government has in the past told FISCR it might use FISA data to find evidence of other crimes — even rape — to coerce people to become informants, and in some cases, metadata (especially that in the corporate store, enhanced by "the full range of analytic tradecraft") could pinpoint not just potential criminals, but people whose visa violations and extramarital affairs might make them amenable to narcing on the people in their mosque (with the additional side effect of building distrust within a worship community). There's not all that much oversight over FBI's use of informants in any case (aside from permitting us to learn that they're letting their informants commit more and more crimes), so it's pretty safe to assume no one is tracking the efficacy of the informants recruited using the powerful tools of the phone dragnet.

Index: Finally, there's the NSA's use of this metadata as a Dewey Decimal System (to use James Clapper's description) to pull already-collected content off the shelf to listen to — a use even alluded to in the NSA's declarations in suits trying to shut down the dragnet.

> 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]

Don't get me wrong. Given how poorly the NSA has addressed its longterm failure to hire enough translators in target languages, I can understand how much easier it must be to pick what to read based on metadata analysis (though see my concerns, above, about whether the NSA's assessment techniques are valid). But when the NSA says, "non-US persons" here, what they mean is "content collected by targeting non-US persons," which includes a great deal of content of US persons.

Which is another way of saying the dragnet serves as an excuse to read US person content.

And however valuable (or, given the NSA's other failures) necessary that may be, that also opens up a whole new way in which this dragnet infringes on US person privacy. Indeed, "reading already-collected content" almost certainly falls under "the full range of SIGINT analytic tradecraft," which may mean that being caught up in the phone dragnet equates to having your content either back door targeted or reverse targeted. Does the NSA read such indexed content before it sends tips out to the FBI to "start" an investigation? How much does the NSA learn from listening to calls between journalists or ACLU lawyers and people 2 degrees away from terror affiliates?

Now, frankly, all four of these admitted uses of the dragnet might be used to support defenders' or opponents' claims about the dragnet. All of them raise big new privacy concerns (which is surely why the defenders have never laid this out). But they might well provide information that is far more valuable in stopping terror attacks then the phone record of Basaaly Moalin's 2-degree phone contact with Aden Ayro

was.

The point is, no one is talking about these uses of the dragnet. No one. And until they do, commentators shouldn't be lecturing anyone about the adequacy or inadequacy of their dragnet assessment.

Of course, one reason we're not talking about all this is because the program defenders don't want to (I'm certain, for example, that one of the other NSA Group Recommendations the Gang of Four opposes is the requirement of warrants for back door searches, but they won't say that out loud). We don't know the full details of these uses, because they're still shrouded in secrecy. It's not even clear that all members of the NSA Review Group learned full details about them.

Perhaps, then, before people write anymore long posts claiming to assess the phone dragnet, they should be insisting on answers to a lot more questions?

The NSA and its defenders have gone to great lengths to prevent the public from conducting real assessments of the phone dragnet's efficacy. That, by itself, should raise concerns. But it should also make it clear that current assessments are just scratching the surface.