“FACTS MATTER” SAID NSA YAY-MAN MICHAEL HAYDEN WHO TOLD SERIAL LIES ABOUT THE PHONE DRAGNET

I’m not sure if you saw last night’s Munk Debate pitting Glenn Greenwald and Alexis Ohanian against Michael Hayden and Alan Dershowitz. I did a whole slew of fact checking and mockery on twitter last night.

But I wanted to pay particular attention to a string of false claims Hayden made about the phone dragnet program.

First, my hobbyhorse, he claimed the database can only be used for terror. (After 1:08)

> If this program — and here we’re talking about the metadata program — which is about terrorism, because the only reason you can use the metadata is to stop terrorism. No other purpose.

Actually, terrorism and … Iranian “terrorism.” It’s unclear when or why or how Iran got included in database access (though it is considered a state sponsor of terror). But according to Dianne Feinstein and Keith Alexander, analysts can also access the database for Iran-related information. Now, maybe they can only access the Iran data if they claim terror. But that’s a very different thing than claiming a tie to al Qaeda.

The real doozies come later (my transcription; after 1:20:40; I’ve numbered the false claims and provided the “facts matter” below).

> I started out with facts matter. So I assume on the metadata issue we’re talking about the 215 program. About the phone records, alright? Because frankly,

> that's the only bulk metadata NSA has on American citizens. **(1)**
>
> [cross talk]
>
> Accusations fit on a bumper sticker. The truth takes longer. NSA gets from American telephone providers the billing records of American citizens. **(2)** What happens to the billing records is actually really important. I didn't make this phrase up but I'm gonna use it. They put it in a lock box, alright? They put it in a lock box at NSA. **(3)** 22 people at NSA are allowed to access that lockbox. **(4)** The only thing NSA is allowed to do with that truly gajillion record field sitting there is that when they have what's called a seed number, a seed number about which they have reasonable articulable suspicion that that seed number is affiliated with al Qaeda – you roll up a safe house in Yay-Man, he's got pocket litter, that says here's his al Qaeda membership card, he's got a phone you've never seen before. Gee, I wonder how this phone might be associated with any threats in the United States. **(5)** So, I'll be a little cartoonish about this, NSA gets to walk up to the transom and yell through the transom and say hey, anybody talk to this number I just found in Yay-Man? And then, this number, say in Buffalo, says well, yeah, I call him about every Thursday. NSA then gets to say okay Buffalo number – by the way, number, not name – Buffalo number, who did you call. At which point, by description the 215 metadata program is over. That's all NSA is allowed to do with the data. There is no data mining, there's no powerful algorithms chugging through it, trying to imagine relationships. **(6)** It's did that dirty number call someone in the United States. The last year for which NSA had

> full records is 2012 — I'll get the 13 numbers shortly **(7)** — but in 2012, NSA walked up to that transom and yelled "hey! anybody talk to this number?" 288 times. **(8)**

(1) Under the SPCMA authority, NSA can include US persons in contact-chaining of both phone and Internet metadata collected overseas. SPCMA has far fewer of the dissemination and subject matter limitations that the Section 215 dragnet has.

(2) NSA doesn't get the "billing records." It gets routing information, which includes a great deal of data (such as the cell phone and SIM card ID and telecom routing information) that wouldn't be included on a phone bill, even assuming a bill was itemized at all (most local landline calls are not). It also gets the data every day, not every month, like a billing record.

(3) Starting in early January 2008, NSA made a copy of the dragnet data and "for the purposes of analytical efficiency" dumped it in with all their other metadata. That allows them to conduct "federated queries," which is contact chaining across authorities (so chains including both foreign collected EO12333 data and domestic Section 215 data). The NSA coaches its analysts to rerun queries that are replicable in EO12333 alone because of the greater dissemination that permits.

(4) The 22 number refers to the people who can approve an identifier for Reasonable Articulable Suspicion, not the people who can conduct queries. Those 22 are:

> the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate.

While we don't know how many analysts are trained on Section 215 dragnet right now, the number was 125 in August 2010.

But even those analysts are not the only people who can access the database. "Technicians" may do so too.

> Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes, but the results of any such queries ill not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes.

And this access — which requires access to the raw metadata — is not audited.

(5) Note, in the past, the government has also accessed the database with "correlated" identifiers — phone numbers and SIM cards associated with the same person. It's unclear what the current status of querying on correlated identifiers is, but that is likely the topic of one of the FISC opinions the

government is withholding, and the government is withholding the opinion in question in the name of protecting an ongoing functionality.

(6) Hayden pretends there's a clear boundary to this program, but even the FISC minimization procedures for it approve the corporate store, where these query results — people 2 degrees from someone subjected to a digital stop-and-frisk — may be subjected to "the full range of [NSA's] analytic tradecraft." So when Hayden says there's no data mining and no powerful algorithms, he's lying about the data mining and powerful algorithms (and content access) that are permitted for identifiers in the corporate store.

(7) Given that DOJ has already released their numbers for FISA use in 2013, I presume it also has the number of identifiers that have been queried.

(8) The 288 number refers to the number of identifiers queried, not the number of queries run. Given that the dragnet serves as a kind of alert system — to see who has had contracts with a certain number over time — the number of actual queries is likely significantly higher, as most of the identifiers were likely run multiple times.