“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.

THE NSA'S RETROACTIVE DISCOVERY OF TAMERLAN TSARNAEV

In the days after the Boston Marathon attack last year, NSA made some noise about expanding its domestic surveillance so as to prevent a similar attack.

But in recent days, we've gotten a lot of hints

that NSA may have just missed Tamerlan Tsarnaev.

Consider the following data points.

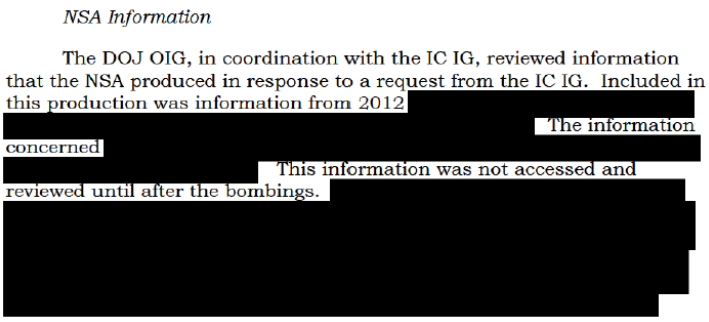
First, in a hearing on Wednesday, Intelligence Community Inspector General Charles McCullough suggested that the forensic evidence found after the bombing might have alerted authorities to Tamerlan Tsarnaev's radicalization.

> Senator Tom Carper: If the Russians had not shared their initial tip, would we have had any way to detect Tamerlan's radicalization?
>
> [McCullough looks lost.]
>
> Carper: If they had not shared their original tip to us, would we have had any way to have detected Tamerlan's radicalization? What I'm getting at here is just homegrown terrorists and our ability to ferret them out, to understand what's going on if someone's being radicalized and what its implications might be for us.
>
> McCullough: Well, the Bureau's actions stemmed from the memo from the FSB, so that led to everything else in this chain of events here. You're saying if that memo didn't exist, would he have turned up some other way? I don't know. I think, in the classified session, we can talk about some of the post-bombing forensics. What was found, and that sort of thing. And you can see when that radicalization was happening. So I would think that this would have come up, yes, at some point, it would have presented itself to law enforcement and the intelligence community. Possibly not as early as the FSB memo. It didn't. But I think it would have come up at some point noting what we found post-bombing.

Earlier in the hearing (around 11:50), McCullough described reviewing evidence "that

was within the US government's reach before the bombing, but had not been obtained, accessed, or reviewed until after the bombing" as part of the IG Report on the attack. So some of this evidence was already in government hands (or accessible to it as, for example, GCHQ data might be).

We know some of this evidence not accessed until after the bombing was at NSA, because the IG Report says so. (See page 20)



NSA Information

The DOJ OIG, in coordination with the IC IG, reviewed information that the NSA produced in response to a request from the IC IG. Included in this production was information from 2012 [redacted] The information concerned [redacted] This information was not accessed and reviewed until after the bombings. [redacted]

That may or may not be the same as the jihadist material Tamerlan posted to YouTube in 2012, which some agency claims could have been identified as Tamerlan even though he used a pseudonym for some of the time he had the account.

> The FBI's analysis was based in part on other government agency information showing that Tsarnaev created a YouTube account on August 17, 2012, and began posting the first of several jihadi-themed videos in approximately October 2012. The FBI's analysis was based in part on open source research and analysis conducted by other U.S. government agencies shortly after the bombings showing that Tsarnaev's YouTube account was created with the profile name "Tamerlan Tsarnaev." After reviewing a draft of this report, the FBI commented that Tsarnaev's YouTube display name changed from "muazseyfullah" to "Tamerlan Tsarnaev" on or about February 12, 2013, and suggested that therefore Tsarnaev's YouTube account could not be located

> using the search term “Tamerlan Tsarnaaev” before that date.20 The DOJ OIG concluded that because another government agency was able to locate Tsarnaev’s YouTube account through open source research shortly after the bombings, the FBI likely would have been able to locate this information through open source research between February 12 and April 15, 2013. The DOJ OIG could not determine whether open source queries prior to that date would have revealed Tsarnaev to be the individual who posted this material.
>
> 20 In response to a DOJ OIG request for information supporting this statement, the FBI produced a heavily redacted 3-page excerpt from an unclassified March 19, 2014, EC analyzing information that included information about Tsarnaev’s YouTube account. The unredacted portion of the EC stated that YouTube e-mail messages sent to Tsarnaev’s Google e-mail account were addressed to “muazseyfullah” prior to February 12, 2013, and to “Tamerlan Tsarnaev” beginning on February 14, 2013. The FBI redacted other information in the EC about Tsarnaev’s YouTube and Google e-mail accounts.

The FBI may not have been able to connect “muazseyfullah” with Tamerlan, but that’s precisely what the NSA does with its correlations process; it has a database that does just that (though it’s unclear whether it would have collected this information, especially given that it postdated the domestic Internet dragnet being shut down).

Finally, there’s the matter of the Anwar al-Awlaki propaganda.

> An FBI analysis of electronic media showed that the computers used by Tsarnaev contained a substantial amount

> of jihadist articles and videos, including material written by or associated with U.S.-born radical Islamic cleric Anwar al-Aulaqi. On one such computer, the FBI found at least seven issues of *Inspire*, an on-line English language magazine created by al-Aulaqi. One issue of this magazine contained an article entitled, "Make a Bomb in the Kitchen of your Mom," which included instructions for building the explosive devices used in the Boston Marathon bombings.
>
> Information learned through the exploitation of the Tsarnaev's computers was obtained through a method that may only be used in the course of a full investigation, which the FBI did not open until after the bombings.

The FBI claims they could only find the stuff on Tamerlan's computer using methods available in full investigations (this makes me wonder whether the FBI uses FISA physical search warrants to remotely search computer hard drives).

But that says nothing about what NSA (or even FBI, back in the day when they had the full time tap on Awlaki, though it's unclear what kind of monitoring of his content they've done since the government killed him) might have gotten via a range of means, including, potentially, upstream searches on the encryption code for Inspire.

In other words, there's good reason to believe — and the IC IG seems to claim — that the government had the evidence to know that Tamerlan was engaging in a bunch of reprehensible speech before he attacked the Boston Marathon, but they may not have reviewed it.

Let me be clear: it's one thing to know a young man is engaging in reprehensible but purportedly protected speech, and another to know he's going

to attack a sporting event.

Except that this purportedly protected speech is precisely — almost exactly — the kind of behavior that has led FBI to sic multiple informants and/or undercover officers on other young men, including Adel Daoud and Mohamed Osman Mohamud, even in the absence of a warning from a foreign government.

And they didn't here.

Part of the issue likely stems from communication failures between FBI and NSA. The IG report notes that "the relationship between the FBI and the NSA" was one of the most relevant relationships for this investigation. Did FBI (and CIA) never tell the NSA of the Russian warning? And clearly they never told NSA of his travel to Russia.

But part of the problem likely stems from the way NSA identifies leads — precisely the triaging process I examined here. That is, NSA is going to do more analysis on someone who communicates with people who are already targeted. Obviously, the ghost of Anwar al-Awlaki is one of the people targeted (though the numbers of young men who have Awlaki's propaganda is likely huge, making that a rather weak identifier). The more interesting potential target would be William Plotnikov, the Canadian-Russian boxer turned extremist whom Tamerlan allegedly contacted in 2012 (and it may be this communication attempt is what NSA had in its possession but did not access until after the attacks). But I do wonder whether the NSA didn't prioritize similar targets in countries of greater focus, like Yemen and Somalia.

It'd be nice to know the answer to these questions. It ought to be a central part of the debate over the NSA and its efficacy or lack thereof. But remember, in this case, the NSA was specifically scoped out of the heightened review (as happened after 9/11, which ended up hiding the good deal of warning the NSA had before the attack).

We've got a system that triggers on precisely the same kind of speech that Tamerlan Tsarnaev engaged in before he attacked the Marathon. But it didn't trigger here.

Why not?

THE PROMISE [SIC] OF BIG DATA

22 pages into the White House report on Big Data, this paragraph appears:

> Government keeps the peace. It makes sure our food is safe to eat. It keeps our air and water clean. The laws and regulations it promulgates order economic and political life. Big data technology stands to improve nearly all the services the public sector delivers.

It presents several claims that are arguably not at all true:

- Government keeps the peace (where? South Chicago? Iraq? Wall Street?)
- Government makes our food safe to eat (with the few inspectors who inspect factory farms? with federal guidelines that don't combat obesity?)
- Government keeps our air and water clean (I'm more comfortable with this claim, until you consider we're melting the planet with

stuff in the air that government doesn't want to regulate)
- Government laws order economic and political life (they may well, but is that order just and good?)

And that, the report says, is all made possible because of BigData.

Some 15 pages later, after it has reviewed the top secret DHS database analyzing all our public called Cerberus, has admitted the government needs to rethink the meaning of metadata across both intelligence and non-intelligence functions, and explained the new continuous evaluation systems to root out insider threats, the report again proclaims Big Data's good.

> When wrestling with the vexing issues big data raises in the public sector, it can be easy to lose sight of the tremendous opportunities these technologies offer to improve public services, grow the economy, and improve the health and safety of our communities. These opportunities are real and must be kept at the center of the conversation about big data.

Meanwhile, the report offers up these other signs of Big Data progress:

- Big data "is also enabling some of the nearly 29 percent of Americans who are 'unbanked' or 'underbanked' [often because of Big Data] to qualify for a line of credit by using a wider range of non-traditional information—such as rent

payments, utilities, mobile-phone subscriptions, insurance, child care, and tuition—to establish creditworthiness."

- "Home appliances can now tell us when to dim our lights from a thousand miles away."
- "Powerful algorithms can unlock value in the vast troves of information available to businesses, and can help empower consumers."
- "The advertising-supported Internet creates enormous value for consumers by providing access to useful services, news, and entertainment at no financial cost."

In short, the whole thing is rather breathless about Big Data.

And in spite of the fact that respondents to a totally unscientific (not Big Data) survey said they were most concerned about intelligence (first) and law enforcement (second), the Big Data report avoided much of the discussion about this,relegating it to discussions of local law enforcement's use of predictive analysis.

And where they do describe surveillance, it's either to boast about how good the security is on their database, as they do for DHS' curiously named "Cerberus" database, or to pretend big data doesn't dominate there, too.

> Today, most law enforcement uses of metadata are still rooted in the "small data" world, such as identifying phone

> numbers called by a criminal suspect. In the future, metadata that is part of the "big data" world will be increasingly relevant to investigations, raising the question of what protections it should be granted. While today, the content of communications, whether written or verbal, generally receives a high level of legal protection, the level of protection afforded to metadata is less so.
>
> Although the use of big data technologies by the government raises profound issues of how government power should be regulated, big data technologies also hold within them solutions that can enhance accountability, privacy, and the rights of citizens. These include sophisticated methods of tagging data by the authorities under which it was collected or generated; purpose- and user-based access restrictions on this data; tracking which users access what data for what purpose; and algorithms that alert supervisors to possible abuses.

And there are a slew of places in the report — where it talks about HIPAA without talking about using Section 215s to get HIPAA data, where it talks about FCRA without talking about NSLs to get financial data, where it neglects to mention NCTC's ability to get federal databases, including those of DHS — where it remains silent about the surveillance piggybacking on the issue at hand.

Perhaps the most frustrating part of the report — aside from the fact that it actually had to advance the recommendation that we only use Big Data collected in schools for educational purposes (setting aside how well or poorly Big Data is serving our students) — is the silence about the things we don't use Big Data for enough, notably solving the financial crisis and regulating banksters (including things like tax

havens, inequality, and shadow banking), or really doing something about climate change.

Big Data, as it appears in the report (as presented by a bunch of boosters) is not something we're going to throw at our most intractable problems. We're just going to use it to turn the lights off on the other side of the country.

And to spy.

THE TRIAGE DOCUMENT

Accompanying a new story on GCHQ/NSA cooperation yesterday, the Intercept released one of the most revealing documents about NSA spying yet. It describes efforts to use Identifier Scoreboard to triage leads such that analysts spend manual time only with the most promising leads. Basically, the NSA aims to use this process to differentiate the 75% of metadata they collect that is interesting but not of high interest into different categories for further analysis.

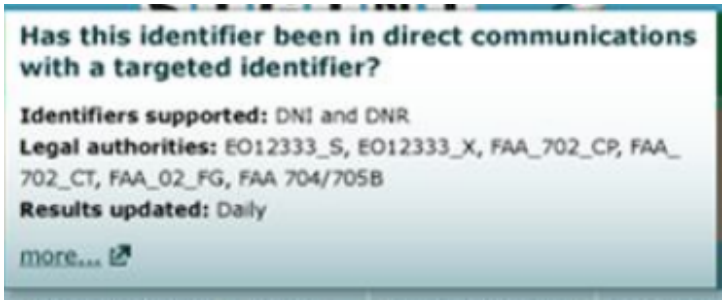
It does so by checking the leads — which are identifiers like email addresses and phone numbers — against collected data (and this extends beyond just stuff collected on the wires; it includes captured media) to see what kind of contacts with existing targets there have been. Not only does the system pull up what prior contacts of interest exist, but also what time frame those occurred and in what number. From there, the analyst can link directly to either the collected knowledge about a target **or the content**.

Before I get into the significance, a few details.

First, the system works with both phone and Internet metadata. That's not surprising, and it

does not yet prove they're chaining across platforms. But it is another piece of evidence supporting that conclusion.

More importantly, look at the authorities in question:



First, FAA. The CP and CT are almost certainly certificates, the authority to collect on counterproliferation and counterterrorism targets. But note what's not there? Cybersecurity, the third known certificate (there was a third certificate reapproved in 2011, so it was active at this time). Which says they may be using that certificate differently (which might make sense, given that you'd be more interested in forensic flows, but this triage system is used with things like TAO which presumably include cyber targets).

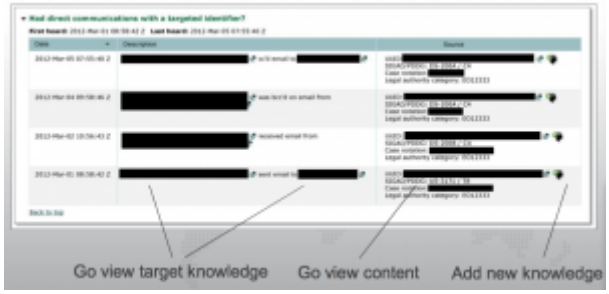
There is, however, a second kind of FAA, "FG." That may be upstream or it may be something else (FG could certainly stand for "Foreign Government, which would be consistent with a great deal of other data). If it's something else, it supports the notion that there's some quirk to how the government is using FAA that differs from what they've told PCLOB and the Presidential Review Group, which have both said there are just those 3 certificates.

Then there's FAA 704/705B. This is collection on US person overseas. Note that FAA 703 (collection on US person who is located overseas but the collection on whom is in the US) is not included. Again, this shows something about how they use these authorities.

Finally, there are two EO12333s. In other slides, we've seen an EO12333 and an EO123333

SPCMA (which means you can collect and chain through Americans), and that may be what this is. Update: One other possibility is that this distinguishes between EO12333 data collected by the US and by second parties (the Five Eyes).

Now go to what happens when an identifier has had contact with a target — and remember, these identifiers are just random IDs at this point.



The triage program automatically pulls up prior contacts with targets. Realize what this is? It's a backdoor search, conducted off an identifier about which the NSA has little knowledge.

And the triage provides a link directly from that the metadata describing when the contact occurred and who initiated it **to the content**.

When James Clapper and Theresa Shea describe the metadata serving as a kind of index that helps prioritize what content they read, this is part of what they're referring to. That — for communications involving people who have already been targeted under whatever legal regime — the metadata leads directly to the content. (Note, this triage does not apparently include BR FISA or PRTT data — that is, metadata collected in the US — which says there are interim steps before such data will lead directly to content, though if that data can be replicated under EO 12333, as analysts are trained to do, it could more directly lead to this content.)

So they find the identifiers, search on prior contact with targets, then pull up that data, at least in the case of EO12333 data. (Another caution, these screens date from a period when NSA was just rolling out its back door search

authorities for US persons, and there's nothing here that indicates these were US persons, though it does make clear why — as last year's audit shows — NSA has had numerous instances where they've done back door searches on US person identifiers they didn't know were US person identifiers.)

Finally, look at the sources. The communications identified here all came off EO12333 communications (interestingly, this screen doesn't ID whether we're looking at EO12333_X or _S data). As was noted to me this morning, the SIGADS that are known here are offshore. But significantly, they include MUSCULAR, where NSA steals from Google overseas.

That is, this screen shows NSA matching metadata with metadata and content that they otherwise might get under FAA, legally, within the US. They're identifying that as EO12333 data. EO12333 data, of course, gets little of the oversight that FAA does.

At the very least, this shows the NSA engaging in such tracking, including back door searches, off a bunch of US providers, yet identifying it as EO12333 collection.

Update: Two more things on this. Remember NSA has been trying, unsuccessfully, to replace its phone dragnet "alert" function since 2009 when the function was a big part of its violations (a process got approved in 2012, but the NSA has not been able to meet the terms of it technically, as of the last 215 order). This triage process is similar — a process to use with fairly nondescript identifiers to determine whether they're worth more analysis. So we should assume that, while BR FISA (US collected phone dragnet) information is not yet involved in this, the NSA aspires to do so. There are a number of reasons to believe that moving to having the providers do the initial sort (as both the RuppRoge plan offered by the House Intelligence Committee and Obama's plan do) would bring us closer to that point.

Finally, consider what this says about probable cause (especially if I'm correct that EO12333_S is the SPMCA that includes US persons). Underlying all this triage is a theory of what constitutes risk. It measures risk in terms of conversations —how often, how long, how many times — with "dangerous" people. While that may well be a fair measure in some cases, it may not be (I've suggested, for example, that people who don't know they may be at risk are more likely to speak openly and at length, and those conversations then serve as a kind of camouflage for the truly interesting, rare by operational security conversations). But this theory (though not this particular tool) likely lies behind a lot of the young men who've been targeted by FBI.

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.

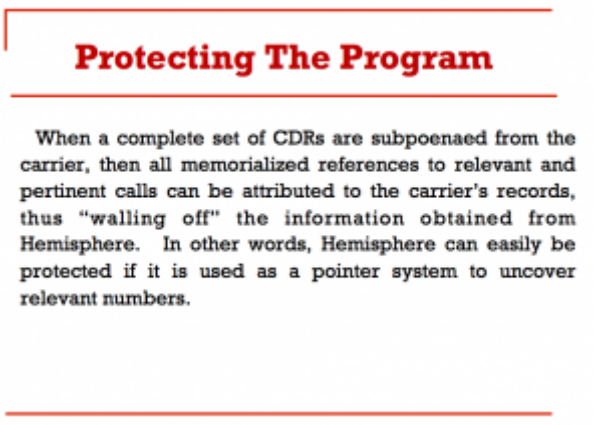
In addition, this seems to reverse the structure of the old dragnet (or rather, replicate some of the problems of the alert system that set off the phone dragnet problems in 2009). It seems an analyst might test a US person identifier — remember, the analyst doesn't even need reasonable articulable suspicion 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.

DOJ INSPECTOR GENERAL INVESTIGATING DEA'S USE OF PARALLEL CONSTRUCTION UNDER HEMISPHERE



Protecting The Program

When a complete set of CDRs are subpoenaed from the carrier, then all memorialized references to relevant and pertinent calls can be attributed to the carrier's records, thus "walling off" the information obtained from Hemisphere. In other words, Hemisphere can easily be protected if it is used as a pointer system to uncover relevant numbers.

As I noted in my last post, DOJ's Inspector General recently created a page showing their ongoing investigations. It shows some things not described in Inspector General Michael Horowitz' last report to Congress.

Of particular interest is this investigation.

> ### *Administrative Subpoenas*
>
> The OIG is examining the DEA's use of administrative subpoenas to obtain broad collections of data or information. The review will address the legal authority for the acquisition or use of these data collections; the existence and effectiveness of any policies and procedural safeguards established with respect to the collection, use, and retention of the data; the creation, dissemination, and usefulness of any products generated from the data; and the use of "parallel construction" or other techniques to protect the confidentiality of these programs.

The description doesn't say it, but this is Hemisphere, the program under which DEA submits administrative subpoenas to AT&T for phone records from any carrier that uses AT&T's backbone. DEA gets information matching burner phones as well as the call records. In addition, it gets some geolocation — and continued to increase what it was getting even after US v Jones raised concerns about such tracking.

The presentation on Hemisphere makes it very clear the government uses "parallel construction" to hide Hemisphere.

> Protecting the Program: When a complete set of CDRs are subpoenaed from the carrier, then all memorialized references to relevant and pertinent calls can be attributed to the carrier's records, thus "walling off" the information obtained from Hemisphere. In other words, Hemisphere can easily be protected if it is used as a pointed system to uncover relevant numbers.

> Exigent Circumstances – Protecting the Program: In special cases, we realize that it might not be possible to obtain subpoenaed phone records that will "wall off" Hemisphere. In these special circumstances, the Hemisphere analyst should be contacted immediately. The analyst will work with the investigator and request a separate subpoena to AT&T.
>
> Official Reporting – Protecting the Program: All requestors are instructed to never refer to Hemisphere in any official document. If there is no alternative to referencing a Hemisphere request, then the results should be referenced as information obtained from an AT&T subpoena.

And this is not the only area where DEA Is using parallel construction to hide where it gets its investigative leads. Reuters reported in August that DEA also uses parallel construction to hide the leads it gets from purportedly national security-related wiretapping.

> A secretive U.S. Drug Enforcement Administration unit is funneling information from intelligence intercepts, wiretaps, informants and a massive database of telephone records to authorities across the nation to help them launch criminal investigations of Americans.
>
> Although these cases rarely involve national security issues, documents reviewed by Reuters show that law enforcement agents have been directed to conceal how such investigations truly begin – not only from defense lawyers but also sometimes from prosecutors and judges.
>
> The undated documents show that federal agents are trained to "recreate" the investigative trail to effectively cover

> up where the information originated, a practice that some experts say violates a defendant's Constitutional right to a fair trial. If defendants don't know how an investigation began, they cannot know to ask to review potential sources of exculpatory evidence — information that could reveal entrapment, mistakes or biased witnesses.
>
> [snip]
>
> The two senior DEA officials, who spoke on behalf of the agency but only on condition of anonymity, said the process is kept secret to protect sources and investigative methods. "Parallel construction is a law enforcement technique we use every day," one official said. "It's decades old, a bedrock concept."
>
> A dozen current or former federal agents interviewed by Reuters confirmed they had used parallel construction during their careers. Most defended the practice; some said they understood why those outside law enforcement might be concerned.

Presuming that Horowitz is investigating whether DEA's extensive use of parallel construction complies with the Constitution (and not, as is possible, whether the sources of this information are being adequately buried), this is welcome news indeed.

But it's also one of several reasons why I'm particularly alarmed, in retrospect, that Horowitz is complaining about his ability to get grand jury information without having to get either Attorney General Holder or Deputy Attorney General James Cole to personally approve it.

After all, the only way you can learn what truly happens in prosecutions that have used parallel construction to hide their sources is to work

backward from the actual prosecution. That would require seeing what the grand jury saw, and what DEA and other agencies had before they got to the grand jury stage. Furthermore, understanding how DEA uses parallel construction would require really broad access to investigations, as drug cases involve large networks of people. That's a lot of requests for information Horowitz would, under the current system, be required to get.

And there's one more thing that likely makes this problem even worse.

As NYT reported in its story on Hemisphere, the actual database is not funded by DEA, but rather by the White House Drug Czar (ONDCP) under the High Intensity Drug Trafficking Area program.

> Mr. Fallon said that "the records are maintained at all times by the phone company, not the government," and that Hemisphere "simply streamlines the process of serving the subpoena to the phone company so law enforcement can quickly keep up with drug dealers when they switch phone numbers to try to avoid detection."
>
> He said that the program was paid for by the D.E.A. and the White House drug policy office but that the cost was not immediately available.
>
> Officials said four AT&T employees are now working in what is called the High Intensity Drug Trafficking Area program, which brings together D.E.A. and local investigators — two in the program's Atlanta office and one each in Houston and Los Angeles.

This has always seemed like a ploy to put the program — which parallels earlier dragnet efforts done solely on Executive authority — in the White House, where it is immune from FOIA and even Congressional oversight.

I can well imagine DEA arguing that Horowitz

cannot touch anything having to do with HIDTA (and therefore with Hemisphere) because it is a White House, not DEA, program. (Note, in Horowitz' testimony he said, in addition to his difficulties getting grand jury information, "We have had similar issues raised regarding our access to some other categories of documents.") Horowitz's investigation of the "legal authority" for the program may well be stymied by claims of Executive Privilege too.

Michael Horowitz appears to be attempting to conduct a badly needed investigation that examines potentially grave Constitutional problems with our Drug War. Will Eric Holder permit him to do that work?

Update: I neglected to link to this post from bmaz right after the Reuters report came out. As he says, DEA has been doing this for decades. Also, read this post describing a case EFF and ACLU are intervening in, in which there is no legal process shown for a lot of the phone records provided in discovery. This is probably the kind of case we're looking at with Hemisphere.

DROPBOX TURNS TO CONDI RICE TO HELP PROTECT USERS' RIGHTS OVERSEAS

On Wednesday, cloud server company DropBox named Condi Rice to its board, touting her brilliance and even her service as Secretary of State, but not her role as George Bush's National Security Advisor during the period he rolled out his most abusive policies.

> Finally, **we're proud to welcome Dr. Condoleezza Rice to our Board of**

> **Directors**. When looking to grow our board, we sought out a leader who could help us expand our global footprint. Dr. Rice has had an illustrious career as Provost of Stanford University, board member of companies like Hewlett Packard and Charles Schwab, and former United States Secretary of State. We're honored to be adding someone as brilliant and accomplished as Dr. Rice to our team.

The privacy community is predictably unimpressed by the involvement of someone so closely tied to civil liberties abuses.

> Dropbox CEO Drew Houston didn't mention the appointment during his keynote at a press event on Wednesday, but a day later, Rice's arrival had eclipsed the rest of the company's carefully crafted public event. Unsurprisingly, some people aren't too happy about the move. Over on Hacker News, a leading barometer for what's on the minds of tech geeks, the day's most popular link connects toDropDropbox, a new site calling on users to boycott the company unless it removes Rice.
>
> The campaign's apparently anonymous creators are calling for her removal in part because of her support for the Bush administration's warrantless wiretapping program, including claims that Rice herself authorized eavesdropping on UN Security Council members. "Why on earth would we want someone like her involved with Dropbox, an organization we are trusting with our most important business and personal data?" the site asks.

DropBox has now responded by claiming it takes someone with Condi's international experience – experience which includes involvement in illegal wiretapping and torture – to protect the rights

of DropBox's hoped-for international customers.

> We're honored to have Dr. Rice join our board — she brings an incredible amount of experience and insight into international markets and the dynamics that define them. As we continue to expand into new countries, **we need that type of insight to help us reach new users and defend their rights**. [my emphasis]

I guess Condi's involvement in harming the rights of so many people overseas makes her an expert on how to protect them?

FINGERPRINTS AND THE PHONE DRAGNET'S SECRET "CORRELATIONS" ORDER

Yesterday, I noted that ODNI is withholding a supplemental opinion approved on August 20, 2008 that almost certainly approved the tracking of "correlations" among the phone dragnet (though this surely extends to the Internet dragnet as well).

I pointed out that documents released by Edward Snowden suggest the use of correlations extends well beyond the search for "burner" phones.

At almost precisely the same time, Snowden was testifying to the EU. The first question he answered served to clarify what "fingerprints" are and how XKeyscore uses them to track a range of innocent activities. (This starts after 11:16, transcription mine.)

> It has been reported that the NSA's XKeyscore for interacting with the raw signals intercepted by mass surveillance programs allow for the creation of something that is called "fingerprints."
>
> I'd like to explain what that really means. The answer will be somewhat technical for a parliamentary setting, but these fingerprints can be used to construct **a kind of unique signature** for any individual or group's communications which are often **comprised of a collection of "selectors" such as email addresses, phone numbers, or user names**.
>
> This allows State Security Bureaus to instantly identify the movements and activities of you, your computers, or other devices, your personal Internet accounts, or even key words or other uncommon strings that indicate an individual or group, out of all the communications they intercept in the world are associated with that particular communication. Much like a fingerprint that you would leave on a handle of your door or your steering wheel for your car and so on.
>
> However, though that has been reported, that is the smallest part of the NSA's fingerprinting capability. You must first understand that any kind of Internet traffic that passes before these mass surveillance sensors can be analyzed in a protocol agnostic manner – metadata and content, both. And it can be today, right now, searched not only with very little effort, via a complex regular expression, which is a type of shorthand programming. But also via any algorithm an analyst can implement in popular high level programming languages. Now, this is very common for technicians. It not a significant work load, it's quite easy.

> This provides a capability for analysts to do things like associate unique identifiers assigned to untargeted individuals via unencrypted commercial advertising networks through cookies or other trackers – common tracking means used by businesses everyday on the Internet – with personal details, such as individuals' precise identity, personal identity, their geographic location, their political affiliations, their place of work, their computer operating system and other technical details, their sexual orientation, their personal interests, and so on and so forth. There are very few practical limitations to the kind of analysis that can be technically performed in this manner, short of the actual imagination of the analysts themselves.
>
> And this kind of complex analysis is in fact performed today using these systems. I can say, with authority, that the US government's claim that "keyword filters," searches, or "about" analysis, had not been performed by its intelligence agencies are, in fact, false. I know this because I have personally executed such searches with the explicit authorization of US government officials. And I can personally attest that these kind of searches may scrutinize communications of both American and European Union citizens without involvement of any judicial warrants or other prior legal review.
>
> What this means in non-technical terms, more generally, is that I, an analyst working at NSA, or, more concerningly, an analyst working for a more authoritarian government elsewhere, can without the issue of any warrant, create an algorithm that for any given time period, with or without human

> involvement, sets aside the communications of not only targeted individuals, but even a class of individual, and that just indications of an activity — or even just indications of an activity that I as the analyst don't approve of — something that I consider to be nefarious, or to indicate nefarious thoughts, or pre-criminal activity, even if there's no evidence or indication that's in fact what's happening. that it's not innocent behavior. The nature of the mass surveillance — of these mass surveillance technologies — create a de facto policy of assigning guilt by association rather than on the basis of specific investigations based on reasonable suspicion.
>
> Specifically, mass surveillance systems like XKeyscore provide organizations such as the NSA with the technical ability to trivially track entire populations of individuals who share any trait that is discoverable from unencrypted communications. For example, these include religious beliefs, political affiliations, sexual orientations, contact with a disfavored individual or group, history of donating to specific or general causes, interactions of transactions with certain private businesses, or even private gun ownership. It is a trivial task, for example, to generate lists of home addresses for people matching the target criteria. Or to collect their phone numbers, to discover their friends, or even, to analyze the proximity and location of their social connections by automating the detection of factors such as who they share pictures of their children with, which is capable of machine analysis.
>
> I would hope that this goes without

> saying, but let me be clear that the NSA is not engaged in any sort of nightmare scenarios, such as actively compiling lists of homosexual individuals to round them up and send them into camps, or anything of that sort. However, they still deeply implicate our human rights. We have to recognize that the infrastructure for such activities has been built, and is within reach of not just the United States and its allies, but of any country today. And that includes even private organizations that are not associated with governments.
>
> Accordingly, we have an obligation to develop international standards, to protect against the routine and substantial abuse of this technology, abuses that are ongoing today. I urge the committee in the strongest terms to bear in mind that this is not just a problem for the United States, or the European Union, but that this is in fact a global problem, not an isolated issue of Europe versus the Five Eyes or any other [unclear]. These technical capabilities don't merely exist, they're already in place and actively being used without the issue of any judicial warrant. I state that these capabilities are not yet being used to create lists of all the Christians in Egypt, but let's talk about what they are used for, at least in a general sense, based on actual real world cases that I can assert are in fact true.
>
> Fingerprints — for example, the kind used of XKeyscore — have been used — I have specific knowledge that they have been used — to track and intercept, to track, intercept, and monitor the travels of innocent citizens, who are not suspected of anything worse than booking a flight. This was done, in Europe, against EU citizens but it is of

> course not limited to that geographic region, nor that population. Fingerprints have also been used to monitor untold masses of people whose communications transit the entire country of Switzerland over specific routes. They're used to identify people — Fingerprints are used to identify people who have had the bad luck to follow the wrong link on an Internet site, on an Internet forum, or even to download the wrong file. They've been used to identify people who simply visit an Internet sex forum. They've also been used to monitor French citizens who have never done anything wrong other than logging into a network that's suspected of activity that's associated with a behavior that the National Security Agency does not approve of.
>
> This mass surveillance network, constructed by the NSA, which, as I pointed out, is an Agency of the US military Department of Defense, not a civilian agency, and is also enabled by agreements with countries such as the United Kingdom, Australia, and even Germany, is not restricted for being used strictly for national security purposes, for the prevention of terrorism, or even for foreign intelligence more broadly.
>
> XKeyscore is today secretly being used for law enforcement purposes, for the detection of even non-violent offenses, and yet this practice has never been declared to any defendant or to any open court.
>
> We need to be clear with our language. These practices are abusive. This is clearly a disproportionate use of an extraordinarily invasive authority, an extraordinarily invasive means of investigation, taken against entire

> populations, rather than the traditional investigative standard of using the least intrusive means or investigating specifically named targets, individuals, or groups. The screening of trillions — I mean that literally, trillions — of private communications for the vaguest indications of associations or some other nebulous pre-criminal activity is a violation of the human right to be free from unwarranted interference, to be secure in our communications and our private affairs, and it must be addressed. These activities — routine, I point out, unexceptional activities that happen every day — are only a tiny portion of what the Five Eyes are secretly doing behind closed doors, without the review, consent, or approval of any public body. This technology represents the most significant — what I consider the most significant.new threat to civil rights in modern times.

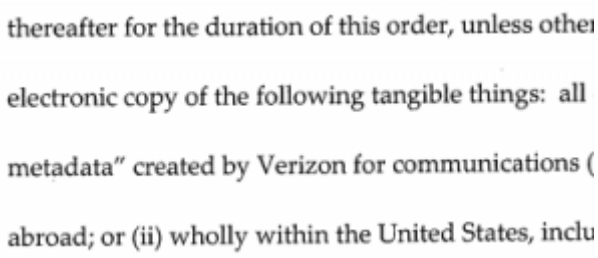
Now, this doesn't guarantee that the NSA correlates identifiers to dump them into XKeyscore (which is, as far as I know, used only on data collected outside the US; the "about" 702 collection is a more limited version of what is done in the US, with returned data likely dumped into databases used with XKeyscore). But Snowden makes it clear such fingerprints involve precisely the identifiers, including phone numbers, used in the domestic dragnets.

Moreover, we know that data in the corporate store — all those people who are two or three degrees away from someone who has been digitally stop-and-frisked — is subject to all the analytical authorities the NSA uses, which clearly includes fingerprinting and use in XKeyscore.

"Correlations" — as the NSA uses in language with the FISC and Congress — are almost certainly either fingerprints, or subset of the fingerprinting process.

And this is, almost certainly, what the government is hiding in that August 20, 2008 order.

JAMES CLAPPER DOESN'T WANT YOU TO KNOW ABOUT VERIZON'S FOREIGN METADATA PROBLEM HE ALREADY TOLD YOU ABOUT


thereafter for the duration of this order, unless othe

electronic copy of the following tangible things: all

metadata" created by Verizon for communications (

abroad; or (ii) wholly within the United States, inclu

Back in September, I noted that the September 3, 2009 phone dragnet Order turned production from a particular telecom back on; it had been turned off in the July 8, 2009 Primary Order.

> In addition, the Custodian of Records of [redacted] shall produce to NSA upon service of the appropriate Secondary Order an electronic copy of the same tangible things created by [redacted] for the period from 5:11 p.m. on July 9, 2009 to the date of this Order, to the extent those records still exist.

In January, after ODNI exposed Verizon's name as the provider directed in all Primary Orders since May 2009 to provide only its non-foreign call records, I laid out when and how the

problem of one provider's foreign data records appears in FISA dragnet orders.

> Up until at least March 5, 2009, all the telecoms were addressed in one paragraph starting, "the Custodian of Records." Starting on May 29, 2009, that's split out into two paragraphs, with the original Custodian of Records paragraph and the one we know to be specific to Verizon. We don't have the following order, dated July 8, 2009, but we know that order shut down production from one provider because it was also producing foreign-to-foreign data; that production was restarted on September 3, 2009.

EFF apparently asked ODNI to formally declassify the parts of that September 3 order, and ODNI unsurprisingly objects.

Though, if it were not already clear this is Verizon we're talking about, a footnote explains,

> All Secondary Orders have been withheld in their entirety as any attempt to redact the identity of the service providers in these Secondary Orders, in compilation with other documents that have been declassified, i.e., the BR 13-80 Primary Order and Verizon Secondary Order, would allow a reader to ascertain the identity of the provider simply by looking at the size of the redacted/blocked material, or comparing any redacted Secondary Order with other classified documents.

The only Secondary Order we have is for Verizon. And as a fairly accomplished redaction comparer, I can confirm that comparing redactions and text blocks only works for the same text. So this footnote only makes sense if the provider in question is Verizon.

In spite of the fact that ODNI already (briefly)

released Verizon's name as the provider in question and exacerbated it with this footnote I'm not surprised they're trying to deny this request.

I am, however, intrigued by the language they use to fight the request, given that we're talking about whether Verizon provides foreign call records under a domestic program.

> The identity of any company ordered to provide call detail records to the NSA clearly relates to "any function of the National Security Agency," 50 U.S.C. §3605. Indeed, it relates to relates to one of the NSA's primary functions, its SIGINT mission. NSA's SIGINT responsibilities include establishing and operating an effective unified organization to conduct SIGINT activities as set forth in E.O. 12333, section 1.7(c), as amended. In performing its SIGINT mission, NSA exploits foreign electromagnetic signals to obtain intelligence information necessary to the national defense, national security, and the conduct of foreign affairs. NSA has developed a sophisticated worldwide SIGINT collection network that acquires, among other things, foreign and international electronic communications. The technological infrastructure that supports NSA's foreign intelligence information collection network has taken years to develop at a cost of billions of dollars and untold human effort. It relies on sophisticated collection and processing technology.
>
> Pursuant to its SIGINT mission, and as authorized by the FISC, NSA quickly analyzes past connections and chains communications through telephony metadata collected pursuant to Section 215. Unless the data is aggregated, it may not be feasible to detect chains of

> communications that cross communication networks. The ability to query accumulated telephony metadata significantly increases the NSA's ability to rapidly detect persons affiliated with the identified foreign terrorist organizations who might otherwise go undetected.

From there, ODNI's declaration goes on to claim that if Verizon's name were made public, the bad guys would know to avoid Verizon. Which is sort of nonsense, given the reports that Verizon provides not just their own customers' records, but also those that transit their backbone.

But I do find it interesting that, in a discussion about hiding the name of a telecom that was accidentally turning over some significant amount of entirely foreign call records under a program that — because it was targeted at domestic users — subjected those records to greater oversight than the foreign records turned over under EO 12333, ODNI started with a discussion of its EO 12333 authorized overseas collection. Particularly given that we know Verizon provides an enormous amount of that overseas collection.

That is, ODNI says that they can't reveal Verizon was the provider that accidentally provided foreign call records under a domestic order — in spite of the fact that they already did — because if they do it will endanger its overseas collection.

THE AUGUST 20, 2008 CORRELATIONS OPINION

On August 18, 2008, the government described to the FISA

Court how it used a particular tool to establish correlations between identifiers. (see page 12)

> A description of how [name of correlations tool] is used to correlate [description of scope of metadata included] was included in the government's 18 August 2008 filing to the FISA Court,

On August 20, 2008, the FISC issued a supplemental opinion approving the use of "a specific intelligence method in the conduct of queries (term "searches") of telephony metadata or call detail records obtained pursuant to the FISC's orders under the BR FISA program." The government claims that it cannot release any part of that August 20, 2008 opinion, which given the timing (which closely tracks with the timing of other submissions and approvals before the FISC) and the reference to both telephony metadata and call detail records almost certainly approves the use of the dragnet – and probably not just the phone dragnet – to establish correlations between a target's multiple communications identifiers.

As ODNI's Jennifer Hudson described in a declaration in the EFF suit, the government maintains that it cannot release this opinion, in spite of (or likely because of) ample description of the correlations function elsewhere in declassified documents.

> The opinion is only six pages in length and the specific intelligence method is discussed at great length in every paragraph of this opinion, including the title. Upon review of this opinion, I have determined that there is no meaningful, segregable, non-exempt information that can be released to the plaintiff as the entire opinion focuses on this intelligence method. Even if the name of the intelligence method was redacted, the method itself could be deduced, given other information that the DNI has declassified pursuant to the President's transparency initiative and the sophistication of our Nation's adversaries **[Ed: did she just call me an "adversary"?!?]** and foreign intelligence services.
>
> [snip]
>
> The intelligence method is used to conduct queries of the bulk metadata, and if NSA were no longer able to use this method because it had been compromised, NSA's ability to analyze bulk metadata would itself be compromised. A lost or reduced ability to detect communications chains that link to identifiers associated with known and suspected terrorist operatives, which can lead to the identification of previously unknown persons of interest in support of anti-terrorism efforts both within the United States and abroad, would greatly impact the effectiveness of this program as there is no way to know in advance which numbers will be responsive to the authorized queries.

ACLU's snazzy new searchable database shows that this correlations function was discussed in at least three of the officially released documents thus far: in the June 25, 2009 End-to-End Review, in a June 29, 2009 Notice to the House

Intelligence Committee, and in the August 19, 2009 filing submitting the End-to-End Review to the FISC.

In addition to making it clear this practice was explained to the FISC just before the Supplemental Opinion in question, these documents also describe a bit about the practice.

They define what a correlated address is (and note, this passage, as well as other passages, do not limit correlations to telephone metadata — indeed, the use of "address" suggests correlations include Internet identifiers).

> The analysis of SIGINT relies on many techniques to more fully understand the data. One technique commonly used is correlated selectors. A communications address, or selector, is considered correlated with other communications addresses when each additional address is shown to identify the same communicant as the original address.

They describe how the NSA establishes correlations via many means, but primarily through one particular database.

> NSA obtained [redacted] correlations from a variety of sources to include Intelligence Community reporting, but the tool that the analysts authorized to query the BR FISA metadata primarily used to make correlations is called [redacted].
>
> [redacted] — a database that holds correlations [redacted] between identifiers of interest, to include results from [redacted] was the primary means by which [redacted] correlated identifiers were used to query the BR FISA metadata.

They make clear that NSA treated all correlated

identifiers as RAS approved so long as one identifier from that user was RAS approved.

> In other words, if there: was a successful RAS determination made on any one of the selectors in the correlation, all were considered .AS-a. ,)roved for purposes of the query because they were all associated with the same [redacted] account

And they reveal that until February 6, 2009, this tool provided "automated correlation results to BR FISA-authorized analysts." While the practice was shut down in February 2009, the filings make clear NSA intended to get the automated correlation functions working again, and Hudson's declaration protecting an ongoing intelligence method (assuming the August 20, 2008 opinion does treat correlations) suggests they have subsequently done so.

When this language about correlations first got released, it seemed it extended only so far as the practice — also used in AT&T's Hemisphere program — of matching call circles and patterns across phones to identify new "burner" phones adopted by the same user. That is, it seemed to be limited to a known law enforcement approach to deal with the ability to switch phones quickly.

But both discussions of the things included among dragnet identifiers — including calling card numbers, handset and SIM card IDs — as well as slides released in stories on NSA and GCHQ's hacking operations (see above) make it clear NSA maps correlations very broadly, including multiple online platforms and cookies. Remember, too, that NSA analysts access contact chaining for both phone and Internet metadata from the same interface, suggesting they may be able to contact chain across content type. Indeed, NSA presentations describe how the advent of smart phones completely breaks down the distinction between phone and Internet metadata.

In addition to mapping contact chains and identifying traffic patterns NSA can hack, this correlations process almost certainly serves as the glue in the dossiers of people NSA creates of individual targets (this likely only happens via contact-chaining after query records are dumped into the corporate store).

Now it's unclear how much of this Internet correlation the phone dragnet immediately taps into. And my assertion that the August 20, 2008 opinion approved the use of correlations is based solely on … temporal correlation. Yet it seems that ODNI's unwillingness to release this opinion serves to hide a scope not revealed in the discussions of correlations already released.

Which is sort or ridiculous, because far more detail on correlations have been released elsewhere.