THE IMMEDIATE PHONE DRAGNET FIXES OBAMA REJECTED

In its report, PCLOB makes it clear that President Obama had most of its recommendations before he gave his speech last Friday.

> PCLOB briefed senior White House staff on the Board's tentative conclusions on December 5, 2013. The PCLOB provided a near final draft of the Board's conclusions and recommendations on Section 215 and the operations of the FISA court (Parts 5, 7 and 8 of this Report) to the White House on January 3, the transparency section (Part 9) on January 8, 2014, and additional statutory analysis on January 14, 2014 (Part 5). On January 8, the full Board met with the President, the Vice President and senior officials to present the Board's conclusions and the views of individual Board members.

Which means Obama was well aware of the four recommendations PCLOB made on immediate privacy fixes (they emphasize these recommendations don't require Congressional or FISC action).

> The Board recommends that the government immediately implement several additional privacy safeguards to mitigate the privacy impact of the present Section 215 program. The recommended changes can be implemented without any need for congressional or FISC authorization. Specifically, the government should:
>
> (a) reduce the retention period for the bulk telephone records program from five years to three years;
>
> (b) reduce the number of "hops" used in contact chaining from three to two;

> (c) submit the NSA's "reasonable articulable suspicion" determinations to the FISC for review after they have been approved by NSA and used to query the database; and
>
> (d) require a "reasonable articulable suspicion" determination before analysts may submit queries to, or otherwise analyze, the "corporate store," which contains the results of contact chaining queries to the full "collection store."

So it's safe to assume President Obama affirmatively rejected the 2 recommendations he did not adopt in any form: reducing the retention period for dragnet data and requiring RAS to search the corporate store.

Noted.

PCLOB REPORT, WORKING THREAD

The report is here. I will do a running update of my comments. Page references will be to the report page numbers, not PDF.

(4) Note PCLOB had access to "various inspector general reports."

(6) Note the dates when WH got these conclusions.

(9) PCLOB confirms what I was the first to point out: this program operated without a legal opinion until July 2013. Told ya so.

(10) One of four reasons the program is illegal is bc 215 is written for FBI, not NSA. Also says it violates ECPA.

(11) PCLOB says FBI would have found Moalin w/o the dragnet. Remember, they were investigating

his hawala and had a tap on Ayro.

(14) PCLOB confirms only two cases (info sharing/minimization and Yahoo) ever got to FISCR.

(15) On the govt's so-called transparency:

> However, to date the official disclosures relate almost exclusively to specific programs that had already been the subject of leaks, and we must be careful in citing these disclosures as object lessons for what additional transparency might be appropriate in the future.

(17) PCLOB provides several immediate relationships and notes that Obama doesn't need Congress to do them.

(19) Note PCLOB's reference to releasing opinions on programs that have been discontinued bc of continuing relevance. Suspect this refers to more than just the Internet dragnet.

(25) Note PCLOB says the data integrity analysts take out "other unwanted data" in addition to high volume numbers. I believe some sensitive numbers are purged at this step.

(30) PCLOB dances around saying that corporate store leads right to content.

> For instance, such calling records may be integrated with data acquired under other authorities for further analysis

(31) PCLOB notes FBI gets reports on the dragnet. It doesn't mention CIA and NCTC or other agencies.

(32) CIA and NCTC have no minimization rules for data that comes from 215 reports:

> Other federal agencies also receive information from the NSA that was obtained through Section 215, but the FISA court's orders do not establish

> rules for how those agencies must handle the information they receive.83 In addition, the government has informed the FISA court that it may provide telephone numbers derived from the program to "appropriate . . . foreign government agencies."84

(33) PCLOB notes that FISC doesn't say what kind of training the dragnet people must get. As a former training professional, their training sucks ass.

(34) Nice description of the monthly reports.

(40) The phrasing for the description of what happened with the Internet dragnet is very interesting.

> After several years of operation, which included significant incidents of noncompliance with the FISA court's orders, the bulk collection of Internet metadata under FISA court approval was terminated. Upon concluding that the program's value was limited, the NSA did not seek to renew it.

(40) PCLOB points to the USA Today reporting on the phone dragnet program to explain the telecom urgency for a legal order. That was May 10, the first dragnet order was May 24. They did it in two weeks.

(41) PCLOB makes it clear the government was already planning on moving to Section 215 when the extension was passed in 2006.

> The collection of telephone records under the President's Surveillance Program was classified, however, and the government's plans to seek new legal authority for that collection were not made public. Thus, congressional debates about the terms on which Section 215 should be renewed included no public discussion of the fact that the

> executive branch was planning to place the NSA's bulk calling records program under the auspices of the reauthorized statute.

(43) Note reference to John Scott Redd.

(44) PCLOB distinguishes the phone dragnet from the Internet one bc the latter was only taking circuits commonly used by terrorist traffic.

(45) The reference to minimization procedures and 2702 in succession makes it clear that Walton's December 2008 response on 2702 was a response to Glenn Fine's IG Report.

(46) Note the [sic] on numbers in the footnote.

(47) PCLOB, like I did, points out the 2009 problems came from continuing features of the illegal program.

(54) Here's a list of the other violations in the phone dragnet. I suspect they're described in the orders the Admin is still withholding.

> The isolated incidents reported to the FISA court comprised the following violations: (1) The NSA inadvertently received a tiny amount of cell site location information from a provider on one occasion (the data was accessible only to technical personnel and was never available to intelligence analysts); (2) An analyst performed a query on a selection term whose RAS approval had expired earlier that month (the agency responded with technical modifications to prevent such incidents); (3) A RAS determination was made based on what was later discovered to be incorrect information (the resulting query results were destroyed, and no intelligence reports were issued based on the query); (4) On several occasions analysts shared the results of queries via email with NSA personnel who were not authorized to receive such

> information (the agency responded with new procedures for email distribution); (5) An analyst sent an email message containing information derived from the Section 215 data to the wrong person, due to a typographical error in the email address (the recipient reportedly deleted the message without reading it, recognizing the error); (6) Information about U.S. persons was on three occasions disseminated outside the NSA before any official made the determinations that are required for such disseminations (officials later concluded that the standards for dissemination were satisfied in each case); (7) The government filed nine reports with the FISA court that lacked certain information required to be in such reports (the missing information involved no wrongdoing or noncompliance, and it subsequently was furnished to the court); (8) The government filed a compliance report with the FISA court on a Monday, instead of on the deadline the previous Friday.
>
> The two other noncompliance incidents were more far-reaching, although both represented inadvertent violations. In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in

> question was not available to intelligence analysts.
>
> In the other incident, the NSA discovered that it had unintentionally received a large quantity of customer credit card numbers from a provider. These related to cases in which a customer used a credit card to pay for a phone call. This problem, which involved cases in which customers used credit cards to pay for phone calls, resulted from a software change implemented by the provider without notice to the NSA. In response to the discovery, the NSA masked the credit card data so that it would not be viewable for intelligence analysis. It also asked providers to give advance notice of changes that might affect the data transmitted to the NSA. The agency later eliminated the credit card data from its analytic stores, although the data remained in the agency's non-analytic online stores and in back-up tapes. Despite repeated efforts to attempt a technical fix, six months later the agency was still receiving a significant amount of credit card information from the provider. As a result of additional efforts, this was reduced to fewer than five credit card numbers per month, and the provider continued to work to eliminate such production entirely.

(58) My favorite line so far:

> Notably, Section 215 requires that records sought be relevant to 'an' authorized investigation.

(61) The PCLOB smackdown on the legal logic behind the dragnet is delightful (is anyone here familiar enough w/Wald's judicial style to tell me whether this is all her?). The passage on "necessity" is important because it pushes back

on underlying claims in OLC memos.

(65) We keep talking about the scope of the data NSA gets. This suggests it's closer to "all."

> As to that type of record, however, the government seeks access to virtually everything.

(69) Ow. I always suspected the White Paper citations on civil discovery were manufactured. PCLOB rips it to shreds.

(73) FN 267 argues Govt has a burden to show relevance. Somewhere, FISC even argued they were presumed regular.

(74) Note reference to House Report on PATRIOT debate—govt was looking for administrative subpoenas.

(80) Reading PCLOB's discussion of the need to have a belief makes me realize that belief was used as the same kind of dodge in the 215 argument as it was in the torture context.

(82) PCLOB calls the phone dragnet "an ongoing surveillance tool." Someone alert DiFi.

(94) PCLOB notes that NSL standards for phone metadata are actually higher than 215 standards. Given my suspicion FBI uses bulk NSLs for subscribe info, I find that partiularly interesting.

(96) I believe I've made this point too: given that there was no judicial opinion that approved the dragnet before it was reauthorized, Congress cannot be said to have authorized it.

(96) I like this:

> Applying the reenactment doctrine to legitimize the government's interpretation of Section 215, therefore, is both unsupported by legal precedent and unacceptable as a matter of democratic accountability.

(97) PCLOB is unaware that the Executive had not complied w/FAA requirements to share legal opinions on at least some of the Section 215 materials. (98) Hahaha! PCLOB did, at least, note that HPSCI did not pass on the 2011 notice to Congress. (99) PCLOB again suggests that the dragnet is designed to collect all call data.

> While the briefing paper explains that the NSA's program operates "on a very large scale" and involves "substantially all" of the calling records generated by "certain" telephone companies, it does not make explicit that the program is designed to collect the records of essentially all telephone calls.

(103) A novel idea:

> And we recommend as a policy matter that all three branches of government, in developing and assessing data collection programs, look beyond the application of cases decided in a very different environment and instead consider how to preserve the underlying constitutional principles in the face of modern communications technology and surveillance capabilities.

(133) PCLOB suggests the only thing protecting the dranget (in, for example, Amnesty v Clapper) from a First Amendment review is standing.

> However, in the cases decided so far, the Court has not reached the underlying question of whether the First Amendment has been violated, because the Court has found that the individuals challenging the surveillance program are not legally entitled to do so because they are unable to show that they are directly affected by the monitoring.

(140) PCLOB associates the Exigent Letters IG Report to this program. Says AT&T provided 2

hops on community of interest. Note the observation that AT&T could do 2 hops is new and not in unredacted text.

(144) PCLOB makes clear what I've been saying: the phone dragnet leads to the content.

> Any attempt to assess the value of the NSA's telephone records program must be cognizant of a few considerations. First, the information that the NSA obtains through Section 215 is not utilized in a vacuum. Rather, it is combined with information obtained under different legal authorities, including the Signals Intelligence that the NSA captures under Executive Order 12333, traditional wiretaps and other electronic surveillance of suspects conducted under FISA court authority, the interception of telephone calls and emails authorized by the FISA Amendments Act of 2008, the collection of communications metadata through FISA's pen register and trap and trace provision, physical surveillance, and the development of informants. The intelligence community views the NSA's Section 215 program as complementing and working in tandem with these and other intelligence sources, enabling analysts to paint a more comprehensive a picture when examining potential national security threats.

(155) PCLOB raises a point I have: why didn't the dragnet find the other unsuccessful attacks?

> Yet, it is worth noting that the program supplied no advance notice of attempted attacks on the New York City subway, the failed Christmas Day airliner bombing, or the failed Times Square car bombing.

(182) Note PCLOB met with John Bates. Interesting that neither PCLOB nor the Review

Group were very sympathetic to FISC concerns.

(193) Mike Rogers has been warned.

> We expect to return to transparency in our future work.

(205) On 12333

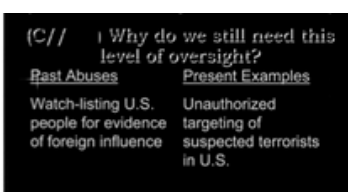
> Our suggestions here focus on FISA authorities and are also relevant to National Security Letters. Our recommendations do not address reporting of activities under Executiv e Order 12333. It has become clear in recent months that E.O. 12333 collection poses important new questions in the age of globalized communications networks, but the Board has not yet attempted to address those issues.

(210) One of Brand's excuses for why PCLOB shouldn't weigh in on law?

> This legal question will be resolved by the courts, not by this Board, **which does not have the benefit of traditional adversarial legal briefing** and is not particularly well – suited to conducting de novo review of long – standing statutory interpretations

---

PROJECT MINARET 2.0: NOW, WITH 58% MORE ILLEGAL TARGETING!



For weeks, I have been trying to figure out why the NSA, in a training program it created in August 2009, likened one of its "present abuses" to Project Minaret. What "unauthorized targeting of suspected terrorists in the US" had they been doing, I wondered, that was like "watch-listing U.S. people for evidence of foreign influence."

Until, in a fit of only marginally related geekdom, I re-read the following passage in Keith Alexander's declaration accompanying the End-to-End review submitted to the FISA Court on August 19, 2009 (that is, around the same time as the training program).

> Between 24 May 2006 and 2 February 2009, NSA Homeland Mission Coordinators (HMCs) or their predecessors concluded that approximately 3,000 domestic telephone identifiers reported to Intelligence Community agencies satisfied the RAS standard and could be used as seed identifiers. However, at the time these domestic telephone identifiers were designated as RAS-approved, **NSA's OGC had not reviewed and approved their use as "seeds" as required by the Court's Orders**. NSA remedied this compliance incident by re-designating all such telephone identifiers as non RAS-approved for use as seed identifiers in early February 2009. NSA verified that although some of the 3,000 domestic identifiers generated alerts as a result of the Telephony Activity Detection Process discussed above, none of those alerts resulted in reports to Intelligence Community agencies. 7
>
> 7 The alerts generated by the Telephony Activity Detection Process did not then and does not now, feed the NSA counterterrorism target knowledge database described in Part I.A.3 below. [my emphasis]

As I'll explain below, this passage means 3,000

US persons were watch-listed without the NSA confirming that they hadn't been watch-listed because of their speech, religion, or political activity.

Here's the explanation.

The passage actually appears in an entirely different part (PDF 37, document 81) of Alexander's declaration from his discussion of the alert list violations (PDF 30, document 74) that started the review of the phone dragnet program. But given the February (2009) timing and the discussion of Telephony Activity Detection alerts, this passage clearly addresses alerts violations.

Before I parse the passage, a few reminders about the NSA's multiple metadata dragnets and the alert system.

The NSA has an interlocking system of metadata query interfaces which we now know mix EO 12333 collected data with data collected under the US based phone and Internet dragnet programs. Data collected overseas is dumped in with data collected directly from Verizon.

The interlocking system apparently does a lot of nifty things, one of which is to alert NSA if any of a watch-list of numbers have had certain kinds of phone activity in the previous day (the NSA has not explained what it does when it receives such alerts, which is part of the issue here). There were over 17,000 people on that list when the NSA first started cleaning up its phone dragnet problem.

The problem with having all that data mixed up in one system is that the standards for access are different based on where the data came from. For EO 12333 collected data (the data collected overseas) there's a foreign intelligence assumption that requires only a valid foreign intelligence purpose; this data can be accessed fairly broadly.

Whereas both the phone (BR) and Internet (PR/TT) dragnets — in which the data was collected by

legal process in the United States — require "Homeland [ack!] Mission Coordinators" within the NSA to sign off on a claim that there is Reasonable Articulable Suspicion that the identifier belongs to someone with a tie to certain approved terror (and Iran) groups — it's basically a digital stop-and-frisk standard signed off by a manager.

That difference between EO 12333 and domestic dragnets created the first problem with the alert list: 90% of the people on the alert list had not had that bureaucratic sign-off, and so should not have been used with the BR phone dragnet data at all. That's the part of the alert problem we hear most about.

But in addition to the "RAS approval" step for the BR phone dragnet, there's an additional bureaucratic step for US persons.

The statute only permits Section 215 to be used against Americans,

> provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

The FISC orders (here's the one in place when NSA first started admitting the problem) accomplished that by reiterating that restriction (7-8) and mandating that,

> NSA's OGC shall review and must approve proposed queries of archived metadata based on "seed" telephone identifiers reasonably believed to be used by U.S. persons before any query is conducted. (8-9)

Note the "archived metadata" language. The NSA maintained that since the alert process happened as the data came into the database, that didn't count as a query of archived metadata. Judge Walton was not impressed.

The NSA had to get its lawyers to sign off on an assertion that the US person identifiers they were using to query the database had not been selected based solely on their religion, their speech, or political activity.

In other words, before NSA could use that US person's identifier either to query the dragnet (which produces a three-degrees of Osama bin Laden report) or to generate alerts, they should have had it RAS-approved by a Homeland [sic] Mission Coordinator **and** undergo a First Amendment review at OGC.

When I was first learning how to write effective bureaucratic documents 20 years ago, I learned that "shall" is the only magic word that can make people do what they're supposed to do; it's the only thing that conveys legal obligation. Apparently it didn't work out that way in this case, because 3,000 US persons — **58% more people than were on the Project Minaret watchlist**, which extended over 3 more years — were on (at a minimum) the alert list without that First Amendment review.

3,000 US persons (that is, either permanent residents or American citizens) were having their communications tracked because of a stop-and-frisk standard suspected tie to terrorism, without NSA affirming that they weren't being tracked because they were politically active Muslims or similar protected behavior.

Retrospectively, it's now clear that this exposure of Americans without First Amendment review was chief among Reggie Walton's concerns when he first responded to the dragnet. It's equally clear that Walton was just learning about the EO 12333 data on the alert list, including that US persons might be included on it.

> The preliminary notice from DOJ states that the alert list includes telephone identifiers that have been tasked for collection in accordance with NSA's SIGINT authority. What standard is

> applied for tasking telephone identifiers under NSA's SIGINT authority? Does NSA, pursuant to its SIGINT authority, task telephone identifiers associated with United States persons? If so, does NSA limit such identifiers to those that were not selected solely upon the basis of First Amendment protected activities?

~~DOJ and Keith Alexander were in no rush to answer Walton's question – the only unredacted response to his question about what happened with US persons~~ The NSA explained,

> Additionally, NSA determined that in all instances where a U.S. identifier served as the initial seed identifier for a report (22 of the 275 reports), the initial U.S. seed identifier was either already the subject of FISC-approved surveillance under the FISA or had been reviewed by NSA's OGC to ensure that the RAS determination was not based solely on a U.S. person's first amendment-protected activities.

That response was dated February 12, 2009, so Walton's response may have been to point out that alerts were effectively queries and a bunch of Americans were being tracked illegally. Note, too, that they're only telling Walton about queries that resulted in report to the FBI or some other agency; they're not denying that these identifiers were used for queries, which would have resulted in the numbers of their contacts being dumped into the corporate store forever.

But there are a few more details from Alexander's declaration, above, that should cause us concern:

- Rather than review these selectors to see if they had been selected based on their

speech, religion, or politics, NSA's OGC simply moved them into a category – non-RAS approved – where such restrictions no longer applied. I would suggest their unwillingness to do such a review is rather striking.

- "Some of the 3,000 domestic identifiers generated alerts as a result of the Telephony Activity Detection Process." They shouldn't have been matched up against the incoming phone dragnet data, but it appears they were, and did produce those kinds of alerts, though NSA rather conspicuously declines to tell us how many people that happened to and how often. We don't know what happened to these 3,000 US person or the people they communicated with after NSA discovered these daily contacts.
- The footnote notes that being on the alert list does not automatically put one in the "counterterrorism target knowledge database," NSA's tracker for suspected terrorists. But the footnote doesn't say that they weren't put in that database, potentially in

> part because of the alerts. Moreover, these "approximately 3,000 domestic telephone identifiers" had already gotten "reported to Intelligence Community agencies." While NSA makes much out of the fact that no query reports got sent on to the FBI and other agencies, that's sort of moot, because the identifiers, if not the names, already had been.

Mind you, to get disseminated to other agencies, these US person identities (if they were treated as such) would need to get sign-off for their intelligence value. Which is why I find OGC's solution — to avoid doing a First Amendment review on them at all — so suspicious. Because high ranking NSA personnel had already done a review, and for some reason were unwilling to do further scrutiny.

3,000 US persons were on a watchlist, potentially because of their religion, politics, or speech. The NSA itself appears to have seen the similarities with Project Minaret, decades earlier.

But we keep hearing there were no abuses.

Updated erroneous link to Keith Alexander declaration.

Update, March 11: The NSA actually did provide more response on EO 12333 collection to Walton, which I hope to return to.

JEREMY SCAHILL: TWO DEGREES OF SEPARATION FROM THE DIRTY WARS DRAGNET

Congratulations to Jeremy Scahill and the entire team that worked on Dirty Wars for being nominated for the Best Documentary Oscar.

This post may appear to be shamelessly opportunistic — exploiting the attention Dirty Wars will get in the days ahead to make a political point before the President endorses the dragnet on Friday — but I've been intending to write it since November, when I wrote this post.

Jeremy Scahill (and the entire Dirty Wars team) is the kind of person whose contacts and sources are exposed to the government in its dragnet.

To write his book (and therefore research the movie, though not all of this shows up in the movie) Scahill spoke with Anwar al-Awlaki's father (one degree of separation from a terrorist target), a number of people with shifting loyalties in Somalia (who may or may not be targeted), and Afghans we identified as hostile in Afghanistan. All of these people might be targets of our dragnet analysis (and remember — there is a far looser dragnet of metadata collected under EO 12333, with fewer protections). Which puts Scahill, probably via multiple channels, easily within 3 degrees of separation of targets that might get him exposed to further network analysis. (Again, if these contacts show up in 12333 collection Scahill would be immediately exposed to that kind of datamining; if it shows up in the Section 215 dragnet, it would happen if his calls got dumped into the Corporate Store.) If Scahill got swept up in the dragnet on a first or second hop, it means all his other sources, including those within government (like the person depicted in

the trailer above) describing problems with the war they've been asked to fight, might be identified too.

Scahill might avoid some of this with diligent operational security — a concerted effort to prevent the government from tracking him along with terrorists (though remember two things: one purpose of the dragnet is to discover burner phones, and his computer got hacked while he was working on this book). But the government's intent is to sweep up records of any conversations that get as close to those hostile to American efforts as Scahill does.

One of my favorite figures in Scahill's book was the Heineken and Johnny Walker swilling Mullah Zabara, a Yemeni tribal leader from Shabwa who expressed the ambivalence Yemenis might feel towards the US.

> Several souther leaders angrily told me stories of US and Yemeni attacks in their areas that killed civilians and livestock and destroyed or damaged scores of homes. If anything, the US air strikes and support for Saleh-family-run counterterrorism units had increased tribal sympathy for al Qaeda. "Why should we fight them? Why?" asked Ali Abdullah Abdulsalam, a southern tribal sheikh from Shabwah who adopted the nom de guerre Mullah Zabara, out of admiration, he told me, for Taliban leader Mullah Mohammed Omar. If my government built schools, hospitals and roads and met basic needs, I would be loyal to my government and protect it. So far, we don't have basic services such as electricity, water pumps. Why should we fight al Qaeda?" He told me that AQAP controlled large swaths of Shabwah, conceding that the group did "provide security and prevent looting. If your car is stolen, they will get it back for you." In areas "controlled by the government, there is looting and

> robbery. You can see the difference." Zabara added, "If we don't pay more attention, al Qaeda could seize and control more areas."
>
> Zabara was quick to clarify that he believed AQAP was a terrorist group bent on attacking the United States, but that was hardly his central concern. "The US sees al Qaeda as terrorism, and we consider the drones terrorism," he said. "The drones are flying day and night, frightening women and children, disturbing sleeping people. This is terrorism."
>
> [snip]
>
> "I don't know this American," he said to my Yemeni colleague. "So if anything happens to me as a result of this meeting—if I get kidnapped—we'll just kill you later."
>
> [snip]
>
> "I am not afraid of al Qaeda. I go to their sites and meet them. We are all known tribesmen, and they have to meet us to solve their disputes." Plus, he added, "I have 30,000 fighters in my own tribe. Al Qaeda can't attack me."

Zabara served as a fascinating source for Scahill. He described seeing Umar Farouk Abdulmutallab while he was staying at Fahd al-Quso's farm.

> Zabara [] later told me he had seen the young Nigerian at the farm of Fahd al Quso, the alleged USS Cole bombing conspirator. "He was watering trees," Zabara told me. "When I saw [Abdulmutallab], I asked Fahd, 'Who is he?'" Quso told Zabara the young man was from a different part of Yemen, which Zabara knew was a lie. "When I saw him on TV, then Fahd told me the truth."

> [2nd bracket original]

This story does not entirely back the narrative the US told about Abdulmutallab and Awlaki at the former's sentencing; it strongly suggests Quso played a role in Abdulmutallab's plotting the government suppressed in public documents and claims, instead attributing that role to Awlaki as part of the case to kill him. While we can't be sure he told the truth, it does seem that Zabara provided necessary nuance to the story our government has told us about executing an American citizen with a drone strike.

Scahill goes onto reveal,

> In January 2013, Zabara was assassinated in Abyan. It is unknown who killed him.

It could, of course, be anyone, quite likely AQAP (who had let Zabara get away with drinking in the past) or the Yemeni government or some other rival.

Jeremy Scahill's reporting — as well as the reporting of scores of journalists who speak to people who might not be terrorists, but might express well-considered ambivalence toward American presence in the countries where we fight — is utterly crucial to our understanding of whether our "war on terror" will achieve its desired end. In the same way that Peter Bergen's reporting (whose conversation with Osama bin Laden would put him one hop away from the lead terrorist) taught us things about our adversary we might not otherwise know, Scahill's reporting helps us understand what our Dirty War looks like on the ground. Just as importantly, this reporting provides details that challenge the government's closely managed narrative about what it is doing in our name.

The Academy apparently thinks Scahill's work has artistic and documentary merit. Our government thinks such work should receive no protection in its dragnet.

DRAGNET AT BERNIE'S: ON SPYING ON CONGRESS

It turns out that Mark Kirk — not Bernie Sanders — was the first member of Congress to raise concerns about the NSA spying on Senators after Edward Snowden's leaks started being published. Kirk did so less than a day after the Guardian published the Verizon order from the phone dragnet, in an Appropriations Committee hearing on the Department of Justice's budget (see at 2:00). After Susan Collins raised the report in the context of drone killing, Kirk asked for assurances that members of Congress weren't included in the dragnet.

> Kirk: I want to just ask, could you assure to us that no phones inside the Capitol were monitored, of members of Congress, that would give a future Executive Branch if they started pulling this kind of thing up, would give them unique leverage over the legislature?
>
> Holder: With all due respect, Senator, I don't think this is an appropriate setting for me to discuss that issue—I'd be more than glad to come back in an appropriate setting to discuss the issues that you've raised but in this open forum—

> Kirk: I'm going to interrupt you and say, the correct answer would say, no, we stayed within our lane and I'm assuring you we did not spy on members of Congress.

The first substantive question Congress asked about the dragnet was whether they were included in it.

After that, a few moments of chaos broke out, as other Senators — including NSA's representative on the Senate Intelligence Committee, Barb Mikulski — joined in Kirk's concerns, while suggesting the need for a full classified Senate briefing with the AG and NSA. Richard Shelby jumped in to say Mikulski should create the appropriate hearing, but repeated that what Senator Kirk asked was a very important question. Mikulski agreed that it's the kind of question she'd like to ask herself. Kirk jumped in to raise further separation of powers concerns, given the possibility that SCOTUS had their data collected.

The **very first concern** members of Congress raised about the dragnet was how it would affect their power.

And then there was a classified briefing and …

… All that noble concern about separation of power melted away. And some of the same people who professed to have real concern became quite comfortable with the dragnet after all.

It's in light of that sequence of events (along with Snowden's claim that Members of Congress are exempt, and details about how data integrity analysts strip certain numbers out of the phone dragnet before anyone contact-chains on it) that led me to believe that NSA gave some assurances to Congress they need not worry that their power was threatened by the phone dragnet.

The best explanation from external appearances was that Congress got told their numbers got protection the average citizen's did not,

perhaps stripped out with all the pizza joints and telemarketers (that shouldn't have alleviated their concerns, as some of that data has been found sitting on wayward servers with no explanation, but members of Congress can be dumb when they want to be).

And they were happy with the dragnet.

Then, 7 months later, Bernie Sanders started asking similar — but not the same —questions. In a letter to Keith Alexander, he raised several issues:

- Phone calls made
- Emails sent
- Websites visited
- Foreign leaders wiretapped

He even defined what he meant by spying.

> "Spying" would include gathering metadata on calls made from official or personal phones, content from websites visited or emails sent, or collecting any other data from a third party not made available to the general public in the regular course of business.

In response, Alexander rejected Sanders' definition of spying (implicitly suggesting it wasn't fair), while using a dodge he repeatedly has: the Americans in question are not being **targeted**, even while they might be collected "incidentally."

> Nothing NSA does can fairly be characterized as "spying on Members of Congress or other American elected officials."
>
> [snip]
>
> NSA may not target any American for foreign intelligence collection without a finding of probable cause that the proposed target of collection is a foreign power or an agent of a foreign

> power. Moreover, as you are aware, whenever an NSA activity results in the incidental collection of information about Americans, that information is handled pursuant to the very robust procedures designed to protect privacy interests — procedures that must be approved by the Attorney general or the Foreign Intelligence Surveillance Court, as appropriate. All those protections apply to members of Congress, as they do to all Americans.

Alexander then addressed just one of the three kinds of spying Sanders raised: phone data (which, if I'm right that NSA strips Congressional numbers at the data integrity stage, is the one place Alexander can be fairly sure Sanders' contacts won't be found).

> Your letter focuses on NSA's acquisition of telephone metadata…

And used the controls imposed on the raw data of the phone dragnet as an excuse for not answering Sanders' question.

> Among those protections is the condition that NSA can query the metadata only based on phone numbers reasonably suspected to be associated with specific foreign terrorist groups. For that reason, NSA cannot lawfully search to determine if any records NSA has received under the program have included metadata of the phone calls of any member of Congress, other American elected officials, or any other American without that predicate.

Alexander totally ignored Sanders' two other specified concerns: emails sent and websites visited.

Which is mighty convenient, because for a very large segment of **that** collection (the internet

metadata collected under EO 12333 and via PRISM, though not the data collected domestically before 2011 or domestic upstream collection), NSA believes it doesn't even need Reasonable Articulable Suspicion to search on US person identifiers. The same is true for any phone dragnet data that has been returned on a query and dumped into the "corporate store," or any phone data collected overseas. NSA could easily search in those databases for Sanders' name and identifiers — it insists it can! — to provide him a specific answer to his question about Internet metadata.

The one Alexander rather pointedly didn't answer.

Of course, former FISC Judge John Bates has told NSA — on two different occasions — that collecting US person data domestically only becomes illegal once NSA knows it is doing it, strongly implying that the NSA would do well to retain plausible deniability about doing so if it doesn't want any trouble from the FISC.

Frankly, I think all members of Congress, especially those like John McCain and Mark Kirk who spend a lot of time talking to leaders we probably do wiretap as much as we can, should be worried about having their conversations surveilled (and I think that explains why Congress in general and McCain in particular got newly concerned about the spying when the extent of foreign leader wiretapping became clear). Because they chat up foreign leaders so frequently, they are likely to be caught up as "incidental" collections.

The could find out, of course! Just ask NSA to do a back door search, of most things but raw US collected metadata, and the NSA has the ability to tell them whether they've been searched.

IS PCLOB HOLDING OUT FOR EO 12,333 INFORMATION?

As you know, I've been tracking the way President Obama seems to want to game the various legislative and review group recommendations with his own.

Which is why I'm interested in this anonymous complaint, from someone in the White House, that PCLOB has not yet released its report.

> Before making his final decisions, the president was supposed to receive a separate report from a semi-independent commission known as the Privacy and Civil Liberties Oversight Board, which was created by Congress. However, **that panel's report has been delayed without explanation until at least late January, meaning it won't reach the president until after he makes his decisions public**.
>
> Members of that oversight board met with the president on Wednesday and have briefed other administration officials on some of their preliminary findings. In a statement, the five-member panel said its meeting with the Mr. Obama focused on the NSA phone collection program and the Foreign Intelligence Surveillance Court, which oversees the data sweeps.
>
> It's unclear why the president will announce his recommendations before receiving the report from the privacy and civil liberties board. **One official familiar with the review process said some White House officials were puzzled by the board's delay**. The report would still be available to Congress, where legislators are grappling with several bills aimed at dismantling or preserving

> the NSA's authority. [my emphasis]

The complaint is interesting not just because it betrays some consternation that the White House won't be able to control the timing on all of this.

Last we heard from PCLOB on November 4, they said publicly that that report would focus on just Section 215 and 702 programs, the two programs the Administration has been trying to provide a limited hangout on since June (though in their Semi-Annual Report from November 3, they also said they were focusing on 12333 guidelines).

But different board members were also focusing on EO 12333 activities. PCLOB Chair David Medine asked about the theft of Google and Yahoo data off their fiber in Europe; Patricia Wald asked whether EO 12333 guidelines legally governed the dissemination of Section 215 data even if the FISC imposed more stringent guidelines; Medine asked whether searches of the corporate store (phone dragnet query results) are governed by EO 12333; and James Dempsey asked what governs the back door searches of data collected under EO 12333.

PCLOB board members clearly get that they can't understand the NSA's activities without understanding what goes on under EO 12333. Yet on one occasion (in response to the Google and Yahoo question), NSA's General Counsel Raj De tried to defer any answer because it was not a Section 215 or 702 question.

> MR. DE: Even by the terms of the article itself there is no connection to the 702 or 215 programs that we are here to discuss. I would suggest though that any implication which seemed to be made in some of the press coverage of this issue that NSA uses Executive Order 12333 to undermine, or circumvent or get around the Foreign Intelligence Surveillance Act is simply inaccurate.

Later, Dempsey asked ODNI's General Counsel Robert Litt when PCLOB was going to get the guidelines NSA used for "other types of collection," meaning that collected under EO 12333.

> MR. DEMPSEY: We have asked about, in fact months ago, several months ago we asked about guidelines for other types of collection, and where do we stand on getting feedback on that? Because you said 18, for example, is the minimization provisions for collection outside the United States, and that's pretty old. Where do we stand on looking at how that data is treated?
>
> MR. LITT: I think we're setting up a briefing for you on that. I believe we're setting up a briefing for you on that. We did lose a few weeks.
>
> MR. DEMPSEY: No, I understand. I was wondering if you could go beyond saying we're setting up a briefing.
>
> MR. LITT: Well, I mean we're in the process of reviewing and updating guidelines for all agencies under 12333. It's an arduous process. You know, it's something that we've been working on for some time and we're continuing to work on it.

They're referring to a letter PCLOB sent back in August about outdated guidelines limiting the dissemination of US person data, a James Clapper response a month later promising and a follow-up 10 days later, on October 3, reminding PCLOB had asked for a briefing and updates on agencies' EO 12333 procedures.

And a month later, PCLOB still had not gotten either the briefing or the written description of where agencies were.

During that entire time, it was becoming more and more clear that the NSA might be moving

programs overseas (and therefore under EO 12333) that had been governed by FISA. If that is happening, it's a matter of significant concern.

Reports on Obama's review say he wants to roll out reforms that might cover any disclosures to come.

> Obama is expected to deliver a national address announcing a set of intelligence-gathering changes. His aim is to set in place guidelines that will convince critics he is serious about reform and that will withstand future disclosures.
>
> [snip]
>
> "The bulk of the work on this is the policy review, not reacting to what the next story is," said another senior administration official, who requested anonymity to discuss the internal deliberations. "We don't know what the next thing will be, and we do have to deal with what comes next. But getting the policy right is what's important so that as new things come, we've addressed the core of it.

I'm of the opinion that the disclosures to come will continue to focus attention on what the NSA does under EO 12333.

So is that what's holding up PCLOB?

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.

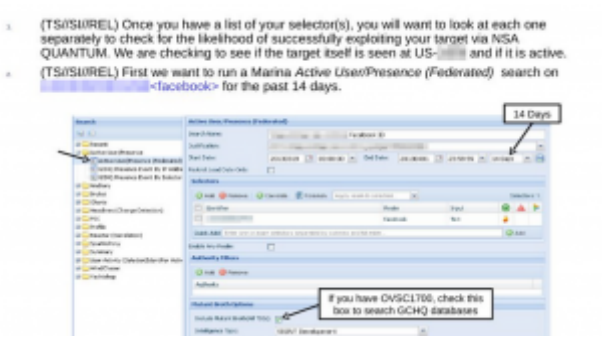
The point is, no one is talking about these uses of the dragnet. No one. And until they do, commentators shouldn’t be lecturing anyone about the adequacy or inadequacy of their dragnet assessment.

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.

HOW NSA HUNTS METADATA "CONTENT" IN SEARCH OF YOUR DIGITAL TRACKS



Der Speigel has posted a set of slides associated with their story on how NSA's TAO hacks targets.

The slides explain how analysts can find

identifiers (IPs, email addresses, or cookies) they can most easily use to run a Quantum attack.

Because NSA is most successful hacking Yahoo, Facebook, and static IPs, it walks analysts through how to use Marina (or "QFDs," which may be Quantum specific databases) to find identifiers for their target on those platforms. If they can't find one of them, it also notes, analysts can call on GCHQ to hack Gmail. Once they find other identifiers, they can see how often the identifier has been "heard," and how recently, to assess whether it is a still-valid identifier.

The slides are fascinating for what they say about NSA's hacking (and GCHQ's apparent ability to bypass Google's encryption, perhaps by accessing their own fiber). But they're equally interesting for what they reveal about how the NSA is using Internet metadata.

The slides direct analysts to enter a known identifier, to find all the other known identifiers for that user, which are:

> determined by linking **content** (logins/email registrations/etc). It is worth verifying that these are indeed selectors associated to your target. [my emphasis]

This confirms something — about Internet metadata, if not yet phone metadata — that has long been hinted. In addition to using metadata to track relationships, they're also using it to identify multiple identities across programs.

This makes plenty of sense, since terrorists and other targets are known to use multiple accounts to hide their identities. Indeed, doing more robust such matching is one of the recommendations William Webster made after his investigation of Nidal Hasan's contacts with Anwar al-Awlaki, in part because Hasan contacted Awlaki via different email addresses.

But it does raise some issues. First, how accurate are such matches? The NSA slides implicitly acknowledge they might not be accurate, but it provides no clues how analysts are supposed to "verify[] that these are indeed selectors associated to your target." In phone metadata documents, there are hints that the FISC imposed additional minimization procedures for matches made with US person identifiers, but it's not clear what kind of protection that provides.

Also, remember NSA was experiencing increased violation numbers in early 2012 in significant part because of database errors, and Marina errors made up 21% of those. If this matching process is not accurate, that may be one source of error.

Also, note that NSA itself calls this "content," not metadata. It may be they've associated such content via other means, not just metadata collection, but given NSA's "overcollection" of metadata under the Internet dragnet, almost certainly collecting routing data that count as content, it does reflect the possibility they themselves admit this goes beyond metadata. Moreover, this raises real challenges to NSA claims that they don't know the "identity" of the people they track in metadata.

Now, none of this indicates US collection (though it does show that NSA continues to collect truly massive amounts of Internet traffic from some location). But the slide above does show NSA monitoring whether this particular user was "seen" at US-[redacted] in the last 14 days. US-[redacted] is presumably a US-associated SIGAD (collection point). (They're looking for a SIGAD from which they can successfully launch Quantum attacks, so seeing if their target's traffic uses that point commonly.) While that SIGAD may be offshore, and therefore outside US legal jurisdiction, it does suggest this monitoring takes place within the American ambit.

At least within the Internet context, Marina

functions not just as a collection of known relationships, but also as a collection of known data intercepts, covering at least a subset of traffic. They likely do similar things with international phone dragnet collection and probably the results of US phone dragnet in the "corporate store" (which stores query results).

In other words, this begins to show how much more the NSA is doing with metadata than they let on in their public claims.

Update: 1/1/14, I'm just now watching Jacob Appelbaum's keynote at CCC in Berlin. He addresses the Marina features at 22:00 and following. He hits on some of the same issues I do here.

JUDGE PAULEY'S DELIBERATE BLIND SPOT: SYSTEMATIC SECTION 215 ABUSES

Sorry for my silence of late, particularly regarding William Pauley's ruling finding the phone dragnet legal. The good news is my mom can now reach the light switch in her sewing room without risk of falling.

As noted, Judge Pauley ruled against the ACLU in their suit challenging the phone dragnet. A number of commentators have pointed to some bizarre errors or focus in Pauley's ruling, including,

- Pauley says the government could not find the "gossamer threads" of terrorist plotters leading up to 9/11. They did find them. They

simply didn't act appropriately with them.

- He unquestioningly considers the 3 uses of Section 215 (with Zazi, Headley, and Ouazzani) proof that it is effective. He does not note that even Keith Alexander has admitted it was only critical in one case, one not even mentioned in the government's filings in this case.
- He ignores the role of the Executive in willingly declassifying many details this program, instead finding it dangerous to allow the ACLU to sue based on an unauthorized leak. The government has actually been very selective about what Snowden-leaked programs they've declassified, almost certainly to protect even more problematic programs from legal challenge.
- He claims Congress has renewed Section 215 7 times (including 2001, it was renewed it 5 times).
- He claims there is no doubt the Intelligence and Judiciary Committees knew about the rulings underlying the program in spite of the fact that some rulings were

> not provided until after Section 215 was renewed; he admits that the limits on circulation of notice in 2011 was "problematic" but asserts the Executive met its statutory requirements (he doesn't deal with the evidence in the record that the Executive Branch lied in briefings about the conduct of the dragnet).

There are also Pauley's claims about the amount of data included — he says the government collects all phone metadata; they say NSA collects far less data. This is a more complicated issue which I'll return to, though maybe not until the New Year.

But I'm most interested in the evidence Pauley points to to support his claim that the FISC (and Congress) conduct adequate oversight over this program. He points to John Bates' limits to the government's intentional collection of US person data via upstream collection rather than Reggie Walton's limits to Section 215 abuses.

> For example, in 20011, FISC Judge Bates engaged in a protracted iterative process with the Government—over the Government's application for reauthorization of another FISA collection program. That led to a complete review of that program's collection and querying methods.

He then immediately turns to Claire Eagan's opinion reiterating that the government had found and dealt with abuses of the phone dragnet program.

In other words, for some bizarre reason he introduces a series of rulings pertaining to

Section 702 — and not to Section 215 — to support his argument that the government can regulate this Section 215 collection adequately.

It's particularly bizarre given that we have far more documents showing the iterative process that took place in 2009 pertaining directly to the phone dragnet. Why even mention the Bates rulings on upstream collection when there are so many Reggie Walton ones pertaining directly to Section 215?

I suspect this is because Pauley relies so heavily on the adequacy of the minimization procedures imposed by the FISC, as when he cites Claire Eagan's problematic opinion to claim that without adequate minimization procedures, FISC would not approve Section 215 phone dragnet orders.

> Without those minimization procedures, FISC would not issue any section 215 orders for bulk telephony metadata collection.

(Note, Pauley doesn't note that the government has not met the terms of the Section 215 itself with regards to minimization procedures, which among other things would require an analysis of the NSA using a statute written for the FBI.)

The only way Pauley can say the limits he points to in his analysis — that NSA can only analyze 3 hops deep, that FBI only gets summaries of the queries, that every query got approved for RAS — is if he ignores that for the first 3 years of the program, all of these claims were false.

He uses similar analysis to dismiss concerns about the power of metadata.

> But [ACLU's contention that the government could use metadata analysis to learn sensitive details about people] is at least three inflections from the Government's bulk telephony metadata collection. First, without additional legal justification—subject to rigorous

> minimization procedures—the NSA cannot even query the telephony metadata database. Second, when it makes a query, it only learns the telephony metadata of the telephone numbers within three "hops" of the "seed." Third, without resort to additional techniques, the Government does not know who *any* of the telephone numbers belong to.

These last assertions are all particularly flawed. Not only have these minimization procedures failed in the past, not only has the government been able to go four hops deep in the past (which could conceivably include all Americans in a query), not only is there abundant evidence — which I'll lay out in a future post — that the government does know the identities of at least some of those whom it is chaining, but there are two ways the government accesses this data for which none of this is true: when "data integrity analysts" fiddle with the data to prepare it for querying, and when it is placed in the "corporate store" and analyzed further.

All the claims about minimization Pauley uses to deem this program legal have big big problems.

The NSA conducted a fraud on the FISC for 3 years (and still is, to the extent they claim the violations under the program arose from complexity rather than their insistence on adopting all the practices used under the illegal program for the FISC-authorized program). Yet Pauley points to the FISC to dismiss any Constitutional concerns with this program.

And to do that, he ignores the abundant evidence that all his claims have been — and may still be, in some cases — false.

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.