FBI IS NOT "SURVEILLING" WIKILEAKS SUPPORTERS IN ITS NEVER-ENDING INVESTIGATION; IS IT "COLLECTING" ON THEM?

The FOIA for records on FBI's surveillance of WikiLeaks supporters substantially ended yesterday (barring an appeal) when Judge Barbara Rothstein ruled against EPIC. While she did order National Security Division to do a more thorough search for records, she basically said the agencies had properly withheld records under Exemption 7(A) for its "multi-subject investigation into the unauthorized disclosure of classified information published on WikiLeaks, which is 'still active and ongoing' and remains in the investigative stage." (Note, the claim that the investigation is still in what FBI calls an investigative stage, which I don't doubt, is nevertheless dated, as the most recent secret declarations in this case appear to have been submitted on April 25, 2014, though Rothstein may not have read them until after she approved such *ex parte* submissions on July 29 of last year.)

In so ruling, Rothstein has dodged a key earlier issue, which is that all three entities EPIC FOIAed (DOJ's Criminal and National Security Division and FBI) invoked a statutory Exemption 3 from FOIA, but refused to explain what statute they were using.

> 2 Defendants also rely on Exemptions 1, 3, 5, 6, 7(C), 7(D), 7(E), and 7(F). The Court, finding that Exemption 7(A) applies, does not discuss whether these alternative exemptions may apply.

I have argued — and still strongly suspect — that the government was relying, in part, on Section 215 of PATRIOT, as laid out in this post.

In addition to the Exemption 3 issue Rothstein dodged, though, there were three other issues that were of interest in this case.

First, we've learned in the 4 years since EPIC filed this FOIA that their request falls in the cracks of the language the government uses about its own surveillance (which it calls intelligence, not surveillance). EPIC asked for:

1. All records regarding any individuals **targeted for surveillance for support for or interest in** WikiLeaks;
2. All records regarding **lists of names of individuals** who have demonstrated support for or interest in WikiLeaks;
3. All records of any **agency communications** with Internet and social media companies including, but not limited to Facebook and Google, regarding **lists of individuals** who have demonstrated, through advocacy or other means, support for or interest in WikiLeaks; and
4. All records of any **agency communications** with financial services companies including, but not limited to Visa, MasterCard, and PayPal, regarding **lists of**

> **individuals** who have demonstrated, through monetary donations or other means, support or interest in WikiLeaks. [my emphasis]

As I've pointed out in the past, if the FBI obtained datasets rather than lists of the people who supported WikiLeaks from Facebook, Google, Visa, MasterCard, and PayPal, FBI would be expected to deny it had lists of such supporters, as it has done. We've since learned about the extent to which it does collect datasets when carrying out intelligence investigations.

Then there's our heightened understanding of the words "target" and "surveillance" which are central to request 1. The US doesn't *target* a lot of Americans, but it does *collect* on them. And when it does so — even if it makes queries that return their identifiers — it doesn't consider that "surveillance." That is, the FBI would only admit to having responsive data to request 1 if it were obtaining FISA or Title III warrants against mere supporters of WikiLeaks, rather than — say — reading their email to Julian Assange, whom FBI surely has targeted *and still targets* under Section 702 and other surveillance authorities, or even, as I guarantee you has happened, looked up people after the fact and discovered they had previous conversations with Assange. We've even learned that NSA collects vast amounts of Internet communications that talk "about" a targeted person's selector, meaning that Americans' communications might be pulled if they used WikiLeaks or Assange's Internet identifiers in the body of their emails or chats. None of that would count as "targeted" "surveillance," but it is presumably among the kinds of things EPIC had in mind when it tried to learn how FBI's investigation of WikiLeakas was implicating completely innocent supporters.

I noted the way FBI's declaration skirted both

these issues some years ago, and everything we've learned since only raises the likelihood that FBI is playing a narrow word game to claim that it doesn't have any responsive records, but out of an act of generosity it nevertheless considered the volumes of FBI records that are related to the request that it nevertheless has declared 7(A) over. Rothstein's order replicates the use of the word "targeting" to discuss FBI's search, suggesting the distinction is as important as I suspect.

> Plaintiff first argues that the release of records concerning individuals who are simply supporting WikiLeaks could not interfere with any pending or reasonably anticipated enforcement proceeding since their activity is legal and protected by the First Amendment. Pl.'s Cross-Mot. at 14. This argument is again premised on Plaintiff's speculation that the Government's investigation is targeting innocent WikiLeaks supporters, and, for the reasons previously discussed, the Court finds it lacks merit.

All of which brings me to the remaining interesting subtext of this ruling.

Five years after the investigation into WikiLeaks must have started in earnest, 20 months after Chelsea Manning was found guilty for leaking the bulk of the documents in question, and over 10 months since Rothstein's most recent update on the "investigation" in question, Rothstein is convinced these records may adequately be withheld because there is an active investigation.

While it's possible DOJ is newly considering charges related to other activities of WikiLeaks — perhaps charges relating to WikiLeaks' assistance to Edward Snowden in escaping from Hong Kong, though like Manning's verdict, that was over 20 months ago — it's also very likely

the better part of whatever ongoing investigation into WikiLeaks is ongoing is an intelligence investigation, not a criminal one. (See this post for my analysis of the language they used last year to describe the investigation.)

Rothstein is explicit that DOJ still has — or had, way back when she read fresh declarations in the case — a criminal investigation, not just an intelligence investigation (which might suggest Assange's asylum in the Ecuador Embassy in London is holding up something criminal).

> In stark contrast to the CREW panel, this Court is persuaded that there is an ongoing criminal investigation. Unlike the vague characterization of the investigation in CREW, Defendants have provided sufficient specificity as to the status of the investigation, and sufficient explanation as to why the investigation is of long-term duration. See e.g., Hardy 4th Decl. ¶¶ 7, 8; Bradley 2d Decl. ¶ 12; 2d Cunningham Decl. ¶ 8.

Yet much of her language (which, with one exception, relies on the earliest declarations submitted in this litigation) sounds like that reflecting intelligence techniques as much as criminal tactics.

> Here, the FBI and CRM have determined that the release of information on the techniques and procedures employed in their WikiLeaks investigation would allow targets of the investigation to evade law enforcement, and have filed detailed affidavits in support thereof. Hardy 1st Decl. ¶ 25; Cunningham 1st Decl. ¶ 11. As Plaintiff notes, certain court documents related to the Twitter litigation have been made public and describe the agencies' investigative techniques against specific individuals. To the extent that Plaintiff seeks those

> already-made public documents, the Court is persuaded that their release will not interfere with a law enforcement proceeding and orders that Defendants turn those documents over.
>
> [snip]
>
> In the instant case, releasing all of the records with investigatory techniques similar to that involved in the Twitter litigation may, for instance, reveal information regarding the scope of this ongoing multi-subject investigation. This is precisely the type of information that Exemption 7(A) protects and why this Court must defer to the agencies' expertise.

I'm left with the impression that FBI has reams of documents responsive to what EPIC was presumably interested in — how innocent people have had their privacy compromised because they support a publisher the US doesn't like — but that they're using a variety of tired dodges to hide those documents.

PATRIOT EXTENSION: CONGRESS CAN'T JUST EXTEND PATRIOT

I've been remiss in laying out what I think the real solution for Section 215 is; I hope to get to that later this week.

Meanwhile, in the House, the question of what to do about the phone dragnet is already heating up. Adam Schiff, newly appointed ranking member in the House Intelligence Committee, is trying to buck up reform advocates in the face of calls for MOAR HAYSTACKS following the HebdoCharlie

attack.

> Schiff told me that those who are hoping for reform of bulk metadata collection need to remain vigilant against the possibility that lawmakers will seize on the Paris horror to blunt the case for change.
>
> "Some will argue that the events in Paris make it impossible to reform any of our intelligence gathering programs," Schiff said. "But as long as we can accomplish these reforms bolstering our privacy, while maintaining our security, we should do so."

Remember, Schiff was the first to call publicly to have the telecoms hold the phone records.

Newly appointed Chair Devin Nunes, however, not only wants to reauthorize PATRIOT but also FISA (which isn't expiring).

> Q: What do you think should be the path forward for reform of the Foreign Intelligence Surveillance Act Courts? Do you support consideration and passage of the FISA Court Reform Act of 2013? If not, do you have your own proposals for FISA reform?
> A: I believe the FISA court system is working well and striking the right balance between protecting Americans' constitutional rights and allowing for effective intelligence operations to catch terrorists. So I don't think it needs reform at this time – we don't want to further encumber intelligence and law enforcement communities who already have a difficult task in tracking those who wish to attack Americans at home and abroad.
>
> [snip]
>
> Our immediate priorities will be analyzing the president's budget,

> crafting the intelligence authorization bill and working with other committees to reauthorize FISA and the Patriot Act.

I hope we can hold him to his observation that FISC is working great, because most "reform" efforts (especially the RuppRoge effort out of the House Intelligence Committee) took authority out of FISC's hands and put it into the IC's.

One thing is missing from this discussion, on all sides.

Congress needs to do more than just extend PATRIOT, if they want full dragnet. They need to extend it, probably by starting with immunity, and probably some other tweaks, to be able to access all the phone records they want. That'll be harder to do if it's not done under cover of "reform."

THE PHONE DRAGNET CLASSIFIED APPENDIX

The government has been releasing a bunch of documents under FOIA while we're all out celebrating: a classification review of the two earlier Section 215 IG Reports, as well as NSA's reports to the Intelligence Oversight Board (though thus far, NSA has mistakenly linked to 1Q 2012 rather than 2Q 2012, which should be one of the most important reports for reasons I'll come back to).

In this post I just want to review the phone dragnet classified appendix included as part of the 2008 DOJ IG Report on the use of Section 215. We've known this appendix — one of two attached to this report (the other, which may be as long as 16 pages, remains classified) — dealt

with the phone dragnet since the phone dragnet was revealed. One thing this report provides are clear dates (which I used to update the dates in my phone dragnet tracker), including exact (in case of the first addition) and rough updates for additional "agents of a foreign power" that may be chained on.

Here are details of interest:

The fourth redaction on the 2nd page of the appendix — in the sentence starting "The queries would attempt to identify…" — is rather interesting syntactically. The redaction should read something like "terrorist associates" or something similar. But in this context, it ties the contact chaining much more closely to the contact-chaining process. Somewhere there must be language purporting to make this case specifically, but the redaction here is remarkably short to do so.

The appendix notes in the first full paragraph on page 3 that the dragnet application promised the NSA Director would inform the Intelligence Committees (but not the Judiciary Committees) about the dragnet. That's curious because we have every reason to believe the NSA did not inform the Intel Committees about the Internet dragnet until after PATRIOT reauthorization, as reflected by this April 27, 2005 briefing to SSCI. Presumably, the December 15, 2005 disclosure of the dragnet led the FISC to discover that Congress hadn't been briefed.

The discussion of the additional terrorist group approved for contact chaining on page 4 seems heavily redacted. I wonder if NSA got Iran approved as early as 2006, with the later approvals being additional al Qaeda affiliates?

At least according to the changes noted in the dragnet orders, the only known addition in the second dragnet order was the pre-approval for FISA targets to be RAS seeds under the dragnet. I'm not sure whether the redaction here would refer to this change, but if it does, it is odd it remains redacted. But it's also

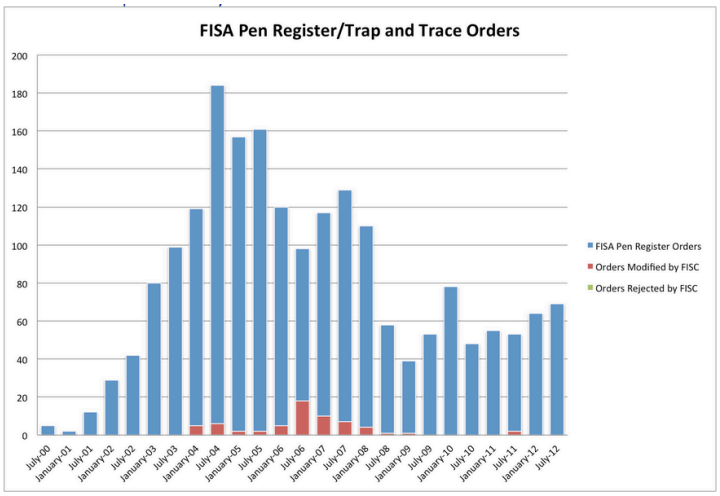
possible the government started collecting some other kind of telephony metadata in that order.

With the exception of the first order, it appears DOJ's IG was working from the applications for the dragnet, not the orders. And the narrative of the dragnet appears to be silent on a number of changes, including the elimination of the compensation paragraph, the addition of spot checks (both in the November 15, 2006 order), and the exception of pre-authorized RAS approval for dockets 06-2081, 07-449, and PAA.

Most interesting still is the report's silence on the change allowing NSA to put the BRFISA data in with other data for the purposes of analytical efficiency. That first shows up in the first dragnet order of 2008 — which the appendix helpfully clarifies was signed on January 10, 2008. It's possible the IG Report doesn't note it (or some of the other changes) because it was only supposed to treat Section 215 for 2006. Perhaps the other changes were done via amendment not shared with the IG (perhaps because of that scope issue). In any case, I find the timing of the order (which admittedly was dictated by the expiration date of the prior order). That would put the change — which I've speculated might relate to the roll-out of ICREACH — just days after Michael Mukasey signed the SPCMA order which allowed chaining on EO 12333 data on US persons. I increasingly believe all these things — ICREACH, SPCMA, and the insertion of FBI into the heart of the FISA process — were necessarily rolled out together.

One other silence of note: This appendix, at least, makes no mention of the 4- and 15-page October 31, 2006 opinions withheld from the EFF and ACLU FOIAs. That's not surprising: if it had been central to the phone dragnet, the government probably would have had to release it. I wonder, though, if they pertain to the dragnet program discussed in the second, still unreleased appendix (and I wonder if that is the CIA money transfer program).

THE CONGRESSIONAL PRTT REPORTS



In addition to liberating the document dump pertaining to the Internet dragnet program. (See my working
threads: one, two, three, four, five.), EPIC has been fighting several other parts of the FOIA for the PRTT documentation to Congress. I'm going to have three more posts on these materials. This post will comment on the reports to Congress, all of which (except the December 2006 one, which I'll ask them to fix) are available here.

Here's a summary of the changes from report to report.

- April 2001 (covering July 2000 to December 2000): US persons described in sketches provided at request of SSCI, some applications filed in 1999, numbers not broken out by USP, CIA not

included, PRTT explicitly only FBI

- December 2001 (covering first half 2001): signed by Jay Bybee as Acting, US persons described in sketches provided at request of SSCI, PRTT explicitly only FBI
- April 2002 (covering second half 2001): signed by Larry Thompson as Acting, 7 applications filed after PATRIOT, includes descriptions of the investigations as well as of USPs, CIA not included, PRTT explicitly only FBI
- December 2002 (covering first half 2002): signed by Ted Olson as Acting, CIA not included, PRTT explicitly only FBI
- September 2003 (covering second half of 2002): stop providing sketch of each American targeted; signed by John Ashcroft, CIA not included, PRTT explicitly only FBI
- December 2003 (covering first half of 2003): signed by John Ashcroft. mostly-redacted delayed PRTT approval for one target, CIA not included, PRTT explicitly only FBI

- September 2004 (covering second half 2003): transmittal letters not included, not mentioned, CIA not included, PRTT explicitly only FBI
- December 2004 (covering first half 2004): transmittal letters signed by AAG, first modifications, CIA not included, PRTT explicitly FBI and NSA
- June 2005 (covering second half 2004): transmittal letters not included, not mentioned, modifications, the following report says that this report described combined orders, but that part is redacted (there is one footnote with a 7E exemption), CIA not included, PRTT not explicitly FBI and NSA
- December 2005 (covering first half 2005): transmittal by AAG, definition of aggregate to include corporation etc, "at least" aggregate number, combined orders, modifications, CIA not included, PRTT not explicitly FBI and NSA
- July 2006 (covering second half 2005) transmittal by AAG, definition of

aggregate, delay from flood, “at least” aggregate number, more explicit description of combined with anticipation of end per PATRIOT, language on “scope of FISC jurisdiction,” modifications, CIA not included, PRTT not explicitly FBI and NSA

- December 2006 (covering first half 2006): transmittal by Acting AAG, definition of aggregate, “at least” aggregate number, more explicit break out of combined, modifications, CIA not included, PRTT not explicitly FBI and NSA
- June 2007 (covering second half 2006): transmittal letters not included, language on modifications and explanation for rise in number, reorganization of OIPR, footnote on some people listed (probably under trad FISA) may be targets of PRTT, no USP numbers broken out, include all 3 agencies with NSA and FBI PRTT numbers combined, modifications
- December 2007 (covering first half 2007):

transmittal letters not included, “at least” number, modifications, include all 3 agencies, with FBI and NSA combined for PRTT

- June 2008 (covering second half 2007): transmittal letters not included, “at least” number, modifications, include all three agencies, with FBI and NSA combined for PRTT
- December 2008 (covering first half 2008): transmittal letters not included, “at least” number, last modifications, include all 3 agencies, with FBI and NSA combined for PRTT
- June 2009 (covering second half 2008): transmittal letters not included, no more “at least” number, no modifications, include all 3 agencies, with FBI and NSA combined for PRTT
- December 2009 (covering first half 2009): transmittal letters not included, supplemental order, include all 3 agencies, with FBI and NSA combined for PRTT
- June 2010 (covering second half 2009): transmittal letters not included, adjust

targeted number for previous period (perhaps without explanation), include all 3 agencies with FBI and NSA combined for PRTT

- December 2010 (covering first half 2010): transmittal letters not included, note one not considered util following period, break out FBI application, no NSA application to FISC
- June 2011 (covering second half 2010): transmittal letters not included, introduction of "named US persons" category, one NSA denied in part (probably July Bates opinion), one approved, mention of compliances meetings with telecoms
- December 2011 (covering first half 2011): transmittal letters not included, redaction of number and "named" in US persons targeted in narrative section, 4 approved outside reporting period, 3 NSA PRTT approved
- June 2012 (covering second half 2011): transmittal letters not included, redaction of number and "named" in US

persons targeted in narrative section, and numerical breakout, 4 earlier FBI applications approved, 1 NSA PRTT approved (somewhere something in 2011 must have been withdrawn, given the approved numbers)
- December 2012 (covering first half 2012): transmittal letters not included, number and "named" unredacted (including for previous period), no NSA application submitted
- June 2013 (covering second half 2012 and submitted after first Snowden leaks): transmittal letters not included, number and "named" unredacted, no NSA application submitted

Here's an explanation of what I make of these details:

How you count US persons

Throughout this reporting requirement, DOJ has been obligated to include the number of US persons targeted. How it has done so has varied by period. Here's how it breaks out by reporting period (I'm doing it this way so we can match it up to known techniques).

July 2000 through December 2001: US person subjects of investigation described by sketch but not broken out by number

January 2002 through June 2002: US person targets identified by number and sketch

July 2002 through December 2004: US person targets identified by number “who were targeted”; sketches replaced by general language about First Amendment review

January 2005 through June 2006: Orders include a definition of aggregate that includes corporations and other non-individual legal persons, these orders provided an “at least” aggregate number (with a footnote explaining why that is redacted). This method covers most of the reports during the “combined” period. Update: The DOJ IG Report on Section 215 use in 2006 may explain some of this: for 215 orders in this period, FBI did not count the requested records of non-subjects, which would likely apply to combined orders.

July 2006 through December 2006: This report includes no discernible US person breakout.

January 2007 through June 2008: These reports used an “at least” number to count US persons.

July 2008 through June 2010:This period included exact numbers for USP targets, and also no longer includes modifications (which often are minimization procedures).

July 2010 through December 2012: This period uses “named US persons” as a reporting category, and to the extent it’s relevant, breaks out the NSA orders.

Note, some of the differential reporting (such as the “aggregate” language for the period before Congress got briefed on the bulk PRTT) to be get around informing Congress of certain collections. Some—such as the apparently still-current “named USP” suggests there’s a lot of incidental collection the government doesn’t count (which would be likely in the use of stingrays, though the prior use of target could be done there too).

The Agencies

Note the variation in agencies named, with PRTT being listed as FBI only, then being listed as

NSA and FBI, then all government, then both again, and finally, broken out by agency. This likely stems most significantly from efforts to hide that they were using PRTT for the dragnet, then incorporation of NSA into the FBI dragnet numbers.

The NSA numbers first get broken out for the December 2010 report, with a statement there were no NSA applications in the first half of 2010. That accords with the understanding that the Internet dragnet got shut down around October 30, 2009, then Bates approved it again in July 2010 (which would be the partial declination marked).

Who signs the transmittals

I was interested that John Ashcroft didn't a bunch of reports during a period when DOJ provided narratives of the Americans targeted. Also, for the first few periods of Stellar Wind, the signee was not read into Stellar Wind. I've increasingly noticed AGs having someone else sign something as a workaround, and that may have been true here, too (remember that the government was obtaining Internet metadata even before Stellar Wind).

But then, to the extent we still got transmittal letters (they stopped entirely in June 2007), they were signed by the Congressional Liaison.

ED MARKEY MAY NOT BE ADEQUATELY PREPARED TO VOTE ON USA FREEDOM ACT

Update: I realize something about this classification guide. While it was updated in 2012 (so after the Internet dragnet got shut

down) it was dated August 2009, so while it was still running. So that part of this may not be location data. But the FBI almost certainly still does do fun stuff w/PRTT because it's the one part of PRTT that remains classified.

1.8. (S//REL TO USA, FVEY) The fact that FBI obtains FISA counterterrorism court orders on behalf of NSA.	SECRET// REL TO USA, FVEY	1.4(c)*	25 Years*	(TS//SI//NF) For FBI Pen Register Trap Trace (PR/TT), classification is TOP SECRET//SI// NOFORN.

Ed Markey, who is absolutely superb on tracking Title III surveillance, continues that tradition today with a letter to Eric Holder asking about the US Marshall Program DirtBox surveillance program revealed last week by WSJ.

Among his questions are:

> Do other agencies within DOJ operate similar programs, in which airplanes, helicopters or drones with attached cellular surveillance equipment are flown over US airspace?
>
> What types of court order, if any, are sought and obtained to authorize searches conducted under this program?
>
> In what kind of investigations are the "dirtbox" and similar technology used to locate targets? Are there any limitations imposed on the kinds of investigations in which the dirtbox and similar technology can be used?
>
> According to media reports, the dirtbox technology, which is similar to a so-called "stingray" technology, works by mimicking the cellular networks of U.S. wireless carriers. Upon what specific legal authority does the Department rely to mimic these cellular networks?
>
> Do the dirtbox and stingray send signals through the walls of innocent people's homes in order to communicate with and identify the phones within?
>
> What, if any, policies govern the collection, retention, use and sharing

> of this information?
>
> Are individuals—either those suspected of committing crimes or innocent individuals—provided notice that information about their phones was collected? If yes, explain how. If no, why not?

I could be spectacularly wrong on this point, but I very very strongly believe the answer to some of his questions lie in a bill Markey is all set to vote for tomorrow.

We know that the government — including the FBI — uses Title III Pen Registers to obtain authorization to use Stingrays; so one answer Markey will get is "Title III PRTT" and "no notice."

Given that several departments at DOJ use PRTT to get Stingrays on the criminal side, it is highly likely that a significant number of the 130-ish PRTT orders approved a year are for Stingray or related use.

Using that logic gets us to the likelihood that FBI's still unexplained PRTT program — revealed in this 2012 NSA declassification guide — also uses Stingray technology to provide location data. That's true especially given that NSA would have no need to go to FBI to get either phone or email contacts, because it has existing means to obtain that (though if the cell phone coverage of the Section 215 dragnet is as bad as they say, it may require pen registers for that).

2.19. (TS//SI//NF) The fact that NSA receives or requests from FBI Pen Register Trap Trace (PR/TT) FISA warrants in order to get data about terrorist groups.	TOP SECRET//SI// NOFORN	1.4(c)*	25 Years*	(TS//SI//NF) The classification level is TOP SECRET//SI// NOFORN regardless of whether the terrorist group is specified for which NSA is seeking or obtaining FISA PR/TT authority.
2.24. (S//REL TO USA, FVEY) Statistics or statistical trends relating to FBI FISA targets, including numbers of court orders, targets, facilities, or selectors, or combinations or subcategories thereof, without mention of techniques involved.	SECRET// REL TO USA, FVEY	1.4(c)*	25 Years*	(TS//SI//NF) For FBI Pen Register Trap Trace (PR/TT), the classification is TOP SECRET//SI// NOFORN.

3.13. (TS//SI//NF) **Minimized** evaluated FBI PR/TT FISA data that does not disclose specific methods or techniques.	TOP SECRET//SI// NOFORN	1.4(c)*	25 Years*	(U) Methods are governed by the classification guides applicable to the specific methods involved.

The guide distinguishes between individual orders, which are classified SECRET, and "FBI Pen Register Trap Trace," which therefore seems to be more programmatic. The FBI PRTT is treated almost exactly like the then undisclosed phone dragnet was in the same review, as a highly classified program where even minimized information is TS/SCI.

Now, it's possible (ha!) that this is a very limited program, just targeting individual targets in localized spots for a brief period of time.

It's also possible the government scaled this back after the *US v. Jones* decision.

But it's equally possible that this is a bulky dragnet akin to the phone dragnet, one that will be invisible in transparency measures under USA Freedom Act because location trackers are excluded from that reporting.

I do hope Markey insists on getting answers to his questions before he votes for this bill tomorrow.

USA GAG FREEDOM ACT

As you likely know, there have been two developments with NSLs in the last few days. First, Twitter sued DOJ, on First Amendment grounds, to be able to publish how many NSLs and FISA orders it has received. And EFF argued before the 9th Circuit that the entire NSL statute should be declared unconstitutional.

These developments intersect with the USA Freedom Act in an interesting way. In the 9th Circuit, the Court (I believe this is Mary

Murguia based on tweets from lawyers who were there, but am not certain) asked why Congress hasn't just fixed the Constitutional problems identified in Doe v. Mukasey with NSL gag orders.

That set off DOJ Appellate lawyer Douglas Letter hemming and hawing in rather unspecific language (my transcription).

> Mary Murguia: Have any measures been taken to Congress to try to change that reciprocal notice procedure, to make it legal as the 2nd Circuit suggested?
>
> Douglas Letter: Your honor, my understanding is, and I'm a little hesitant to talk about this in this sense, as we know proposals can be made to Congress and who knows what will happen? The government is working on some, a, is working with Congressional staffers etcetera, we would hope that at some point we would have legislation. We do not as this point. I'm not, I'm not going to here make any predictions whether anything passes.

What Letter was talking about — bizarrely without mentioning it — was a provision addressing the unconstitutional NSL gags in USA Freedom Act.

The provision fixes one part of the NSLs by putting the onus on FBI to review every year whether gags must remain in place.

> (3) TERMINATION.—
>
> (A) IN GENERAL.—In the case of any request under subsection (b) for which a recipient has submitted a notification to the Government under section 3511(b)(1)(A) or filed a petition for judicial review under subsection (d)—
>
> (i) an appropriate official of the Federal Bureau of Investigation shall, until termination of the nondisclosure

> requirement, review the facts supporting a nondisclosure requirement annually and upon closure of the investigation; and
>
> (ii) if, upon a review under clause (i), the facts no longer support the nondisclosure requirement, an appropriate official of the Federal Bureau of Investigation shall promptly notify the wire or electronic service provider, or officer, employee, or agent thereof, subject to the nondisclosure requirement, and the court as appropriate, that the nondisclosure requirement is no longer in effect.

This would fix the problem identified by the 2nd Circuit.

Except that, bizarrely, it would require FBI to do what Letter represented to the Court FBI could not do — review the gags every year. Presumably, they assume so few providers will challenge the gag that they'll be able to manage those few yearly reviews that would be required.

Which might be what this language is about.

> (B) CLOSURE OF INVESTIGATION.—Upon closure of the investigation—
>
> (i) the Federal Bureau of Investigation may petition the court before which a notification or petition for judicial review under subsection (d) has been filed for a determination that disclosure may result in the harm described in clause (i), (ii), (iii), or (iv) of paragraph (1)(B), if it notifies the recipient of such petition;
>
> (ii) the court shall review such a petition pursuant to the procedures under section 3511; and
>
> (iii) if the court determines that there is reason to believe that disclosure may result in the harm described in

> clause (i), (ii), (iii), or (iv) of paragraph (1)(B), the Federal Bureau of Investigation shall no longer be required to conduct the annual review of the facts supporting the nondisclosure requirement under subparagraph (A).

That is, in addition to fixing the constitutional problem with NSLs, USAF provides FBI way out of the supposedly onerous problem that fix requires, by establishing a way to get a permanent gag.

The NSL provisions in USAF have not gone totally unnoticed. Perhaps appropriately, one of the few public comments on it came from the EFF. It lumps it in with FBI's exemption from reporting back door searches.

> The FBI is exempt from Section 702 reporting, and the bill appears to provide a path for the FBI to get permanent gag orders in connection with national security letters.

And bill champion Kevin Bankston is acutely aware of the dynamic as well; after Twitter announced his suit he suggested this was a good reason to pass USAF.

Me, I'd rather let the courts work and get the leverage we might get that way.

Especially since it seems like FBI is more able to review yearly gag renewals that Letter told the court.

THE HEMISPHERE DECKS: A COMPARISON AND SOME HYPOTHESES

Last week, Dustin Slaughter published a story using a new deck of slides on the Hemisphere program, the Drug Czar program that permits agencies to access additional telecommunications analytical services to identify phones, which then gets laundered through parallel construction to hide both how those phones were found, as well as the existence of the program itself.

It has some significant differences from the deck released by the New York Times last year. I've tried to capture the key differences here:

	NYT	Declaration
Scope	AT&T network; CDRs for any telephone carrier that uses an AT&T switch Access to AT&T subscriber info Roaming provided, location available	"Telecom propriety" (2) though "only calls that hit the Hemisphere switches" (12) Some subscriber information unavailable (elsewhere references to "official subscriber information") Local, long distance, international, cell Temporary roaming and location provided with CDRs
Timing	1 hour response/CDRs 1 hour old	1-hour exigent; 2-5 day typical response/CDRs few hours old/CDRs 2 hours old
Customers	Fed, state, local administrative and grand jury subpoenas (mentions recent WA approval) DEA and DHS mentioned	Administrative order, CA court order , or grand jury 6 federal agencies, including FBI and US Marshals
Features	Dropped phones, additional phones, international phones, IMEI & ISEI search on AT&T network, mapping, pinging	Dropped, additional phones, international phones, temporary roaming, location
Dropped phone success rate	Candidates for the replacement phone are ranked by probability	94%
Aging	26 year old long distance and international records available in 2013 Program started in 2007	10 year old records, date unknown

The biggest difference is that the NYT deck — which must date to no earlier than June 2013 — draws only from AT&T data, whereas the Declaration deck draws from other providers as well (or rather, from switches used by other

providers).

In addition, the Declaration deck seems to reflect approval for use in fewer states (given the mention of CA court orders and the recent authorization to use Hemisphere in Washington in the AT&T deck), and seems to offer fewer analytical bells and whistles.

Thus, I agree with Slaughter that his deck predates — perhaps by some time — the NYT/AT&T deck released last year. That would mean Hemisphere has lost coverage, even while it has gained new bells and whistles offered by AT&T.

While I'm not yet sure this is my theory of the origin of Hemisphere, some dates are worth noting:

From 2002 to 2006, the FBI had telecoms onsite to provide CDRs directly from their systems (the FBI submitted a great number of its requests without any paperwork). One of the services provided — by AT&T — was community of interest tracking. Presumably they were able to track burner phones (described as dropped phones in these decks) as well.

In 2006, FBI shut down the onsite access, but retained contracts with all 3 providers (AT&T, Verizon, and probably Sprint). In 2009, one telecom — probably Verizon — declined to renew its contract for whatever the contract required.

AT&T definitely still has a contract with FBI, and in recent years, it has added more services to what it offers the FBI.

It's possible the FBI multi-provider access moved under ONCDP (the Drug Czar) in 2007 as a way to retain its authorities without attracting the attention of DOJ's excellent Inspector General (who is now investigating this in any case). Though I'm not sure that program provided the local call records the deck at least claims it could have offered. I'm not sure that program got to the telecom switches the way the deck seems to reflect. It's possible, however, that the phone dragnet in place before it was moved

to Section 215 in 2006 did have that direct access to switches, and the program retained this data for some years.

The phone dragnet prior to 2006 and NSL compliance (which is what the contracts with AT&T and one other carrier purportedly provide now) are both authorized in significant part (and entirely, before 2006) through voluntary compliance, per David Kris, the NSA IG Report, and the most recent NSL report. That's a big reason why the government tried to keep this secret — to avoid any blowback on the providers.

In any case, if I'm right that the program has lost coverage (though gained AT&T's bells and whistles) in the interim, then it's probably because providers became unwilling, for a variety of reasons (and various legal decisions on location data are surely one of them) to voluntarily provide such information anymore. I suspect that voluntary compliance got even more circumscribed with the release of the first Horizon deck last year.

Which means the government is surely scrambling to find additional authorities to coerce this continued service.

JOHN "BATES STAMP" LIVES UP TO THE NAME

On February 19, 2013, John Bates approved a Section 215 order targeting an alleged American citizen terrorist. He hesitated over the approval because the target's actions consisted of protected First Amendment speech.

> A more difficult question is whether the application shows reasonable grounds to believe that the investigation of [redacted] is not being conducted solely upon the basis of activities protected

> by the first amendment. None of the conduct of speech that the application attributes to [4 lines redacted] appears to fall outside the ambit of the first amendment. Even [redacted] — in particular, his statement that [redacted] — seems to fall well short of the sort of incitement to imminent violence or "true threat" that would take it outside the protection of the first amendment. Indeed, the government's own assessment of [redacted] points to the conclusion that it is protected speech. [redacted] Under the circumstances, the Court is doubtful that the facts regarding [redacted] own words and conduct alone establish reasonable grounds to believe that the investigation is not being conducted solely on the basis of first amendment.

He alleviated his concerns by apparently relying on the activities of others to authorize the order.

> The Court is satisfied, however, that Section 1861 also permits consideration of the related conduct of [redacted] in determining whether the first amendment requirement is satisfied. The text of Section 1861 does not restrict the Court to considering only the activities of the subject of the investigation in determining whether the investigation is "not conducted solely on the basis of activities protected by the first amendment." Rather, the pertinent statutory text focuses on the character (protected by the first amendment or not) of the "activities" that are the "basis" of the investigation.

Later in the opinion, Bates made it clear these are activities of someone besides the US citizen target of this order, because the activities in question were not being done by US persons.

> Such activities, of course, would not be protected by the first amendment even if they were carried out by a United States person.

If I'm right that behind the redactions Bates is saying the activities of associates were enough to get beyond the First Amendment bar for someone only expressing support, then it would seem to require Association analysis. But then, Bates, the big fan of not having any help on his FISC opinions, wouldn't consider that because the government never does.

Ah well. At least we can finally clarify about whether or not the FISC is a rubber stamp for Administration spying. No. It's a Bates stamp — in which judges engage in flaccid legal analysis in secret before approving fairly troubling applications. Which is just as pathetic.

ICREACH AND FBI'S PRTT PROGRAM

I'll have a more substantive post about what we learn about NSA's broader dragnet from the Intercept's ICREACH story.

But for the moment I want to reiterate a point I made the other day. ICREACH is important not just because it makes NSA data available to CIA and FBI. But also because it makes CIA and FBI data available for the metadata analysis the NSA conducts.

The documents describe that to include things like clandestine intelligence and flight information.

But there's one other program that ought to be of particular concern with regards to NSA's programs. As I laid out here, FBI had a Pen

Register/Trap and Trace "program" that shared information with the NSA at least until February 2012, several months after NSA had ended its PRTT Internet dragnet program.

> **The secrecy behind the FBI's PRTT orders on behalf of NSA**

1.8. (S//REL TO USA, FVEY) The fact that FBI obtains FISA counterterrorism court orders on behalf of NSA.	SECRET// REL TO USA, FVEY	1.4(c)*	25 Years*	(TS//SI//NF) For FBI Pen Register Trap Trace (PR/TT), classification is TOP SECRET//SI// NOFORN.

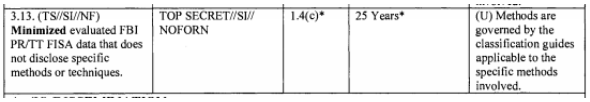
> Finally, there's a series of entries on the **classification guide for FISA programs** leaked by Edward Snowden.
>
> These entries show that FBI obtained counterterrorism information using PRTTs for NSA — which was considered Secret.
>
> But that the FBI PR/TT *program* — which seems different than these individual orders — was considered TS/SI/NOFORN.

2.19. (TS//SI//NF) The fact that NSA receives or requests from FBI Pen Register Trap Trace (PR/TT) FISA warrants in order to get data about terrorist groups.	TOP SECRET//SI// NOFORN	1.4(c)*	25 Years*	(TS//SI//NF) The classification level is TOP SECRET//SI// NOFORN regardless of whether the terrorist group is specified for which NSA is seeking or obtaining FISA PR/TT authority.

> If you compare these entries with the rest of the classification guide, you see that this information — the fact that NSA gets PRTT information from FBI (in addition to information from Pen Registers, which seems to be treated differently at the Secret level) — is treated with the same degree of secrecy as the actual targeting information or raw collected data on all other programs.
>
> This is considered one of the most sensitive secrets in the whole FISA package.

2.24. (S//REL TO USA, FVEY) Statistics or statistical trends relating to FBI FISA targets, including numbers of court orders, targets, facilities, or selectors, or combinations or subcategories thereof, without mention of techniques involved.	SECRET// REL TO USA, FVEY	1.4(c)*	25 Years*	(TS//SI//NF) For FBI Pen Register Trap Trace (PR/TT), the classification is TOP SECRET//SI// NOFORN.

> Even minimized PRTT data is considered

> TS/SCI.
>
> 
>
> | | | | | |
> |---|---|---|---|---|
> | 3.13. (TS//SI//NF) **Minimized** evaluated FBI PR/TT FISA data that does not disclose specific methods or techniques. | TOP SECRET//SI// NOFORN | 1.4(c)* | 25 Years* | (U) Methods are governed by the classification guides applicable to the specific methods involved. |
>
> Now, it is true that this establishes an exact parallel with the BR FISA program (which the classification guide makes clear NSA obtained directly). So it may be attributable to the fact that the existence of the programs themselves was considered a highly sensitive secret.
>
> So maybe that's it. Maybe this just reflects paranoia about the way NSA was secretly relying on the PATRIOT Act to conduct massive dragnet programs.
>
> Except there's the date.
>
> This classification guide was updated on February 7, 2012 — over a month *after* NSA shut down the PRTT program. Also, over a month after — according to Theresa Shea — the NSA **destroyed** all the data it had obtained under PRTT. (Note, her language seems to make clear that this was the NSA's program, not the FBI's.)
>
> That is, over a month after the NSA ended its PRTT program and destroyed the data from it (at least according to sworn declarations before a court), the NSA's classification guide referred to an FBI PRTT program that it considered one of its most sensitive secrets. And seemed to consider active.

I have no idea what this program entailed — and no one else has even picked up on this detail. It's possible NSA's Internet dragnet just moved under the FBI's control. It's possible (this is my current operative wildarseguess) that FBI's PRTT program collects location data; the Bureau uses PRTT orders to get individualized location data, after all.

Whatever it is, though, the existence of ICREACH would make that data available to NSA in a form it could use to include it in contact chaining of metadata (which may be why it figures so prominently in NSA's classification guide). And note: FBI's minimization procedures are far more lenient than NSA's, so whatever this data is, NSA may be able to do more with it given that FBI collected it.

And as with a number of other things, even the Pat Leahy version of USA Freedom would weaken protections for PRTT data.

WORKING THREAD, INTERNET DRAGNET 5: THE AUDACIOUS 2010 REAPPLICATION

At some point (perhaps at the end of 2009, but sometime before this application), the government tried to reapply, but withdrew their application. The three letters below were sent in response to that. But they were submitted with the reapplication.

*See also **Working Thread 1**, **Working Thread 2**, **Working Thread 3**, Working Thread 4, and **Internet Dragnet Timeline**. No one else is doing this tedious work; if you find it useful, **please support it**.*

U. **First Letter in Response to FISC Questions Concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**,

(15/27) In addition to tagging data itself, the source now gets noted in reports.

(16/27) NSA wanted all analysts to be able to query.

(16/27) COntrary to what redaction seemed to indicate elsewhere, only contact chaining will be permitted.

(17/27) This implies that even technical access creates a record, though not about what they access, just when and who did it.

(17/27) NSA asked for the same RAS timelines as in BRFISA — I think this ends up keeping RAS longer than an initial PRTT order.

(18/27) "Virtually every PR/TT record contains some metadata that was authorized for collection, and some metadata that was not authorized for collection … virtually every PR/TT record contains some data that was not authorized by prior orders and some that was not."

(21/27) No additional training for internal sharing of emails.

(21/27) Proof they argue everything that comes out of a query is relevant to terrorism:

> Results of queries of PR/TT-sourced metadata are inherently germane to the analysis of counterterrorism-related foreign intelligence targets. This is because of NSA's adherence to the RAS standard as a standard prerequisite for querying PR/TT metadata.

(22/27) Note "relevance" creep used to justify sharing everywhere. I really suspect this was built to authorize the SPCMA dragnet as well.

(23/27) Curious language about the 2nd stage marking: I think it's meant to suggest that there will be no additional protection once it circulates within the NSA.

(24/27) NSA has claimed they changed to the 5 year age-off in December 2009. Given the question about it I wonder if that's when these letters were sent?

(24/27) Their logic for switching to USSID-18:

> these procedures form the very backbone for virtually all of NSA's dissemination practices. For this reason, NSA believes a weekly dissemination report is no longer necessary.

(24-5/27) The explanation for getting rid of compliance meetings is not really compelling. Also note that they don't mention ODNI's involvement here.

(25/27) "effective compliance and oversight are not performed simply through meetings or spot checks."

(27/27) "See the attached word and pdf documents provided by OIG on an intended audit of PR/TT prior to the last Order expiring as an example." Guess this means the audit documents are from that shutdown period.

V. **Second Letter in Response to FISC Questions concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**,

W. **Third Letter in Response to FISC Questions Concerning NSA Bulk Metadata Collection Using Pen Register/Trap and Trace Devices**.

(2) DNI adopted new serial numbers for reports, so as to be able to recall requests.

(3) THey're tracking the query reports to see if they can withdraw everything.

(3) THis is another of the places they make it clear they can disseminate law enforcement information without the USSID requirements.

(4) It appears the initial application was longer than the July 2010, given the reference to pages 78-79.

Q: **Government's Application for Use of Pen Register/Trap and Trace Devices for Foreign Intelligence Purposes**. (around July 2010)

There are some very interesting comparisons with the early 2009 application, document AA.

(1) Holder applied directly this time rather than a designee (Holder may not have been confirmed yet for the early 2009 one).

(2) The redacted definition of foreign power in AA was longer.

(3) “collect” w/footnote 3 was redacted in AA.

(3) Takes out reference to “email” metadata.

(3) FN 4 both focuses on “Internet communication” rather than “email [redacted]” as AA did, but it also scopes out content in a nifty way.

(3) FN 5 appears to define “Internet comm.”

(4) They add “databases and/or archives” though “archives” was only withdrawn from AA because Walton has just prohibited its use. Also, this uses “repositories” plural.

(4) Defined “identifiers” here used to be email [redacted].

(4) “As appropriate” language at bottom is new.

(5) THere was a footnote on “subject of any FBI investigation” in AA.

(5) “metadata” in middle of page used to be “data.”

(5) As with Holder, here Alexander replaces a surrogate in AA.

(5) This admits they will share with foreign governments; AA did not.

(6) In 2, “information” was “metadata,” and “collected” was “acquired.” Facilities (or its predecessor) redacted in AA.

(6) Govt didn’t submit memo of law w/AA.

(7) Govt didn’t include USSID 18 in AA.

(7) Note reference to April 2010 FBI number; in AA this was December 2008. Both seem to be about 3 months before the application.

(7) Last redaction is “the NSA” in AA.

(8) There's a shift from talking about pen register devices (in AA) to talking about PR authority.

(9) No mention of "below the bcc line" which was in AA and original application.

(9) Unique markings is new—was added by Walton previous fall.

(9) Defeat list obv neW.

(12) The "auditible record" in AA was listed out.

(12) FN 10: this associated language is particularly important.

(13-14) The "DNI has independent responsibility" language is new, and does not have a parallel in the BR FISAs either before or after.

(14) The order on this compliance stuff has been tweaked a bit. Also, they replaced "shall" with "will" throughout.

(15) description of changes in methods is new

(15) Now they've switched back to talking about "devices" again.

(16) Obv this is all new.

R. **Memorandum of Law and Fact in Support of Application for Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes**,

(2) They repeat—then add a long footnote—to their new definition of "not content."

(3) They've decided what they did before was all legal and therefore should be able to collect it all.

(4) The bid to getting rid of past minimization procedures is missing a comma.

(5) Note reference to single doc recovered (this would be before OBL killing).

(9) The "particularly importance" language may suggest "some" limits, but they're likely very

small.

(11) Now they use “content” in the traditional fashion.

(14) They must not specify even all the locations they’re collecting given the post-redaction sentence.

(15) Just some of the data will be subject to “multi-level validation” before going into the repositories.

(16) A long redaction before we get to the part of querying we’re used to. Makes me think of the call-chaining prep as described earlier.

(21) Important discussion of how they changed this starts here: Note it probably explains the different language they used relating to collection versus acquiring.

(22) Here’s where they do their DRAS =/= content.

(23) Once again the govt is speaking broadly about what Congress intended. I wonder whether this was timed to the 2010 reauthorization of PATRIOT?

(24) Here we go:

> Information that is both located in the appropriate field and is in the appropriate format for addressing is by definition ‘addressing information.’ Nothing in the pen register statutes requires “addressing information” to be used for the functional or technical purposes of addressing at the time of collection.

(25) They’re also getting rambunctious with the definition of “facilities” but that’s all redacted.

(29) Once again they argue the FISC has “limited’ authority with respect to a PRTT application.

> The Government continues to believe that the language of the Certification should be determinative of this issue and incorporates those previously advanced arguments as if set forth more fully herein.

(30) This is one of my favorite comments from these documents.

> Relevance here is not properly measured through scientific metrics or the number of reports issued over the course of a year and it does not require a statistical "tight fit" between the volume of proposed collection and the much smaller proportion of information that will be directly "relevant" to the investigations of the Foriegn Powers to protect against international terrorism. *See* Opinion and Order, docket number PR/TT [redacted], at 49-50. Rather, relevance here properly is measure in packets of metadata that over an extended period of time, can help to fill in information that provides a more complete picture of the communications practices of these Foreign Powers and their agents.

(36) Lots of pretty unconvincing language in here as to whether this stuff really counts as DRAS.

(45) The discussion in footnote 25 has an error in the reference to the House Report, which should go back to the earlier referenced one. Here's the discussion that is redacted.

> Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than '' dialing, routing, addressing, and signaling''

> information, such as the the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.
>
> This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, applies across the board to all communications media, and to actual connections as well as attempted connections (such as busy signals and similar signals in the telephone context and packetsthat merely request a telnet connection in the Internet context).

(46) They distinguish between this and the information in a pager.

(46) Wonder what the subject of the District Court opinions are: location?

(50) In footnote 28, the government dismisses language prohibiting the collection of other stuff as irrelevant to their question of whether they can collect stuff that's not DRAS but allegedly not content.

(55) I think they have redacted some, but not all, of the email "validation" references elsewhere.

(56) The redacted stuff must get closer to admitting this stuff is meaningful content.

(59) The government counterposes "individualized warrant" against collecting all metadata.

(60) I'd be curious whether the Kerr citation treats the same stuff they're saying isn't content.

(62) Really curious redaction in FN 33. Especially since I believe FISC changed minimization procedures for TItle I in 2008.

(63) Compare the statement on balance here with the far more outrageous one in the 2004

application.

(64) This recurrent rebuttal to efficacy questions makes me wonder whether Ron Wyden and Russ Feingold were already pushing that issue—we know that Wyden and Udall spent much of 2011 doing so.

> the measure of efficacy required to make a search "reasonable" is not a numerically demanding success rate for the search.

(65) Hey! THat redaction after "chaining" that disappeared for a while in 2009 is back, suggesting they're planning more than simple chaining.

(70) They call 2-hop connection a "direct contact" with an identifier.

(71) Actually don't know if "compliance report" is same thing as E2E report.

(72) THey pretend PRTT doesn't regulate use normally.

(72) They claim the applications imposed controls, not the orders, maintaining structure that they're the ones imposing minimization.

(72) Court has asserted, the Government has supported that assertion

(73) This is where the government claims the Court has authority to query everything.

(73) It relies on "known and extended absence provision" of FBI minimization (the logging language reminds me of the changes made in 2008, per Moalin).

(74) Govt uses language prohibiting intentional violations in criminal statutes to say that bc this wasn't intentional they should be able to access the data good faith. Which of course pretends it wasn't intentional.

S. **Declaration of General Keith B. Alexander, U.S. Army, Director, NSA, in Support of Pen**

Register/Trap and Trace Application, T. **Exhibit D in Support of Pen Register/Trap and Trace Application**. U. **First Letter in Response to FISC Questions Concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**: V. **Second Letter in Response to FISC Questions concerning NSA bulk Metadata Collection Using Pen Register/Trap and Trace Devices**, W. **Third Letter in Response to FISC Questions Concerning NSA Bulk Metadata Collection Using Pen Register/Trap and Trace Devices**.

F. **FISC Primary Order**. July 2010:

(4) There seems much more emphasis on the assistance of providers; this language parallels what's in USAF.

(10) Bates switched the "will" language back to "shall" here. They also took out the ODNI language.

(12) Here's the language permitted them to access the data; it seems like it would amount to virtually all of it.

G. **FISC Memorandum Opinion Granting in Part and Denying in Part Application to Reinitiate, in Expanded Form, Pen Register/Trap and Trace Authorization**,

(8) It's interesting that they relied on a Leiter statement from a previous docket; the US approach to AQAP changed in the interim.

(11) The footnote likely admits that this application would be drawing on far more communications.

(11) Director of NSA has informed me that at no time did NSA collect any category of information … other than the [redacted] categories of meta data." "This assurance turned out to be untrue.""There is not the physical possibility of our having [collected content]

(17) Was 1000 analysts displayed in the compliance docs?

(19) The delegated approval and not for CT purpose may not be declass in other docs

(20) Overcollection was discovered by OGC

(21) Still interested in Bates' comment abt why it was allowed to continue? Did NSA delay in telling Bates?

(22) "the extraordinary fact that NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."

(23) The government did run emergency queries on at least several subjects and reported those to the court

(29) Footnote 30 modifies the redacted sentence(s). It shows inconsistent judgments on whether the government can record the "contents" of PRTT.

(35) Some of what they're discussing (which is redacted later) is logging into an account and/or processing or transmitting an email or IM communication. That counts as signaling to Bates.

(72) 11-24 fold increase in volume.

(80) This should make this not a PRTT.

> At this pre-collection stage, it is uncertain to which facilities PR/TT devices will be attached or applied during the pendency of the initial order. … For this reason, and because the Court is satisfied that other specifications in the order will adequately demarcate the scope of authorized collection, the Court will issue an order that does not identify persons pursuant to Section 1842(d)(2)(A)(ii). However, once this surveillance is implemented, the government's state of knowledge may well change. Accordingly, the Court expects

> the government in any future application to identify persons (as described in Section 1842(d)(2)(A)(ii)) who are know to the government for any facility that the government knows will be subjected to PR/TT surveillance during the period covered by the requested order.

(86) Apparently there's a think (data mining?) that they only do to the corporate store.

(108) "The government's descriptions of the overcollected information make clear that the information concerns the identity of the parties, the existence of the communications, or both.

July to August 2010: First of clarifying letters on dragnet order. FF: Government's First Letter to Judge Bates to Confirm Understanding of Issues Relating to the FISC's Authorization to Collect Metadata.

August 2010: Second clarifying letter on dragnet order. GG: **Government's Second Letter to Judge Bates to Confirm Understanding of Issues Relating to the FISC's Authorization to Collect Metadata**:

These both just ask for clarification of Bates' opinion on 5 issues. But it shows there was at least a several week delay in implementing the new collection.