WORKING THREAD, INTERNET DRAGNET 4: LATER 2009 DOCUMENTS

The early focus on the dragnet violations was on the phone dragnet. At the end of March, however, DOJ started preparing to look more closely at the PRTT program in late April 2009, which may be why some of the following violations got disclosed to Reggie Walton in conjunction with a May reauthorization application. The CIA, FBI, and NCTC access to the PRTT seems to have been a bigger issue than the BR FISA data.

All that said, when the NSA completed its End-to-End report sometime in fall 2009, they didn't report all that much beyond the violations noted in May (though they did note the NSA did not shut down some automatic process when it said it did), mostly by claiming they didn't realize the original dragnet order meant what it said (in spite of the violation in the first dragnet order).

It was only after that that they noticed FISC NSA had been collecting content from the start of the program (see document O). Once they admitted that, NSA decided not to reapply for a Primary Order, and Reggie Walton issued a supplemental order (document E) ordering them not to collect any more, but also not to access the data they did have. Only after that did DOJ submit the End-to-End report, accompanied by DOJ and Keith Alexander reports that admitted the content violation.

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

K. Supplemental Declaration of Chief, Special FISA Oversight and Processing, Oversight and

Compliance, Signals Intelligence Directorate, the National Security Agency. This is referenced in C.

(1) This document, from the Compliance Chair, references an Application for the Internet dragnet. That language appears at the end of declaration , BB.

(2) The statement then says pages 7-9 describe the automated query processes that provided PRTT data to analysts not cleared for it. The use of ""formerly provided" suggests it is the February (est) application s/he is talking about, because Walton shut those down with his Order. But note there are 4 pages of query descriptions in that section (most redacted). So if it's the case that this is the February application, then it means some queries don't — didn't — get circulated outside PRTT cleared analysts.Because this appears to reference that February application, it would seem to have to be before a May reauthorization.

C. **FISC Supplemental Order.** May 29, 2009.

In response to document K and other notices and in conjunction with a Primary Order approval we don't have, Walton issued this Supplemental Order asking for more information on the violations newly revealed.

- Sharing of both automatic and manual query results with all NSA analysts
- Continuing an automated query for weeks past the time the government said it had been shut down
- Compilation of defeat list

Given that this was signed May 29, the previous order would have been signed in the first few days of March, 2009.

June 12, 2009: NSA **alerts** Congress to Internet dragnet master defeat list.

June 16, 2009: NSA notifies of access by CIA, FBI, and NCTC to **both** the phone and Internet dragnet databases.

L. **Government's Response to the FISC's Supplemental Order Requesting a Corrective Declaration**, Probably June 16, 2009

This is the filing and declaration on sharing broadly with other analysts. Curiously, in no unredacted place do they explain why dissemination for Internet has to be different for phone dragnets.

(2) Thus far, 3 digits worth of reports derived from PRTT metadata. (Though they may be using parenthetical numbers.)

H. **Declaration of NSA Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency**, Probably June 16.

(2) Describes sharing with FBI, CIA, and NCTC, as well as two redacted entities, which might be foreign partners.

(2) For a report written by non-cleared analyst, shared with CIA, FBI, Army INSCOM (Alexander's former gig), DNI, DIA, and AFOSI. (Those groups sound more likely cyber than terror, but the description is completely redacted).

(3) Note they exclude stuff that references PRTT sources but don't contain PRTT info. They admit this in footnote 1.

I. **Government's Response to the FISC's May 29, 2009 Supplemental Order**, June 18, 2009.

(2) Note how they discuss the "metadata system." The rules on keeping the PRTT data separate were stronger than on the phone dragnet side.

(3) They redact the discussion about the false leads noisy metadata causes.

(4) Something like a 9 character number of selectors on defeat list.

(5) They're pointing to language in the orders

(the technical massaging) to justify having done this, while admitting an application was erroneous.

(7) This makes clear why the language on analyst access for metadata management changed in the orders: because there's both an automated (algo-driven, presumably) method of identifying defeat terms, and analysts do so in the normal course of work.

(8) Less than 10% of CT analysts had query rights.

J. **Declaration of NSA Chief, Special FISA Oversight and Processing, Oversight and Compliance, Signals Intelligence Directorate, the National Security Agency**. June 18, 2009.

(3) Elsewhere they had left some language about spam, but they don't do so here.

(6) The oversight appears to have used a word other than identifier to described what gets listed—or at least they redacted it.

(7) Description of "international crime and narcotics" product line, including human trafficking.

(8) One related line is redacted—wonder what it was?

FISC Order on dissemination outside of NSA (phone dragnet version; Internet dragnet **version**; **combined**) June 22, 2009

(4) The sharing authorizer was originally named the "Chief of Customer Response."

(Supplement 3) The technical process is called "Chain summary building" — that is redacted in the declaration.

NN: **NSA IG Memo Announcing its Audit of NSA's Controls to Comply with the FISA Court's Order Regarding Pen Register/Trap and Trace Devices**: In the responses to questions about the application, they reveal this was done in response to an order from Judge Walton. It lays out how and who will conduct the audit. It has

to include documents from two different times, given that the second, less formal document, notes it was shut down.

DD: **NSA's Pen Register Trap and Trace FISA Review Report**, before October 31, 2009

Note this was completed before NSA noticed the content collection.

(3) This is really funny. NSA was submitting a supposed comprehensive review and claimed it collected no content.

(5) NSA does make a copy of the PRTT data (this should have been a violation as well, I think).

(5) E2E seems to suggest intake does a contact chain summary on everything, which would be stunning.

(5) Definition of "contact chain summary" is classified FVEY, not NF.

(6) The auto queries went automatically to non PRTT analysts.

[once this doc is OCRed, look for archive. NSA is using it in the fashion they were told not to.]

(6) References additional audits—still trying to figure out whether the IG review that got shut down was in 2009 or 2011.

(6) It took them until 2009 to give analysts individual access accounts.

(7) Notes processes weren't described correctly and that such descriptions will be fixed with next application — so look to the 2010 application to see what they were really doing.

(7) Footnote 7 makes me wonder if they had to add new file transfer controls.

(7) Earlier they've told us they had to train tech people to prevent them from adding new processes to the PRTT data; here they claim software cannot be implemented w/o required testing and approval.

(7) The auto tools had used a system wide certification.

(8) A data enrichment function?

(9) The third function was redacted. Identifying multiple accounts for the same person?

(9) And right after that reference, the report discusses correlated selectors.

(12) Repeats incredible claim that PRTT system never queried w/selectors that hadn't been RAS approved.

(12) NSA kept scanning internal records for new contacts.

(16) They were sharing w/CIA, FBI, and NCTC because they had been:

> This matter stemmed from a collaboration practice recommended by the Directors of NSA, CIA and FBI that was in place prior to the inception of the first PR/TT Order. An interagency group established by the Directors of the NSA, CIA and FBI had recommended in 202 that NSA create a common target knowledge database to allow joint research and information exchanges [redacted]

(17) It appears there were only 3 characters of reports disseminated on PRTT data

(17) THey had not yet figured out whether the USP reports had been derived fr PRTT data

(19) Both PRTT analysts and techs stored PRTT data in shared directories. NSA says not to worry about this, though, because it would take knowledge or chance to find them.

(20) Huh, what could go wrong?

> The internal NSA communications paths on its classified networks are not encrypted, but are subject to strong physical & security access controls.

(22) Note references to audits.

(24) The date-stamping of incoming data was being referenced in the BRFISA side already by this point.

(25) NSA said this just weeks before they had to admit they had never been in compliance.

> Although no corrective measure is infallible, NSA has taken significant steps to eliminate the possibility of any future compliance issues and to ensure that mechanisms are in place to detect and respond quickly if any were to occur.

(32) There are some interesting details in this chart. For example, the tools on the right provide more detail than the text did. One that's partly redacted is "Identify [redacted]." Also note the system "chains" DNR and DNI, but just "transacts" DNI (Internet). I also think they're trying to hide that the alert system was the same for both DNR and DNI.

[There appear to be some pages not included here]

(36) Note they hide what a contact chain summary shows, besides that two selectors communicated.

(37) A redacted term describes a system that conducts "integrated analysis of multiple types of metadata, facilitating more comprehensive target activity tracking."

(39) The selector description makes it pretty clear this is not just about email.

O. **Preliminary Notice of Potential Compliance Incident**. Probably before October 31, 2009

Kris writes this: admits they discovered they got content. It said they would:

- Stop something – which may or may not be ingesting new data

- Not query the data within NSA's PR/TT database until this matter was resolved

OO: **NSA IG Memo Suspending its Audit of NSA after the NSA's PRTT Metadata Program Expired**:

E. **FISC Supplemental Order**. Probably on October 30, 2009.

On timing, note that the Memo of Law accompanying the 2010 reapplication (document R) says (footnote 10) Walton issued the supplemental order on the day the previous order expired, which likely is be October 30.

(2) Even after NSA submitted the preliminary notice, above, DOJ submitted a proposed application to reauthorize collection, probably to start on October 30, 2009. That reiterated the preliminary notice things they wouldn't do (one of which is entirely redacted). That said only that that NSA would not "ingest" the data.

(3) After FISC staff scheduled a hearing on their reapplication, DOJ notified FISC it would not submit a final application to reauthorize the program. Walton may have gone further than their pledge not to "ingest" data: he said the "devices … will cease collecting any such information when the current authority expires."

(4) In his specific order prohibiting collection, Walton did not tie it to PRTT authorities: (in its documentation, the government generally referred to collections pursuant to PRTT, making their statements inapplicable to the SPCMA collection under 12333, which had already started).

> No information of the type that had been authorized for collection under Docket PR/TT and previous dockets may be collected after 5:00 pm. Eastern Time, [probably October 30, 2009]

That should have applied to EO 12333 data, as well, at least within the US.

(5) One part of Walton's order remains redacted.

EE: **DOJ Report to the FISC NSA's Program to Collect Metadata**, Probably after October 31, 2009

(2) ODNI hiding reference to phone circuits here.

(3) There were 2 expansions beyond al Qaeda for chaining.

(4) Odd. The report lists the BR FISA notice, not the first one in PRTT.

(5-6) It appears NSA submitted the E2E after the dragnet got shut down—this notice appears to be the overcollection one, and the E2E describes the collection expiring.

(6) NSA doesn't deal with dissemination issues because the program got shut down. Which means the problems may have been worse than noted. Note too involvement of NSD in the E2E. This could mean they continued to use the PRTT data under the SPCMA banner.

(8) DOJ didn't address the things addressed in III b1, b9, b10, and b11 in the report.

(8) DOJ says problems stemmed from focus on analysts.

(9) NSA kept some of its metadata too long.

(12) This is the first I've seen mention of doing dragnet searches for detainee proceedings.

(12) Is this reference to the URL access to data for CIA et al?

(15) E2E admits tech people had to be trained to prevent them from creating processes that accessed PRTT data w/o understanding of restrictions on data.

(16) Govt tried to map out the info collected under PRTT.

(16) You can see in footnote 19 they were already planning on coming back to claim this all could have been authorized under FISA.

CC. **Declaration Lieutenant General Keith B. Alexander, U.S. Army, Director, NSA, Concerning NSA's Implementation of Authority to Collect Certain Metadata**.

(3) Alexander appears to date the completion of the E2E to a month ("in [redacted]") not a date.

(7) Alexander talks about raised threat level in September 2002 to justify giving CIA/FBI access. Of course, those threats came from torture.

(10) Alexander contrasts CT dissemination with FI. This should raise concerns about USAF.

(12) Suggestion CIA/FBI accessed info when it was not in a formal DB

(13) Audit of target knowledge database did not include entire period. "Logs were not able to be retrieved." No discussion of why not.

(16) Again, this admits they used PRTT for detainee matters. Also, this use did not undergo normal approval processes.

(19) Apparently 12333 dissemination doesn't require a reason for dissemination.

(31) Alexander references the stand-up of the Director of Compliance. But we knew this was after that.