WORKING THREAD: SECTION 215 DRAGNET DOCUMENT DUMP, PART II

It's fundraising week. Please support the work I do with a donation.

This is part of a working thread on yesterday's Section 215 dragnet. Part I is here. The documents are here.

IG Report

(i) Note that the cover letter was signed by the Acting IG, Brian McAndrew, but the report itself was signed by Joel Brenner.

(3) The IG Report uses a lot of passive voice where it should assign some responsibility for implementing controls.

(4) Note this recommendation is redacted but almost certainly is S 215 or S 332, based on the distribution list.

(4) Note the definition of processing.

(8) Note the finding the info assurance was adequate turned out to be wrong, as people were just wandering into this database.

(9) The audits OIG was supposed to conduct didn't happen, per the description on page 31 of the Alexander declaration. This is sort of a big deal. Was OIG excluded (as they had been under the illegal program)? Or did they just not do their job?

(13) Note the review started immediately after the program started and by its own admission "did not conduct a full range of compliance and/or substantive testing."

(18) Curious whether NSA introduced the word

"archive" in the table.

(19) The language on metadata retention is another tell: they describe not "keeping" the data but "keeping it online" while avoiding mention of archive.

Compliance Incidents, Feb 26, 2009 & Supplemental Alexader

(4) Three different analysts querying databases. Again the timing on this is interesting, from day after election to day after transferring power. Note there's still no discussion of where all those other identifiers went.

(SAlexander 2) Note the reference to telecoms remains unredacted.

(SAlexander 7) The 2/18 problem might explain where the 27,090 from the 11/2 review came from: they were simply using 12333 data to access the BR automatically. The fact that they started developed "EAR" as their firewall in January, before they supposed discovered the problem with 12333 access might support that.

(SAlexander 8) Alexander describes here that,

> Prior to 15 January 2009, audits of BR FISA queries were impleneted as spot checks of analyst queries or would be limited to a single day's worth of queries. After one of these spot checks identified improper queries conducted by two analysts, the Agency decided to conduct a more comprehensive audit of all analysts queries of the BR FISA metadata conducted between 1 November 2008 to 23 January 2009. Alexander Declaration at 22-23.

Here's how that read in the original declaration.

> Although the Agency and DoJ have conducted previous audits of queries

> made against the BR FISA data, in response to the BR Compliance Order as well as in light of recent instances of improper querying that were the subject of separate notices to the Court, the Agency initiated an audit of all queries made of the BR FISA data repository since 1 November 2008 to determine if any of the queries during this timeframe were made on the basis of non-RAS approved identifiers. While this review is still ongoing, to date this review has revealed no instances of improper querying of the BR FISA data repository, aside from improper queries that were the subject of a previous compliance notice to the Court. From the time these two analysts were granted access to the BR FISA data repository on 11 and 12 December 2008 until the time NSA terminated their access in January 2009, these two analysts were responsible for 280 improper queries.
>
> ---

[Lost a bunch here, picking up with August Declaration]

(2) Note that as late as 8/19/13 the govt was just submitting its request for renewal. DiFi and Kit Bond had asked for statements about renewal of PATRIOT much earlier in the year.

> Based on these findings and actions, the Government anticipates that it will request in the Application seeking renewal of docket number BR 09-09 authority that NSA, including certain NSA analysts who obtain appropriate approval, be peiliiitted to resume non-automated querying of the call detail records using selectors approved by NSA.

(3) Note the expansion of groups that could be check expanded in 4 steps.

> The Primary Order in docket number BR 06-05 authorized NSA to query the BR metadata using telephone identifiers associated with . Later authorizations expanded the telephone identifiers that NSA could use for queries to those associated with see docket number BR 06-05 (motion to amend granted in August 2006), and, later, th , see docket number BR 07-10 (motion to amend granted in Rine 2007). The Court's authorization in docket number BR 09-09 approved querying related t . See Priman,, Order, docket number BR 09-09, at 5-7. (TS//S1//NT)

I'm particularly interested when Iran and Shabaab got added. The former because it may have been very early (given Iraq), the latter because this timeline may mean it was a stretch for Moalin.

(6) This discussion makes it clear it's contact chaining and something else.

(7) Note how the last paragraph shifts, talking about telephone identifiers, whereas in the previous paragraph it had talked about numbers.

(8-9) Note how little they've gotten from this: [Compare to page 17 in initial report]

> NSA acts on and otherwise makes use of the results of its BR metadata queries. Id. at 3. Where appropriate, it provides those results to other U.S. Government and foreign government agencies. From May 2006 (when the Court issued the first Orders in this matter) through May 2009, NSA disseminated 277 reports containing,. approximately 2,900 telephone identifiers that NSA had identified through its analysis of the BR metadata
>
> [snip]
>
> The FBI has opened predicated

> international terrorism investigations based, at least in part, on BR metadata tips, including twenty-seven full investigations between May 2006 and the end of 2008. Id. at 7-9. In those cases, BR metadata provided predication for opening the investigation.' Id. at 7. Examples are set forth in the accompanying Declaration of the FBI Director. Id. at 9-19 In other cases, BR metadata provided additional information regarding an existing investigation and advanced that investigation. Id. at 5-6. In any such case, the BR metadata was a valuable source of foreign intelligence for the FBI, assisting it in uncovering the operations of and in thwarting terrorist activities targeting the United States, its citizens, and its interests abroad." Id. at 19. TTSitS+44F4—

Also note the neat 10% ratio here.

(10) Why the delay between December 15 and when DOJ found out about this the next month? And how many illegal identifiers were they up to by then?

(10) Note the report claims the end-to-end review found the added identifiers, but at least for the foreign ones, that's not possible (they were stopped in December).

(11) As I projected, the "data integrity analysts" were playing with data outside the analytical framework.

> NSA discovered during the end-to-end review that Data Integrity Analysts were, as part of their authorized access to the BR metadata, identifying identifiers not associated with specific users and sharing those identifiers with analysts through out the NSA not authorized to access the BR metadata.

(12) Note the reference to historical practice:

> While Historically NSA tools permifted queries of non-RA_S-approved identifiers based on [redacted]

This may be the first acknowledgment that this was a historical (illegal) program that simply continued the earlier practices.

End to End Report filing

(14) Note while they say they'll always keep EAR on, they don't say they'll always keep the PKIs off

(17) Note there seems to be just one agency redacted that had data that needed to be purged

(18) Is it possible his foreign to foreign metadata comes form a telecom? Too long for AT&T, too short for Verizon.

Alexander declaration (unnumbered—uses filing page numbers)

(72) Note the reference to the redacted issues. That may be the overproduction issue.

(73) Why is it such a problem NSA received foreign-to-foreign numbers?

(74) Note this definition of "identifier:"

> la the context of this Declaration, the term "identifier" means a telephone number, as that term is commonly understood and used, as well as other unique identifiers associated with a particular user or telecommunications device for purposes of billing and/or routing communications, such as International Mobile Subscriber Identity (IIVISI) numbers, International Mobile station Equipment Identity (IIVEI) numbers, and calling. card numbers.

(75) Note they reserve the right to go back to testing the incoming BR against their alert list.

(77) Note the description of system logs. Also ntoe the audit of activity from March to June—there seems to be a bit of time missing.(81) Note that the telephony ACtivity Detection Process deos not automatically feed the knowledge base.

(82) Identifier is correlated when two identifers identify the same communicants. (Burner)

(83) Note the long footnote amid discussion of correlated IDs.

(84) They ceased treating correlated as RAS approved w/Reggie's order

(85) They didn't redact "Look Ahead" here.

(86-87) Note the timing: they admit the defeat list dates to 2004. But something changed in August 2008.

(89) NSA admits they hadn't air-gapped the BR data. But it looks like they simply got what they had implemented approved, rather than air-gapping it.

(90) As you read the "Data Integrity Analysts'" moving data, remember that they were still finding their data (possibly from pre-BR period) on servers in 2012.

(91) A bunch of contractors had been querying the BR metadata while designing its replacement. THe funniest part is NSA "discovering" this:

> uring the review NSA discovered that a group of software developers designing a next generation metadata analysis graphical user interface (GUI),

It turns out these developers also have maintenance responsibilities (making it likely they're contractors).

> The developers on [redacted—the new system] also have maintenance responsibilities of the operational system, [redacted], where their access to BR FISA is warranted on a continual basis.

Unlike every other discovery in the report, this doesn't indicate what date the court was informed of the violation

Also note that the summarized returns, at least, had moved in July from Lotus Notes to NSA I-Series. (ALexander dec at 36).

(93) NSA did finally require tech personnel to log access in July 2009.

(95) "An oral competency test"?!? Does it document results?

(97) Note Director of Compliance reports TO Alexander, not around him, like an IG would.

(98) Note the NSA redacted almost the entire discussion of why FBI, CIA, and NCTC personnel (250 in all) had access to BR data.

(103) Note that there was email address info in the BR data that the 47 external people accessed. Why would there be email addresses? VOIP?

(104) The agencies all said there were no finished products as a result of hte BR data access (tho the CIA was having "conversations"). At FBI, it was primarily people working closely with FBI's NSA team.

(105-6) Criminal and detainee discovery goes through the litigation support team and it doesn't access BR data.

(107) By 7/29/09 there had been 208 disseminations w/USP identities.

(108) THey only started laying out what the foreign intelligence finding was in July 2008; yet for most of 2008, they still didn't include what that foreign intelligence purpose was.

8/3/09 Alexander Declaration

(11) Note that as of August 2009, NSA did not consider Moalin a hit (unless his is the case referred to on 13)

(12) Here are the numbers as of this report.

> The foregoing discussion is not hypothetical. As noted on page seven of NSA's end-to-end report on the Agency's implementation of the Business Records Order, between inception of the first Business Records Order in May 2006, and May 2009, NSA issued 277 5
>
> The number of reports included in my Declaration of 13 February 2009 was 275. This was based upon information gathered on 6 February 2009. Further review has taken into account the fact that an additional report was issued after 6 February, but before 13 February. Some of these reports had been cancelled for various reasons and some of the cancelled reports were reissued with corrections. Therefore, the correct number of unique reports as of the 13 February 2009 declaration should have been 274. My Declaration also stated that there were 2,549 selectors tipped in these reports. The actual number of selectors tipped in the 274 reports is 2,888.

Mueller Declaration 8/13/09

(9) By 2008, 27 Full Investigations were tied to BR data. But since 2006 until now, only 12 domestic cases have been made. This suggests that only about 1/4 of these investigations became prosecutable cases.

(10) The first of these seems to be Basaaly MOalin, based on the earlier tip and closed investigation.

End-to-End Report, 6/25/09

(2) Note the systems attached to BR: 8 systems, 248 sub-components

(3) FN 3 says the 27,000 number is of Station Table. Note there were also 63,000 non-RAS approved IDs

(12) Note the description of how they had to share BR data w/all CT analysts bc only 20 analysts have access to the DB, but there are over 1000 CT analysts.

(13) Note FN 15 boasting of the protections for the DB access, which assumes everyone in NSA is safe.

(14) The discussion of letting all analysts access the returns is actually not detailed in the Alexander declaration (Check). Note too they just assume this will continue.

(21) This is what it looks like when the NSA admits it doesn't (didn't) have controls:

> Prior to the EAR, NSA was relying on analytic due diligence to query [redacted] with only RAS-approved selectors.

(23) No track changes function to permit a workaround

(24) They have very thin evidence of any audits, but they're sure DOJ never found a bad RAS designation

(28) REquired reading of the court order during this transition period, but now?