SHORTER NSA: THAT WE DISCOVERED WE HAD NO FUCKING CLUE HOW WE USE OUR SPYING IS PROOF OVERSIGHT WORKS

It's fundraising week. Please donate if you can.

James Clapper's office just released a bunch of documents pertaining to the Section 215 dragnet. It reveals a whole slew of violations which it attributes to this:

> The compliance incidents discussed in these documents stemmed in large part from the complexity of the technology employed in connection with the bulk telephony metadata collection program, interaction of that technology with other NSA systems, and a lack of a shared understanding among various NSA components about how certain aspects of the complex architecture supporting the program functioned. These gaps in understanding led, in turn, to unintentional misrepresentations in the way the collection was described to the FISC. As discussed in the documents, there was no single cause of the incidents and, in fact, a number of successful oversight, management, and technology processes in place operated as designed and uncovered these matters.

More candidly it admits that no one at NSA understood how everything works. It appears they're still not sure, as one Senior Official Who Refused to Back His Words admitted,

> "I guess they have 300 people doing compliance at NSA."

"I guess" is how they make us comfortable about their new compliance program.

Ultimately, this resulted them in running daily Section 215 collection on a bunch of numbers that—by their own admission—they did not have reasonable articulable suspicion had some time to terrorism. When they got caught, that number consisted of roughly 10 out of 11 of the numbers they were searching on.

The rest of this post will be a working thread.

Update: Here is the Wyden/Udall statement. It strongly suggests that the other thing the government lied about — as referenced in John Bates' October 3, 2011 opinion — was the Internet dragnet.

> With the documents declassified and released this afternoon by the Director of National Intelligence, the public now has new information about the size and shape of that iceberg. Additional information about these violations was contained in other recently-released court opinions, though some significant information — particularly about violations pertaining to the bulk email records collection program — remains classified.
>
> In addition to providing further information about how bulk phone records collection came under great FISA Court scrutiny due to serious and on-going compliance violations, these documents show that the court actually limited the NSA's access to its bulk phone records database for much of 2009. The court required the NSA to seek case-by-case approval to access bulk phone records until these compliance violations were addressed. In our judgment, the fact that the FISA Court was able to handle these requests on an individual basis is further evidence that intelligence

> agencies can get all of the information they genuinely need without engaging in the dragnet surveillance of huge numbers of law-abiding Americans.

The original order required NSA to keep the dragnet on "a secure private network that NSA exclusively will operate." Yet on the conference call, the Secret-Officials-Whose-Word-Can't-Be-Trusted admitted that some of the violations involved people wandering into the data without knowing where they were. And an earlier violation made it clear in 2012 they found a chunk of this data that tech people had put on their own server.

The order also requires an interface with security limitations. Again, we know tech personnel access the data outside of this structure.

That order also only approves 7 people to approve queries. That number is now 22.

(9) We need to see a copy of the first couple of reports NSA gave to FISC with its reapplications to see how things got so out of control.

(10) This approval was signed by Malcom Howard. Among other things he was in the White House during the Nixon-Ford transition period.

The original authorization for 215 was a hash. Reggie Walton got involved in 2008 and cleaned it up (though not convincingly) in this supplemental order. He relies, significantly, on the "any tangible thing" language passed in 2006. (2-3)

Reggie relies on Russ Feingold's warning about the scope of 215 to drum up legislative history. He doesn't submit those who argued against Feingold as to scope, probably because the govt didn't give it to him.

Reggie makes thin mention of Pen Register/Trap&Trace and never explains why they don't use that.

Notice that Reggie had to start dealing w/compliance issues almost immediately after he wrote a real legal authorization for this shit (as opposed to what Malcom did). This first compliance document makes it clear that he released another opinion, where the standard for collection is. A dangerous way to write opinions. It also 1) makes it likely the telecoms saw only one of the two documents (and therefore couldn't make real argumetns) and 2) COMPLETELY undermines all the squawking govt has made about not being able to release the underlying 215 opinion (which has zero redactions in it).

Note the redaction in the footnote on page 2. That EITHER is redacted solely to hide "all American" from us—preventing us from suing. OR, it's an attempt to hide they were lying to Reggie back then.

(3) Note the Deputy AAG signed the application for this. There are hints throughout the Moalin case that an AAG signed some of the declarations in his case rather than the AG, though that may have been earlier.

Reggie asks for information and the first thing NSA does (in this February 2009 document) is tell him why he shouldn't cancel the program.

(4) Note that the standards for search had already expanded by 2007. I wonder if that's when they added Iran?

(5) "NSD has no record of any other executive branch personnel who knew that the alert list included non-RAS-approved identifiers." But that doesn't mean NSD doesn't know of any. Nice way to use a changeover in Admin.

(7) Note how they didn't mention the alert list

when they first approved this. Remember, this is when FBI was transitioning off having AT&T onsite doing this site. In completely related news, Valerie Caproni JUST TODAY was confirmed a judge. She probably shouldn't be given what these documents reveal.

(7) Note the scrambling effort to clean up the alert list in the days after Obama took over.

(9) NSA is basically saying the FISC should have known about the alert list because it was in the procedures. They have that approach now because there's stuff in the procedures that is not reflected in the law.

(11) NSA OGC didn't think this alert business was important. And yet NSA boasts about what good NSA OGC engages in.

(11) There's a lot in here, such as the reference to "automated chaining" that suggests they did contact chaining with alert list numbers they found to be of interest, as well.

(11) Footnote 12 makes it clear why the NSA's current collect/analyze distinction is so dangerous. Because they don't count things that happen in between as relevant.

(12) Note they were doing automated chaining with USP IDs on some other collection of data. Remember, too, that they would have had old telephone metadata from during the illegal collection.

(12) Look at the big chunk of terror groups considered acceptable searches.

(13) Footnote 13 suggests there were lists before this alert process started in 2006. Remember the FBI was transitioning off their in-house system at this time, so it's a good guess that's where they came from.

(14) Footnote 14 seems to contradict what the Officials-Who-Can't-Be-Trusted said, in that it has a MUCH higher number of alert numbers and that contact chaining was used on them.

(16) Note the GOVERNMENT cites at least three other docket numbers where they got caught abusing this process. They use it to argue for being allowed to continue with a wrist slap.

(17) Like Mindragye, I don't buy the claims made here. I'm led to suspect that they're not "disseminating" reports directly, which allows them to protect leads that would otherwise be illegal. Also, only 275 reports over 2.5 years?

(18) On last point, see "alerts generated from a comparison of the BR metadata to the alert list were only distributed to NSA SIGINT personnel responsible for counterterrorism activity."

(18) This is alarming:

> Since this compliance incident surfaced, NSA identified and eliminated analyst access to all alerts that were generated from the comparison of non-RAS approved identifiers against the incoming BR metadata and has limited access to the BR alert system to only software developers assigned to NSA's Homeland Security Analysis Center (HSAC), and the Technical Director for the HSAC.

It's alarming because tech personnel are now the people who get unaudited access to this stuff. If it was true then, it suggests they could be playing with this data by deeming some people engaged in illegal activities tech personnel and putting it off the books.

(18) Footnote 18 makes it clear that they ignored minimization procedures (by not masking domestic identifiers that had triggered attention on an identifier) to help analysts "prioritize their work more efficiently."

(19) The NSA only chose to audit all queries made after November 1, 2008 (that is, after it was crystal clear Obama would win the election several days later). But we know that at the end of the reporting period ending November 2, 2008, there were a whole bunch of identifiers that

shouldn't be in the list—enough that could implicate the entire US population.

(19) Others have noted this, but 2 analysts conducted 280 queries using illegal query names in the 44 days leading up to and slightly overlapping with Obama's assuming the Presidency. This should have set sirens off. Apparently not.

(20) Myndrage pointed this out too: the middle paragraph on this page makes it clear they were doing more than 3 hops before they 'fessed up to Reggie. That means everyone in the US almost certainly was included.

(22) This is why informants have grown so much: "and potentially to discover individuals willing to become U.S. Government assets."

(26) The section on why operators shouldn't be held in contempt is breathtaking. Why shouldn't Alexander be held in contempt—or better yet fired?

(27) The people informed about this (the filing doesn't actually specify whether they were informed for the first time) were Dennis Blair (now gone), Valerie Caproni (confirmed yesterday as a lifetime appointed judge), and James Clapper (least untruthful by half DNI). Matt Olson (NTCT head) wrote it. The people who downplayed this catastrophe have, for the most part, done very well for themselves.

(Alexander declaration 2) Note Alexander says the declaration was written with advice of counsel.

(Alexander 4) His claim that no non-RAS identifiers were used conflicts with claims elsewhere.

(Alexander 6) The second source of identifiers (bottom redaction) is surely very stunning.

(Alexander 8) Note his reference to "classes" of terrorist targets. We know from Gitmo docs that the govt has a class system to rank how close terrorist targets are to Al Qaeda, which might

explain the reference (there's a redacted footnote that probably does too). But I also wonder if there are ties to how aggressive against the US?

(Alexander 10) Note they call they people who access the data and take out telemarketers and pizza joints and, I suspect, members of Congress, but whose actions are not auditable, "data integrity analysts." Because America.

Alexander 11) Note he doesn't explain why the lawyers didn't think alerts needed legal review. He just implies they didn't do much. Also note how they regard 12333 as carte blanche. And remember that SSCI only now has started getting reports on 12333 collection. I suspect we have far more to learn about what they're doing that compromises Americans.

(Alexander 12) Note his language on "before the order." What he's not saying is they were already conducting this kind of analysis, under Bush's illegal program. So what this actually reflects are procedures in place under the illegal program that were adopted for the "legal" one.

(Alexander 13) They've renamed "Shift Coordinators" "Homeland Mission Coordinators."

(Alexander 14) The data "not regulated by FISA" is data that was illegally collected under Cheney's program.

(Alexander 16) Why is that white redaction permissible?

(Alexander 17) Why not identify which DOJ people identified the problems with the descriptions of DOJ reps?

(Alexander 18 –cf Alexander 2) Note that Alexander didn't ask any of these lawyers why they gave bad descriptions to FISC. That's how he gets away with "it appears" statements everywhere. Because he has deliberately (per his declaration) not asked the people who could confirm one way or another.

(Alexander 19) Again, they magically weren't focused on the pre-archive activities. But somehow Alexander didn't ask. Also note they were concerned with "some" auditing. Not effective auditing?

(Alexander 20) "As appropriate, NSA plans to keep DoJ and the Court informed concerning the progress of this effort." As appropriate?!?! And where is keeping Congress informed?

(Alexander 21) Footnote 12 seems to suggest the end-to-end review included the Internet metadata program. I question why they decided to include it — I suspect they knew it had the same problems. And I look forward to such time as we learn whether that's what discovered the problems that Ron Wyden keeps talking about.

(Alexander 22) Note he was just trying to come up with a tech fix that would prevent analysts from hopping beyond 3 hops. This suggests a problem with their auditing, on top of everything else.

(Alexander 22) Again, Alexander is only auditing the stuff that happened since it was clear Obama would be elected. And those analysts who went wild in the last days of the Bush Administration? They had just been granted access.

(Alexander 23) "Only a limited number of NSA personnel will possess privileges that would allow the new safety feature to be bypassed temporarily." Uh huh.

(Alexander 25) What conceivable reason could they have for that redaction? Not NSA? CIA or FBI? A Snowden type?

(Alexander 28) Why is the government hiding the IDs of the DOJ personnel who attended that first meeting? If they're senior at all (and I'd be surprised if Matt Olsen weren't among them) they should be revealed. The top NSA people should be too.

(Alexander 30) The nice thing about conducting

oversight by in-person meetings is that you can avoid making a record. And then cancel the meetings as you launch into election season.

(Alexander 28, 30) On 28, Alexander is very vague about when NSA's IG was informed. "NSA notified its Inspector General of this compliance matter sometime after DoJ notified the Court on 15 January 2009." Then, two pages later, it admits that someone in NSA IG thought they should put the policies on the alert list in writing, "but this suggestion was not adopted." Alexander then spends a bunch of time claiming that IG was on board with the way they were using the alert list.

(Alexander 31) Note that NSA IG was only checking in when NSA self-reported a compliance problem, not auditing. The NSA IG at this time was Joel Brenner, who often defends these programs. The SIGINT Directorate was conducting those spot checks with support from OGC. Which means if they found something, it was in chain of command.

(Alexander 33) Note how the language on the alert list is "likely to produce information of foreign intelligence value" "associated with" one of the targets on the BR list. This is not necessarily a tie to these groups.

(Alexander 36) They kept the data on Lotus notes servers until 2008?

(Alexander 36) There were 275 reports that tipped 2,549 identifiers since it started.

(Alexander 37) "Almost invariably, the RAS determinations that the Office of General Counsel reviewed were based on direct contact between the telephone identifier and another identifier already known to be associated with one of the terrorist organizations or entities listed in the Business Records Order." This seems to get far closer to something that was apparent in the Moalin case; they consider conversations with targets not protected under the First Amendment, so so long as you're in contact with an alleged terrorist, that's enough

to turn you into an identifer.

(Alexander 39) Note, once again, the tech people have access.

(Alexander 39) Note the reference to ongoing data preservation order. Holy Land Foundation suit by CAIR on unindicted conspirator? Just a guess.

(Alexander 40) Note they'd doing network analysis in addition to contact chaining.