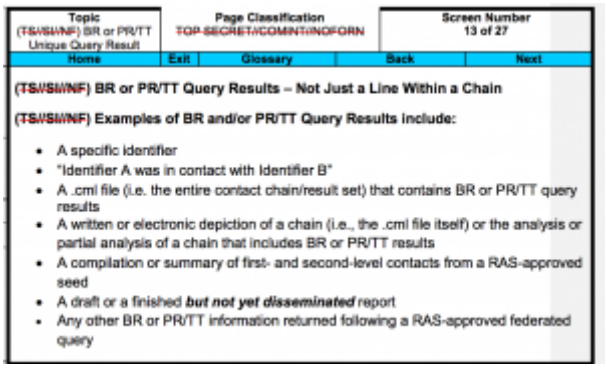
ANOTHER PROBABLE REASON TO SHUT DOWN THE INTERNET DRAGNET: DISSEMINATION RESTRICTIONS



I noted the other day that an NSA IG document liberated by Charlie Savage shows the agency had 4 reasons to shut down the domestic Internet (PRTT) dragnet, only one of which is the publicly admitted reason — that NSA could accomplish what it needed to using SPCMA and FAA collection.

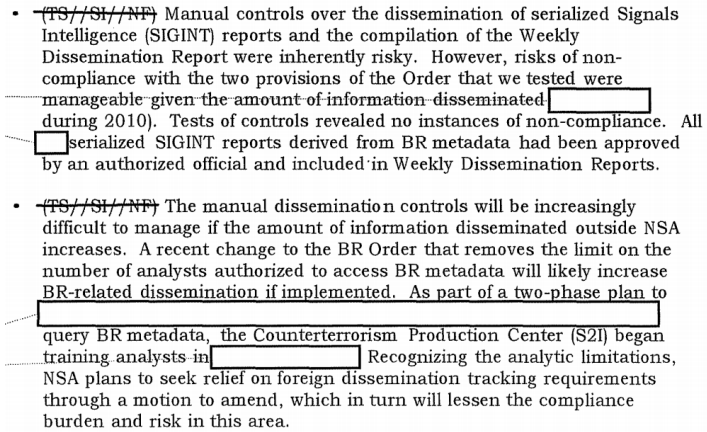
I'm fairly sure another of the reasons NSA shut down the dragnet is because of dissemination restrictions that probably got newly reinvigorated in mid-2011.

I laid out a timeline of events leading up to the shutdown of the Internet dragnet here. I've added one date: that of the draft training program, several modules of which are dated October 17, 2011, released under FOIA (given other dates in the storyboard, the program had clearly been in development as early as November 2010). How odd is that? The NSA was just finalizing a training program on the Internet (and phone) dragnet as late as 6 weeks before NSA hastily shut it down starting in late November 2011. The training program — which clearly had significant Office of General

Counsel involvement — provides a sense of what compliance issues OGC was emphasizing just as NSA decided to shut down the Internet dragnet.

The training program was done in the wake of two things: a series of audits mandated by the FISA Court (see PDF 36) that lasted from May 2010 until early 2011, and the resumption of the PRTT Internet dragnet between July and October 2010.

The series of audits revealed several things. First, as I have long argued was likely, the technical personnel who monitor the data for integrity may also use their access to make inappropriate queries, as happened in an incident during this period (see PDF 95 and following); I plan to return to this issue. In addition, at the beginning of the period — before a new selector tracking tool got introduced in June 2010 — NSA couldn't track whether some US person selectors had gotten First Amendment review. And, throughout the audit period, the IG simply didn't review whether less formalized disseminations of dragnet results followed the rules, because it was too hard to audit. The final report summarizing the series of audits from May 2011 (as well as the counterpart one covering the Internet dragnet) identified this as one of the weaknesses of the program, but NSA wanted to manage it by just asking FISC to eliminate the tracking requirements for foreign selectors (see PDF 209).



- ~~(TS//SI//NF)~~ Manual controls over the dissemination of serialized Signals Intelligence (SIGINT) reports and the compilation of the Weekly Dissemination Report were inherently risky. However, risks of non-compliance with the two provisions of the Order that we tested were manageable given the amount of information disseminated [redacted] during 2010). Tests of controls revealed no instances of non-compliance. All [redacted] serialized SIGINT reports derived from BR metadata had been approved by an authorized official and included in Weekly Dissemination Reports.

- ~~(TS//SI//NF)~~ The manual dissemination controls will be increasingly difficult to manage if the amount of information disseminated outside NSA increases. A recent change to the BR Order that removes the limit on the number of analysts authorized to access BR metadata will likely increase BR-related dissemination if implemented. As part of a two-phase plan to [redacted] query BR metadata, the Counterterrorism Production Center (S2I) began training analysts in [redacted] Recognizing the analytic limitations, NSA plans to seek relief on foreign dissemination tracking requirements through a motion to amend, which in turn will lessen the compliance burden and risk in this area.

I found this blasé attitude about dissemination remarkable given that in June 2009, Reggie

Walton had gotten furious with NSA for not following dissemination restrictions, after which NSA did it again in September 2009, and didn't tell Walton about it, which made him furious all over again. Dissemination restrictions were something Walton had made clear he cared about, and NSA IG's response was simply to say auditing for precisely the kind of thing he was worried about — informal dissemination — was too hard, so they weren't going to do it, not even for the audits FISC (probably Walton himself) ordered NSA to do to make sure they had cleaned up all the violations discovered in 2009.

Meanwhile, when NSA got John Bates to authorize the resumption of the dragnet (he signed the order in July 2010, but it appears it didn't resume in earnest until October 2010), they got him to approve the dissemination of PRTT data broadly within NSA. This was a response to a Keith Alexander claim, made the year before, that all product lines within NSA might have a role in protecting against terrorism (see PDF 89).

> NSA's collective expertise in the[] Foreign Powers resides in more than [redacted] intelligence analysts, who sit, not only in the NSA's Counterterrorism Analytic Enterprise, but also in other NSA organizations or product lines. Analysts from other product lines also address counterterrorism issues specific to their analytic missions and expertise. For example, the International Security Issues product line pursues foreign intelligence information on [redacted] including [redacted] The mission of the Combating Proliferation product line includes identifying connections between proliferators of weapons of mass destruction and terrorists, including those associated with the Foreign Powers. The International Crime and Narcotics product line identifies connections between terrorism and human or nuclear smuggling or other forms of international crime. . . . Each of the NSA's ten product lines has some role in protecting the Homeland from terrorists, including the Foreign Powers. Because so many analysts touch upon terrorism information, it is impossible to estimate how many analysts might be served by access to the PR/TT results.

In other words, even as NSA's IG was deciding it couldn't audit for informal dissemination because it was too hard to do (even while acknowledging that was one of the control weaknesses of the program), NSA asked for and got FISC to expand dissemination, at least for the Internet dragnet, to basically everyone. (The two dragnets appear to have been synched again in October 2010, as they had been for much of 2009, and when that happened the NSA asked for all the expansions approved for the Internet dragnet to be applied to the phone dragnet.)

Which brings us to the training program.

There are elements of the training program that reflect the violations of the previous years, from an emphasis on reviewing for access restrictions to a warning that tech personnel should only use their sysadmin access to raw data for technical purposes, and not analytical ones.

But the overwhelming emphasis in the training was on dissemination — which is a big part of the reason the NSA used the program to train analysts to rerun PATRIOT-authorized queries under EO 12333 so as to bypass dissemination restrictions. As noted in the screen capture above, the training program gave a detailed list of the things that amounted to dissemination, including oral confirmation that two identifiers — even by name (which of course confirms that these phone numbers are identifiable to analysts) — were in contact.

> In addition, any summary of that information would also be a BR or PR/TT query result. So, if you knew that identifier A belonged to Joe and identifier B belonged to Sam, and the fact of that contact was derived from BR or PR/TT metadata, if you communicate orally or in writing that Joe talked to Sam, even if you don't include the actual e-mail account or telephone numbers that were used to communicate, this is still a BR or PR/TT query result.

The program reminded that NSA has to report every dissemination, no matter how informal.

> This refers to information disseminated in a formal report as well as information disseminated informally such as written or oral collaboration with the FBI. We need to count every instance in which we take a piece of information derived from either of these two

> authorities and disseminate it outside of NSA.
>
> Normally an NSA product report is the record of a formal dissemination. In the context of the BR and PR/TT Programs, an official RFI response or Analyst Collaboration Record will also be viewed as dissemination. Because this FISC requirement goes beyond the more standard NSA procedures, additional diligence must be given to this requirement. NSA is required to report disseminations formal or informal to the FISC every 30 days.

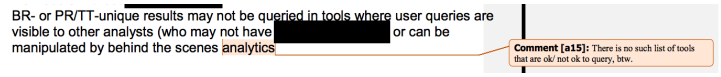
I'm most interested in two other aspects of the training. First, it notes that not all queries obtained via the dragnet will be terrorism related.

> It might seem as though the information would most certainly be counterterrorism-related since, due to the RAS approval process, you wouldn't have this U.S. person information from a query of BR or PR/TT if it weren't related to counterterrorism. In the majority of cases, it will be counterterrorism-related; however, the nature of the counterterrorism target is that it often overlaps with several other areas that include counternarcotics, counterintelligence, money laundering, document forging, people and weapons trafficking, and other topics that are not CT-centric. Thus, due to the fact that these authorities provide NSA access to a high volume of U.S. person information for counterterrorism purposes, the Court Order requires an explicit finding that the information is in fact related to counterterrorism prior to dissemination. Therefore, one of the approved decision makers must document the finding using the proper terminology. It must state

> that the information is related to counterterrorism and that it is necessary to understand the counterterrorism information.

Remember, this training was drafted in the wake of NSA's insistence that all these functional areas needed to be able to receive Internet dragnet data, which, of course, was just inviting the dissemination of information for reasons other than terrorism, especially given FISC's permission to use the dragnet to track Iranian "terrorism." Indeed, I still think think it overwhelmingly likely Shantia Hassanshahi got busted for proliferation charges using the phone dragnet (during a period when FISC was again not monitoring NSA very closely). And one of the things NSA felt the need to emphasize a year or so after NSA started being able to share this "counterterrorism" information outside of its counterterrorism unit was that they couldn't share information about money laundering or drug dealing or … counterproliferation unless there was a counterterrorism aspect to it. Almost as if it had proven to be a problem.

The training program warns that results may not be put into queriable tools that untrained analysts have access to.



\

Note the absolutely hysterical review comment that said there's no list of which tools analysts couldn't use with 215 and PRTT dragnet results. Elsewhere, the training module instructs analysts to ask their manager, which from a process standpoint is a virtual guarantee there will be process violations.

This is interesting for two reasons. First, it suggests NSA was still getting in trouble running tools they hadn't cleared with FISC (the 215 IG Reports also make it clear they were querying the full database using more than just

the contact-chaining they claim to have been limited to). Remember there were things like a correlations tool they had to shut down in 2009.

But it's also interesting given the approval, a year after this point, of an automatic alert system for use with the phone dragnet (which presumably was meant to replace the illegal alert system identified in 2009).

> In 2012, the FISA court approved a new and automated method of performing queries, one that is associated with a new infrastructure implemented by the NSA to process its calling records.68 The essence of this new process is that, instead of waiting for individual analysts to perform manual queries of particular selection terms that have been RAS approved, the NSA's database periodically performs queries on all RAS-approved seed terms, up to three hops away from the approved seeds. The database places the results of these queries together in a repository called the "corporate store."
>
> The ultimate result of the automated query process is a repository, the corporate store, containing the records of all telephone calls that are within three "hops" of every currently approved selection term.69 Authorized analysts looking to conduct intelligence analysis may then use the records in the corporate store, instead of searching the full repository of records.70

That is, in 2011, NSA was moving towards such an automated system, which would constitute a kind of dissemination by itself. But it wasn't there yet *for the PATRIOT authorized collection.* Presumably it was for EO 12333 collection.

As it happened, NSA never did fulfill whatever requirements FISC imposed for using that automatic system with phone dragnet information,

and they gave up trying in February 2014 when Obama decided to outsource the dragnet to the telecoms. But it would seem limits on the permission to use other fancy tools because they would amount to dissemination would likely limit the efficacy of these dragnets.

Clearly, in the weeks before NSA decided to shut down the PRTT dragnet, its lawyers were working hard to keep the agency in compliance with rules on dissemination. Then, they stopped trying and shut it down.

Both the replacement of PRTT with SPCMA and 702, and the replacement of the 215 dragnet with USAF, permit the government to disseminate metadata with far looser restrictions (and almost none, in the case of 702 and USAF metadata). It’s highly likely this was one reason the NSA was willing to shut them down.