THE NSA (SAID IT) ATE ITS ILLEGAL DOMESTIC CONTENT HOMEWORK BEFORE HAVING TO TURN IT IN TO JOHN BATES

The question of whether NSA can keep its Section 215 dragnet data past November 28 has been fully briefed for at least 10 days, but Judge Michael Mosman has not yet decided whether the NSA can keep it — at least not publicly. But given what the NSA IG Report on NSA's destruction of the Internet dragnet says (liberated by Charlie Savage and available starting on PDF 60), we should assume the NSA may be hanging onto that data anyway.

This IG Report documents NSA's very hasty decision to shut down the Internet dragnet and destroy all the data associated with it at the end of 2011, in the wake of John Bates' October 3, 2011 opinion finding, for the second time, that if NSA knew it had collected US person content, it would be guilty of illegal wiretapping. And even with the redactions, it's clear the IG isn't entirely certain NSA really destroyed all those records.

The report adds yet more evidence to support the theory that the NSA shut down the PRTT program because it recognized it amounted to illegal wiretapping. The evidence to support that claim is laid out in the timeline and working notes below.

The report tells how, in early 2011, NSA started assessing whether the Internet dragnet was worth keeping under the form John Bates had approved in July 2010, which was more comprehensive and permissive than what got shut down around October 30, 2009. NSA would have had SPCMA running in big analytical departments by then,

plus FAA, so they would have been obtaining these benefits over the PRTT dragnet already. Then, on a date that remains redacted, the Signals Intelligence Division asked to end the dragnet *and* destroy all the data. That date has to post-date September 10, 2011 (that's roughly when the last dragnet order was approved), because SID was advising to not renew the order, meaning it happened entirely during the last authorization period. Given the redaction length it's likely to be October (it appears too short to be September), but could be anytime before November 10. [Update: As late as October 17, SID was still working on a training program that covered PRTT, in addition to BRFISA, so it presumably post-dates that date.] That means that decision happened at virtually the same time or after, but not long after, John Bates raised the problem of wiretapping violations under FISA Section 1809(a)(2) again on October 3, 2011, just 15 months after having warned NSA about Section 1809(a)(2) violations with the PRTT dragnet.

The report explains why SID wanted to end the dragnet, though three of four explanations are redacted. If we assume bullets would be prioritized, the reason we've been given — that NSA could do what it needed to do with SPCMA and FAA — is only the third most important reason. The IG puts what seems like a non sequitur in the middle of that paragraph. "In addition, notwithstanding restrictions stemming from the FISC's recent concerns regarding upstream collection, FAA §702 has emerged as another critical source for collection of Internet communications of foreign terrorists" (which seems to further support that the decision post-dated that ruling). Indeed, this is not only a non sequitur, it's crazy. Everyone already knew FAA was useful. Which suggests it may not be a non sequitur at all, but instead something that follows off of the redacted discussions.

Given the length of the redacted date (it is one character longer than "9 December 2011"), we can say with some confidence that Keith Alexander

approved the end and destruction of the dragnet between November 10 and 30 — during the same period the government was considering appealing Bates' ruling, close to the day — November 22 — NSA submitted a motion arguing that Section 1809(a)(2)'s wiretapping rules don't apply to it, and the day, a week later, it told John Bates it could not segregate the pre-October 31 dragnet data from post October 31 dragnet data.

Think how busy a time this already was for the legal and tech people, given the scramble to keep upstream 702 approved! And yet, *at precisely the same time*, they decided they should nuke the dragnet, and nuke it immediately, before the existing dragnet order expired, creating another headache for the legal and tech people. My apologies to the people who missed Thanksgiving dinner in 2011 dealing with both these headaches at once.

Not only did NSA nuke the dragnet, but they did it quickly. As I said, it appears Alexander approved nuking it November 10 or later. By December 9, it was gone.

At least, it was gone as far as the IG can tell. As far as the 5 parts of the dragnet (which appear to be the analyst facing side) that the technical repository people handled, that process started on December 2, with the IG reviewing the "before" state, and ended mostly on December 7, with final confirmation happening on December 9, the day NSA would otherwise have had to have new approval of the dragnet. As to the the intake side, *those* folks started destroying the dragnet before the IG could come by and check their before status:

> However, S3 had completed its purge before we had the opportunity to observe. As a result we were able to review the [data acquisition database] purge procedures only for reasonableness; we were not able to do the before and after comparisons that we did for the TD systems and databases

> disclosed to us.

Poof! All gone, before the IG can even come over and take a look at what they actually had.

Importantly, the IG stresses that his team doesn't have a way of proving the dragnet isn't hidden somewhere in NSA's servers.

> It is important to note that we lack the necessary system accesses and technical resources to search NSA's networks to independently verify that only the disclosed repositories stored PR/TT metadata.

That's probably why the IG repeatedly says he is confirming purging of the data from all the "disclosed" databases (@nailbomb3 observed this point last night). Perhaps he's just being lawyerly by including that caveat. Perhaps he remembers how he discovered in 2009 that every single record the NSA had received over the five year life of the dragnet had violated Colleen Kollar-Kotelly's orders, even in spite of 25 spot checks. Perhaps the redacted explanations for eliminating the dragnet explain the urgency, and therefore raise some concerns. Perhaps he just rightly believes that when people don't let you check their work — as NSA did not by refusing him access to NSA's systems generally — there's more likelihood of hanky panky.

But when NSA tells — say — the EFF, which was already several years into a lawsuit against the NSA for illegal collection of US person content from telecom switches, and which already had a 4- year old protection order covering the data relevant to that suit, that this data got purged in 2011?

Even NSA's IG says he thinks it did but he can't be sure.

But what we can be sure of is, after John Bates gave NSA *a second* warning that he would hold them responsible for wiretapping if they kept

illegally collecting US person content, the entire Internet dragnet got nuked within 70 days — gone!!! — all before anyone would have to check in with John Bates again in connection with the December 9 reauthorization and tell him what was going on with the Internet dragnet.

Update: Added clarification language.

Update: The Q2 2011 IOB report (reporting on the period through June 30, 2011) shows a 2-paragraph long, entirely redacted violation (PDF 10), which represents a probably more substantive discussion than the systematic overcollection that shut down the system in 2009.

Timeline

July 2010: John Bates rules categories of PRTT data not approved by Colleen Kollar-Kotelly illegal but authorizes the resumption of the PRTT dragnet (though it does not restart immediately).

Around September 10 (probably September 16), 2011: Last reauthorization of Internet dragnet.

October 3, 2011: John Bates rules upstream collection of US person content illegal.

October 13, 2011: Briefing order to respond to Section 1809(a)(2) concerns.

October 17, 2011: Date on draft training program covering both BRFISA and PRTT programs.

October 31, 2011: Government submits new minimization procedures to address problems with upstream collection.

November 22, 2011: Government claims Section 1809(a)(2) doesn't apply.

November 29, 2011: Government claims it can't separate out Internet transactions collected

under prior minimization procedures, and therefore cannot comply with new minimization procedures, but promises to amend the October 31 MPs to account for this.

November 30, 2011: John Bates approves the October 31 MPs pending changes for the past collection.

Late November: Approval for destruction of data and beginning of destruction.

December 2: Start of observed purge.

December 7: Second step of purge.

December 9: Completion of observed purge and expiration of last Internet dragnet order.

April 2012: NSA makes a "corporate decision" to purge all the upstream collection from prior to October 31, 2011, and "orally informs" the court.

Content notes

[cover] They've redacted the date of the report, which I'd WAG was in spring 2012.

[Ellard letter] XThey've redacted the data again ~~and the full title (or perhaps date) of the report. If its the title they've redacted, it might say something like "NSA repositories."~~ Correction: The redaction after the title is the internal tracking number of the report. It's probably something like (STL-10-0004M).

[Ellard letter] The first of numerous caveats that this report only applies to "declared" databases, along with a "disclosed to us" caveat.

[Ellard letter] This says the data was destroyed before the PRTT order expired on December 9, which would put the authorization for that order around September 10.

[1] The dates in the first redaction are probably October 2009 (which may be general) and October 2010.

[1] The second redaction may describe who was targeted with the dragnet (as that's what similar redactions on the phone side always say).

[1] The third redaction is roughly 15 characters.

[1] The fourth redaction is roughly 10 characters (but doesn't include the year). That probably dates the decision to sometime after September (which has 9 digits before spaces and a date), and probably means it occurred in the single digits of October, which would take up 9 digits plus spaces before or after, though it's possible it happened in late October or early November.

[1] The first reason to kill the dragnet.

[2] In the middle of redacted reasons 2 and 4 to kill the dragnet is the paragraph saying NSA could do what it needed with SPCMA and FAA. For some reason it invokes Bates' October 3, 2011 decision on upstream 702 collection.

[2] It appears the redacted date describing Keith Alexander approving the expiration and destruction of the dragnet is one digit longer than the 9 December date mentioned later in the sentence. This means it has to be either late November — which I'm all but certain it is — or early September.

[2] 2nd use of "declared."

[3] This page lists the 6 locations of PRTT, which has 4 subsections within the corporate database.

[4] This redaction is the same length as the approval date for destroying the data, meaning it is late November.

[4] Admission that they can't ensure the data is gone, especially from the Data Acquisition

Directorate.

[5] This 6 entry table probably correlates with the 6 locations of PRTT on page 3. The S3 is probably intake systems. The other redacted language describes what part of the structured repositories got destroyed.

[5] Another use of “declared.”