2011 INTERNET DRAGNET AUDIT DIDN'T FIND SIGNIFICANT VIOLATION REPORTED TO IOB

This will be the second of three posts on the NSA IG's failures to correct problems with the Internet (PRTT) dragnet. In the first, I showed how quickly NSA nuked the PRTT (or at least claimed to) after John Bates ruled, a second time, that NSA could not illegally wiretap the content of Americans' communications. Here, I'll examine another IG Report, completed earlier in 2011 and also liberated by Charlie Savage, that appears to show the PRTT dragnet was hunky dory just weeks before it became clear again that it was not.

The report (see PDF 4-23) must date to between March 15 and May 25, 2011. It was related to a series of reports on the phone dragnet (these reports appear to have been solicited by or encouraged by Reggie Walton in the wake of the 2009 dragnet problems) that Savage liberated earlier this year. It lists all those reports on pages A-2 to A-3. But it lists the final, summary report in that series, (ST-10-0004L), as a draft, dated March 15, 2011. The copy provided to Savage is the final, dated May 25, 2011 (see PDF 203).

The reason for doing this, the PRTT report, is curious. The report notes "we began this review in [redacted, would be some time in summer 2009] but suspended it when NSA allowed the PR/TT Order to expire." That is, this was the report that got started, but then halted, when someone discovered that every single record the NSA had collected under the program included categories of information violating the rules set by FISC in 2004.

But then NSA started a review of the phone dragnet covering all the activity in 2010 (reflected in monthly reports in Savage's earlier release). So the NSA decided to do a review of PRTT at the same time. But remember: the Internet dragnet was shut down until at least July 2010, when John Bates authorized its resumption, and it took some time to turn the dragnet back on. That means NSA conducted a review of a dragnet that was largely on hiatus or just resuming. During the review period, both the phone and Internet dragnet reflect few finalized reports based on either dragnet. Indeed, it appears likely that there were *no* phone dragnet disseminations in August 2010 (see 155). There are probably two explanations for that. It suggests that after Reggie Walton told NSA they had to start following the rules, the amount of intelligence they got from the dragnet appears to have gone down from both the phone and Internet dragnet. But there may be a reason for that: we know that in 2011 NSA was training analysts to re-run queries that came up in both FISA and EO 12333 searches using EO 12333, so the results could be disseminated more broadly. So it's likely that a lot of what had been reports reporting FISA authorized data before 2009 (which didn't always follow FISC's rules) started getting disseminated as EO 12333 authorized reports afterward. Still, in the case of the Internet dragnet reviewed for this report, "the dissemination did not contain PR/TT-derived USP information" so they "did not formally test dissemination objectives" (see footnote 1). *None of the reports on the US Internet dragnet reviewed in some period in 2010 included US person data*.

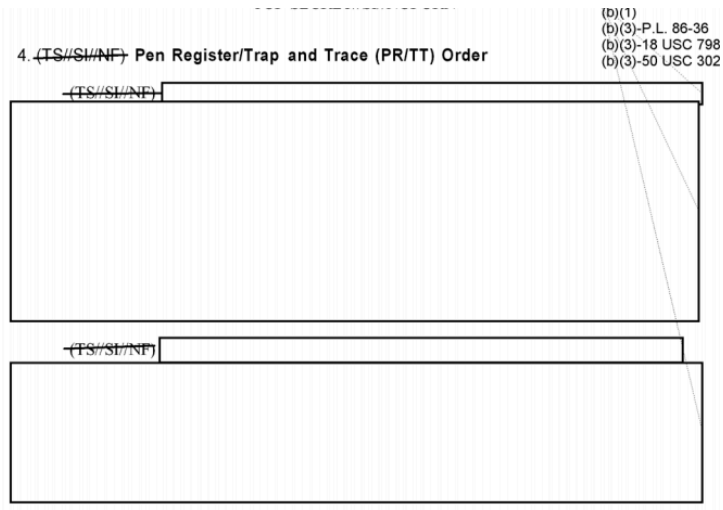
So much for collecting all of Americans' email records to catch Americans, I guess.

All that said, both the Internet and phone dragnet found that the dragnets had adequate controls to fulfill the requirements of the FISC orders, but did say (this is laid out in unredacted form more explicitly in the phone dragnet report) that the manual monitoring of

dissemination would become unworkable if analysts started using the dragnet more. The phone dragnet reports also suggest they weren't good at monitoring less formal disseminations (via email or conversation), and by the time of these summary reports, NSA was preparing ask FISC to change the rules on reporting of non-US person dissemination. Overall in spring 2011, NSA's IG found, the process worked according to the rules, but in part only because it was so little used.

That's the assessment of the PRTT dragnet as of sometime between March and May 2011, less than 9 months before they'd nuke the dragnet really quickly, based mostly off a review of what NSA was doing during a period when the dragnet was largely inactive.

Which is all very interesting, because sometime before June 30, 2011 there was a PRTT violation that got reported — in a far more extensive description than the actual shut down of the dragnet in 2009 — to Intelligence Oversight Board. (see PDF 10)



There's no mention of reporting to Congress on this, which is interesting because PATRIOT Act was being reauthorized again during precisely this period, based off notice, dated February 2, 2011, that the compliance problems were largely solved.

So here's what happened: After having had its IG investigation shut down in fall 2009 because NSA

had never been in compliance with limits on the PRTT dragnet, NSA's IG tried again during a period when the NSA wasn't using it all that much. It gave NSA a clean bill of health no earlier than March 15, 2011. But by June 30, 2011, something significant enough to get reported in two full paragraphs to IOB happened.

It turns out things weren't quote so hunky dory after all.