UNTIL AT LEAST 2014, NSA WAS HAVING TROUBLES PREVENTING BACK DOOR SEARCHES OF UPSTREAM SEARCHES

Since NSA's practice of conducting back door searches — searches of already collected data based off the targeting of foreigners — became widely known, the spooks have offered a few assurances about why we don't have to worry about these back door searches. For example, the US person identifiers have to be pre-approved and the NSA won't conduct back door searches of upstream data, which sometimes includes entirely domestic communications.

According to the Semiannual Reports on Section 702 released some weeks ago, those assurances are fairly hollow, or at least were during the 2013 to 2014 timeframe.

The March 2014 report, which covers the period from December 1, 2012 through May 31, 2013, revealed that the semiannual review process could not directly monitor back door searches on US person identifiers because that information is not kept in a centralized place.

> It should be noted both that NSA's efforts to review queries are not limited to Section 702 authorities and that, at this time, content queries are not specifically identified as containing United States person identifiers. As such, and as the Government previously represented to Congress, NSD and ODNI cannot at this time directly monitor content queries using United States person identifiers because these records are not kept in a centrally located repository. While the

> changes described above in NSA's super audit process have not changed this status, NSA is exploring whether future queries using United States person identifiers could be identified and centralized. In the meantime, and in accordance with NSA's minimization procedures, NSD and ODNI review NSA's approval of any United States person identifiers used to query unminimized Section 702- acquired communications.

This appears to indicate that internal overseers could not audit the actual queries completed, but instead only reviewed the identifiers used to query data to make sure they were approved. Which, in turn, means the NSA's targeting of foreigners and dissemination of reports on them got monitored more closely than NSA's spying on Americans.

The following report — completed in October 2014 and covering the period June 1, 2013 through November 30, 2013 — reports a predictable consequence of the inability to monitor the actual queries conducted as back door searches: prohibited back door searches on upstream data.

> (TS//SI//NF) The joint oversight team, however, is concerned about the increase in incidents involving improper queries using United States person identifiers, including incidents involving NSA's querying of Section 702-acquired data in upstream data using United States Person identifiers. Specifically, although section 3(b)(5) of NSA's Section 702 minimization procedures permits the scanning of media using United States person identifiers, this same section prohibits using United States person identifiers to query Internet communications acquired through NSA's upstream collection techniques. NSA [redacted] incidents of non-compliance with this subsection of its minimization

> procedures, many of which involved analysts inadvertently searching upstream collection. For example, [redacted], the NSA analyst conducted approved querying with United States persons identifiers ([redacted]), but inadvertently forgot to exclude Section 702-acquired upstream data from his query.

While the actual number is redacted, the number is high enough to refer to to "many" improper searches of upstream content.

That explicit violation of the rules set by Bates in 2011 was part of a larger trend of back door search violations, including analysts not obtaining approval to query Americans' identifiers.

> (TS//SI//NF) In addition, section 3(b)(5) of NSA's Section 702 minimization procedures requires that queries using United States person identifiers must be first be approved in accordance with NSA internal procedures. In this reporting period, [redacted] NSA was in non-compliance with this requirement, either because a prior authorization was not obtained or the authorization to query had expired. For example, in NSA Incidents [redacted] NSA analysts performed queries using United States person identifiers that had not been approved as query terms. These queries occurred for a variety of reasons, including because analysts continued queries on terms that they suspected (but had not confirmed) were used by United States persons, forgot to exclude Section 702 data from queries [redacted], or did not realize that [redacted] constitute a United States person identifier even if the analyst was seeking information on a non-United States person.

Among other things, the third redaction in this passage appears to suggest that analysts conduct back door searches on data generally, presumably including both EO 12333 and 702 obtained data, but have to affirmatively exclude Section 702 data to stay within the rules laid out in the minimization procedures.

Consider the timing of this: the reporting of "many" back door search and other US person query violations occurred in the first post-Snowden period. While the fact NSA *did* back door searches was knowable from the 2012 SSCI report on Section 702 renewal, it did not become general knowledge among members of Congress and the general public until Snowden leaked more explicit confirmation of it. And all of a sudden, as soon as people started complaining about back door searches and Congress considered regulating it, NSA's overseers discovered that NSA wasn't following an explicit prohibition on searching upstream data. One of several risks of back door searching upstream data is it may amount to searching data collected domestically, or even entirely domestic communications.

And while the details get even more redacted, it appears the problem did not go away in the following period, the December 1, 2013 through May 31, 2014 reviews reported in a June 2015 report. After a very long redaction on targeting, the report recommends NSA require analysts to state whether they believe they're querying on a US person.

> Additionally, but separately, the joint oversight team believes NSA should assess modifications to systems used to query raw Section 702-acquired data to require analysts to identify when they believe they are using a United States person identifier as a query term. Such an improvement, even if it cannot be adopted universally in all NSA systems, could help prevent instances of otherwise approved United States person

> query terms being used to query upstream Internet transactions, which is prohibited by the NSA minimization procedures.64

The footnote that modifies that discussion is entirely redacted.

The June 2015 report was the most recent one released, so it is unclear whether simply requiring analysts to confirm that they are querying Americans solved the improper back door searches of upstream data. But at least as of the most recently released report, the two most troubling aspects of Section 702 surveillance — the upstream searching on Internet streams and back door unwarranted searches on US person identifiers — were contributing to "many" violations of NSA's rules.