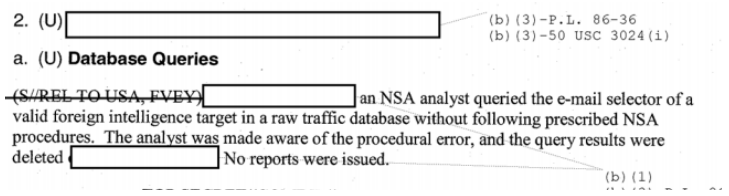
FISA “PHYSICAL SEARCHES” OF RAW TRAFFIC FEEDS, HIDING IN PLAIN SIGHT?

I’m still trudging through NSA’s reports to the Intelligence Oversight Board, which were document dumped just before Christmas. In this post, I want to examine why NSA is redacting one FISA authority, starting with this section of the Q1 2011 report.



2. (U) [redacted]

(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

a. (U) **Database Queries**

~~(S//REL TO USA, FVEY)~~ [redacted] an NSA analyst queried the e-mail selector of a valid foreign intelligence target in a raw traffic database without following prescribed NSA procedures. The analyst was made aware of the procedural error, and the query results were deleted [redacted] No reports were issued.

(b)(1)

During that period, the reports grew to have a bit more structure (this may have been Matt Olsen’s doing, who took over as NSA GC in 2010). Here’s what that Q1 2011 report looks like:

- Violations
    1. EO 12333 violations
    2. FISA violations
    3. Unauthorized data retention
    4. Consensual collection
    5. Unauthorized retention of COMSEC
    6. Computer Network Exploitation (aka hacking, a section which is always entirely redacted and keeps growing in size)
    7. Counterintelligence
    8. Intelligence-related

- OIG Inspections
- Substantive changes to Intelligence Oversight
- Changes to directives and policies
- Procedures

The key change, though, is that the FISA section breaks down by authority, like this, as seen in the Q1 2012 report, which is the most complete example of this

1. NSA/CSS Title I FISA
2. [redacted]
3. BR FISA (phone dragnet)
4. PRTT (Internet dragnet)
5. FAA
    1. 702
    2. 704
    3. 705(b)

After that Q1 2011 report, every single report has that redacted category in the same spot, and every single report redacts it (though I suppose it is possible that whatever is redacted there changes).

I wondered, briefly, if that meant NSA was using a secret authority, some new program that egregiously interpreted a law in a way no one could imagine, just like NSA redefined Section 215 and PRTT. But I don't think that's right.

Rather, I think NSA is making a rather pathetic effort to hide that it uses FISA's physical search provision to obtain emails and other data "stored" in the cloud.

Remember that intercepts (50 USC 1806, which is subchapter I of FISA) and physical search (50 USC 1821, which is subchapter II) are different authorities under FISA, each requiring notice to defendants, though they are usually noticed in the same filing (as here to Reaz Qadir Khan). While it's possible the redacted authority instead designates a different agency (remember that FBI is the front end on a lot of Internet collection), the analysts referred to in these sections are described as NSA analysts. So I suspect it distinguishes between the two types of individualized FISA orders. And it'd be hard to believe there were no IOB violations under 1821, so it must be there somewhere.

Further, I suspect NSA is hiding what appears in some of these reports as a redacted unclassified detail because the descriptions make it clear NSA is querying out of raw traffic databases.

Here's a summary of the violations noted for this redacted authority:

> Q1 2011
>
> Analyst queries email selector of valid foreign intelligence target in raw traffic database without following procedure.
>
> Analyst erroneously targets email selector.
>
> Q2 2011
>
> Nothing to report.
>
> Q3 2011
>
> Nothing to report.
>
> Q4 2011
>
> Analyst cleaning out a newly assigned office found a FISA-derived document from some time ago.
>
> Q1 2012
>
> Data was sent to a server that was not authorized to hold FISA data.
>
> NSA discovered 12 analysts had access to a database for which they had not completed required training.
>
> Q2 2012

> A routine audit revealed an analyst had made two poorly constructed queries.
>
> “An NSA analyst mistaken accessed [redacted] data. The analyst was authorized to view [redacted] data but had not completed the minimization training required by the FISC order. Access to the data has been restricted to database administrators while database capabilities to restrict access are reviewed.”
>
> Q3 2012
>
> NSA notified DOJ that a number of queries had not been reviewed. NSA analysts have been reviewing and reconciling past queries.
>
> An auditor discovered that an analyst had run a database query that included something impermissible.
>
> An NSA analyst discovered an overly broad database query.
>
> An auditor determined an analyst had queried a raw traffic database before conducting required research.
>
> 4Q 2012
>
> An NSA analyst forwarded information in an email the analyst was no longer authorized to receive.
>
> 1Q 2013
>
> Nothing to report
>
> 2Q 2013
>
> “An analyst executed a query of identifiers provided to NSA by [redacted] with a high risk of terrorist connections.” He appears to have been unaware of something about the query and so destroyed the results.
>
> Analysts may have been able to see data

> they did not have authorization (training) to see.

These all seem query driven. And at least some of them access "raw traffic databases." Mind you, there are some Title I violations that also include raw traffic databases (see the database violations in Q2 2011, Q2 2012, and Q1 2013, as well as the unauthorized retention and access violations in Q4 2012, though the retentions violation discusses "authorizations" and so may cross authorities).

There are not, however, any discussions of tasking and detasking violations under the redacted authority, which are the most common kind of violation under FISA. That either suggests the redacted authority collects no communications in real time (which would accord with my understanding of how the NSA has been using physical searches to get data stored on a cloud) or it is not dependent on US presence (which might mean this access data collected overseas on people in the US).

Note, there are also no mentions of telephony traffic under the redacted authority, whereas many, though not all, of the Title I authority violations involve phone traffic (which of course would be harder to get from a stored location).

The other thing the comparison of Title I with this redacted authority makes clear is that there is a special set of minimization procedures for the authority.

This is just a guess, but I'm wondering whether what this redaction hides is the use of physical search orders to permit the search of XKeyscore data, which may either be collected here or overseas. If so, it'd be an interesting question of whether a 5 to 30 day buffer represents communication stored in a physical space.

In any case, given that NSA is hiding reference to an authority that is clearly marked as *unclassified*, it seems ACLU ought to be able to convince a court to liberate the reference.

Defense attorneys barely realize the government uses physical search orders to get cloud content. If they’re using it to do something like access a temporary XKS buffer, then it would raise really interesting Fourth Amendment questions. Which may well be why NSA is hiding it.