WORKING THREAD: NSL IG REPORT

I give up. I'm going to have to do a working thread on the IG Report on FBI's use of NSLs. Here goes. References are to page numbers, not PDF numbers (PDF numbers are page+15).

ix: The report noted that NSL numbers dropped off what they had been 2007 to 2009. It speculates that may have been because of heightened scrutiny. I wonder it wasn't because they were misusing the phone and Internet dragnet programs and getting the information that way. In 2009, after which the NSL numbers grew again, Reggie Walton shut that option down.

x: About half of NSLs during this period were used to investigate USPs.

x: "certain Internet providers refused to provide electronic communication transactional records in response to ECPA NSLs."

xii: They're hiding the current status of permitting the use of NSLs to get journo contacts. Which would seem to confirm they are doing so.

xiii: They're also hiding the status of the OLC memo they used to say they could get phone records voluntarily (see this post for why). They don't hide things very well.

2: It just makes me nuts we're only now reviewing NSL use from 2009. Know what has happened in the interim, for example? A key player in this stuff, Valerie Caproni, has become a lifetime appointed judge.

11: Report notes that FBI tends to always use "overproduction" whether or not it was unauthorized or simply too broad.

17: Footnote 35 seems to suggest they have exceptions to the mandatory reporting requirements. What could go wrong?

39: So as recently as 2009, the tracking system did not alert OGC of manual NSLs in some percentage of the cases.

57 The numbers reported to Congress are off from the numbers shown to IG by as much as 2,800.

58: Love footnote 73, which aims to explain why the NSL numbers reported to Congress are significantly lower than those reported to OIG.

> After reviewing the draft of this report, the FBI told the OIG for the first time that the NSL data provided to Congress would almost never match the NSL data provided to the OIG because the NSL data provided to Congress includes NSLs issued from case files marked "sensitive," whereas the NSL data provided to the OIG does not. According to the FBI, the unit that provided NSL data to the OIG does not have access to the case files marked "sensitive" and was therefore unable to provide complete NSL data to the OIG. The assertion that the FBI provided more NSL data to Congress than to the OIG does not explain the disparities we found in this review, however, because the disparities we found reflected that the FBI reported fewer NSL requests to Congress than the aggregate totals.

The FBI just gives up on 100% accuracy in its NSL numbers.

> After reviewing the draft of this report, the FBI told the OIG that while 100 percent accuracy can be a helpful goal, attempting to obtain 100 percent accuracy in the NSL subsystem would create an undue burden without providing corresponding benefits. The FBI also stated that it has taken steps to minimize error to the greatest extent possible.

59: On the discrepancies, OIG points out the obvious:

> [T]he total number of manually generated NSLs that the FBI inspectors identified is relatively small compared to the total number of 30,442 NSL requests issued by the FBI that year. What remains unknown, however is, whether the FBI inspectors identified all the manually identified generally NSLs issued by the FBI or whether a significant number remains unaccounted for and unreported.

61: The database tracking 2007 requests — a year where there were discrepancies for 215 orders too — "is retired and unavailable."

62: The report doesn't have subscriber only data, which I suspect is obtained in bulk.

63: There is a significant change in the make-up of what FBI is getting in 2009, from subscriber records and toll and financial records in 2008 to toll records, then subscriber and electronic communication records in 2009. I strongly suspect that says some of the 214 and 215 collection moved to NSLs.

71: Apparently it was the release of an earlier OLC memo that led at least 2 Internet companies to refuse NSLs.

> The decision of these [redacted] Internet companies to discontinue producing electronic communication transactional records in response to NSLs followed public release of a legal opinion issued by the Department's Office of Legal Counsel (OLC) regarding the application of ECPA Section 2709 to various types of information. The FBI General Counsel sought guidance from the OLC on, among other things, whether the four types of information listed in subsection (b) of Section 2709 — the subscriber's name, address, length of

> service, and local and long distance toll billing records – are exhaustive or merely illustrative of the information that the FBI may request in an NSL. In a November 2008 opinion, the OLC concluded that the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL.
>
> Although the OLC opinion did not focus on electronic communication transaction records specifically, according to the FBI, [redacted] took a legal position based on the opinion that if the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL, then the FBI does not have the authority to compel the production of electornic communication transactional records because that term does not appear in subsection (b).

73: Oh, that's why 215 orders have expanded: because of the Internet companies that won't respond to NSLs.

> In the absence of a legislative amendment to Section 2709, [2.5 lines redacted].85 Siegel told us that the process of generating and approving a Section 215 application is similar to the NSL process for the agents and supervisors in the field, but then the applications undergo a review process in NSLB and the Department's National Security Division, which submits the application to the Foreign Intelligence Surveillance Court (FISA Court). According to Siegel, a request that at one time could be accomplished with an NSL in a matter of hours if necessary, now takes about 30-40 days to accomplish with a standard Section 215 application.86

> In addition to increasing the time it takes to obtain transactional records, Section 215 requests, unlike NSL requests, require the involvement of FBI Headquarters, NSD, and the FISA Court. Supervisors in the Operations Section of NSD, which submits Section 215 applications to the FISA Court, told us that the majority of Section 215 applications submitted to the FISA Court [redacted] in 2010 and [redacted] in 2011 – concerned requests for electronic communication transaction records.87
>
> The NSD supervisors told us that at first they intended the [3.5 lines redacted] They told us that when a legislative change no longer appeared imminent and [3 lines redacted] and by taking steps to better streamline the application process.
>
> We asked whether the disagreement and uncertainty over electronic communication transactional records has negatively affected national security investigations. An Assistant General Counsel in NSLB told us that the additional time it takes to obtain transactional records through a Section 215 application slows down national security investigations, all of which he said are time-sensitive. He said that an investigative subject can cease activities or move out of the country within the time-frame now necessary to obtain a FISA order.

86: According to the NSD, the FBI can formally request that the NSD expedite the preparation of any FISA application when necessary.

78: Apparently some of the changes in reporting provider overproduction arose in response to the DIOG—but that's classified.

79: During the period covered, FBI personnel

reported 1,398 violations, a huge increase on previous years. IG attributes this to heightened awareness and oversight. Thought 1,000 of the reported incidents were retroactive.

79: The 2008 OLC memo led to some retroactive reporting.

95: IG considers the retention of "associated" toll records (those people on the same family plan) to be a violation. FBI doesn't. I wonder if this is related to "connection chaining"? One of these, however, related to the phone a target used at a lab, sharing with others.

101: OGC first started considering what was included in credit reports in September 2010.

106: Note that manual NSLs violate at a higher rate. While it may be because all of them (allegedly) get reviewed, I wonder whether they're also subject to less pre-NSL oversight?

108: Yup

> FBI inspectors found significantly more compliance failures resulting from the use of manually generated NSLs than from the use of NSLs generated by the NSL subsystem, despite the fact that manually generated NSLs and approval ECs comprised a relativley small portion fo the 2008 and 2009 sample selections.

110: The distant NSL problem seems like it could be significant given how a lot of terrorism investigations run off general ones launched in DC.

111: It sounds like CTD (in DC) submitted NSLs using remote records. The CTAU would contact locals after data already uploaded and ask them to determine if overproduction.

117: IG catches FBI at claiming an improvement in stats by changing their policy on reporting errors.

> Because of the change in IOB policy

> described above, the FBI included uncompounded third party errors in the calculation of the PIOB rate but excluded those errors from the PIOB rate calculation in its 2008 and 2009 reviews.

119: Not sure if the FBI's Inspections people are EVER going to look at NSLs at HQ. Doesn't seem like they have.

120: Note the inclusion of "calling circle" information, in unredacted form, but something equivalent to it in still redacted form. Location?

124: I think this bit — the description of what FBI would like ECPA's definition to be — is redacted elsewhere.

> The proposed amendment would authorize the FBI to obtain name, address, local and long distance connection records (or sessions times and durations), length and types of service, telephone or instrument number (or other subscriber number or identity, including any temporarily assigned network address), means and source of payment (including credit card or bank account number), and records identifying the origin, routing, or destination of electronic communications.

126: There were just 3 manual NSLs between SF and Boston over 2 years.

131: Looks like one of the violations involved getting subject lines and/or URLs.

132: FBI redacted a paragraph of atty-client having to do with whether this subject line type thing was a violation. It involved one of the biggest email providers.

133: Whatever provider in question was providing content in excel spreadsheets until 2011. 2011, of course, is when NSA shut down the (domestic)

dragnet.Though later it becomes clear this is a telecom, not an Internet company.

140: FBI gets 5-6 digits worth of NSLs from Internet provider who was giving some kind of content. In response to recognition they probably got a lot of stuff they shouldn't they just said it would be onerous to clean up their own files.

153: It's clear FBI's getting stuff from AT&T and, probably, Sprint that they shouldn't. Some of this is stuff the telecom has in aggregate — FBI claims they can hand it over because it's not a call record and therefore not protected by ECPA. The other is something that could, but is not, used for billing (location is a good guess). Basically, when the telecoms signed new contracts in 2009, FBI included this without the OGC reviewing it that closely.

157: FBI sometimes gets "associated" records — those on the same family plan. I wonder if this is tied to "connection chaining"?

170: There are no contracts governing the acquisition of:

- Email records
- Financial records
- Consumer credit records

173: FBI doesn't want to say 2703/2709 prohibits hot numbers for some reason—likely because of the alert function they're trying to build on the phone dragnet.

175: DIOG now appears to prohibit the use of NSLs to get community of interest information, but not the use of GJ subpoenas.

180: Standards for declarations supposedly went up in 2006.

182: One of the attorney-client privilege redacted paragraphs discusses the January 8, 2010 OLC opinion.

183: FBI told oversight committees (it does not

say whether this includes both judiciary and intel or not) that it would not change policy. But policy on the phone dragnet side was apparently already to obtain these records.

183: Note the discussion about community of interest requests.

183: A big discussion of how they've changed this policy is totally redacted. The change was in 2012.

185: The reference "even with regard to telephone billing records" suggests they also used the opinion for something else.

193: This section seems to indicate that on 10/7/13 FBI formally told IG they don't use the OLC opinion.

PDF 221: LOL at the FBI citing "redaction" in its response.