SECOND WORKING THREAD ON EXIGENT LETTER IG REPORT

It has taken me a while. But I've finally gotten through the DOJ IG Report on exigent letters. Page numbers below will be to the PDF page.

Page 14: Footnote 1 notes there are Secret and TS/SCI versions of this report. Keep that in mind as you read the redactions—while it's probably safe to assume that Feingold and Wyden (who are both on SSCI) have seen the entire report, it's not clear who else will have seen the entire report.

Page 14: I hadn't really noticed it before, but the time frame on the first IG Report's investigation of exigent letters ended on December 16, 2005—the day that Eric Lichtblau and James Risen exposed the illegal wiretap program. That suggests that the use of exigent letters, among other things, may have changed on that date in response to the discovery of the program. Also note that in Fine's first report on NSLs, he decided to lump 2005 in which the time frame—2002 to 2004—required by statute. This is parallel to what he did with Section 215, suggesting that there were significant changes in 2006 after disclosure of the overall program.

Page 18: Note that the IG Report doesn't say **when** the Public Integrity Section declined to prosecute these abuses. I do hope Fine gets asked that question.

Page 24: Notes that most exigent letters issues from April 2003 to March 2006. That latter date suggests they implemented a fix with the PATRIOT revision passed that month.

Page 28: Note the organization of the Communication Exploitation Section (CXS):

- Document Exploitation (which

became Digital Media Exploitation on March 26, 2006

- Communication Analysis Unit (the section that issued the exigent letters, and therefore working on communities of interest)
- Electronic Communication Analysis Unit (how does this differ from CAU???) (ECAU)
- Electronic Surveillance Operations and Sharing Unit (EOPS)

Does this suggest the EOPS collected this stuff and the others did network analysis on it?

Page 29: Note the final date for the exigent letter range here is November 13, 2006, which is different from the December 16, 2005 used elsewhere

Page 34: Note how Company A (AT&T per EFF's math) does something (maybe "analyze" toll records) that the other two providers don't do (per footnote 26).This is almost certainly the community of interest analysis. This may sugges that by default mean they were working with massive data collection, since it would mean they had access to the signals of their competitors?

There also must be internet analysis in here (which presumably might be the ECAU), which itself would seem to require telecom assistance. So I wonder whether that fully-redacted paragraph describes a contract that does both phone and internet analysis?

Page 35: Does the redaction showing the size of the contract midway down the page appear to be 10 digits? Suggesting the contract would be in the single million range? (That making the

digits something like this: $X,XXX,XXX) Though the amount for Company B seems to consist of words, not just numbers.

Page 36: The language about whether companies were able to provide subscriber data or not closely resembles language surrounding Section 215, which was used during some of this time period to get subscriber data (though possibly in larger batches). And note the redacted second half of the first full paragraph on this page says that they were also doing something in addition to giving meta data and subscriber data. And footnote 28, saying that Company A would only provide subscriber data, suggests that that company (AT&T?) was demanding more than one of the others was, legally.

Page 37: The IG report notes, but does not say explicitly, that the computers at CAU networked into service providers were not segregated from FBI employee space. Are they suggesting FBI employees may have accessed the computers directly?

Page 38: Note the redaction of others that service provider employees communicated to—NSA? OGA?

Page 52: Asst Section Chief CXS 2003-2004, John Chaddic: The practice of exigent letters "seemed consistent with at least one classified FBI program ongoing at the time."

Page 56: Note the reference to numbers coming in from somewhere. Remember the description Lichtblau and Risen used of the program—saying it started in earnest after they got AZ's laptop. The grammar of this passage is consistent with the exploitation of numbers they get off of hardware collected in the field.

Page 62: In a description of a "sneak peek" the report does not redact Oregon, but does redact another location. Why are they hiding just one location? Also note that Oregon is the location of (among other things) al Haramain and Brandon Mayfield.

Page 64: Company A (presumably AT&T) was providing 9 different kinds of records to the FBI.

Page 65: Note the reference to FBI data bases, in addition to some other kind of database used for analysis of calls.

Pate 68: The section on community of interest reports is the first significantly redacted section in the report. It's the part that shows where six degrees of separation from OBL was used to do further investigations.

Page 69: Number of Community of interest reports: 50 exigent letters, 250 NSLs, 350 grand jury subpoenas, with boilerplate attached to requests later on.

Page 72: Per one of the analysts doing the community of interest work, they did not segregate the information out—which means there are still people whose contacts have been collected against whom there was no probable cause.

> The CAU Intelligence Analyst responsible for the team that uploaded toll billing records into the [redacted] database told us that when the responsive data was delivered to his team for uploading, the team could not distinguish [full line redacted] numbers provided by Company A in response to community of interest requests. He said he would only be able to identify the records derived from the community of interest requests by analyzing the information accompanying the original request and other background information. This CAU Intelligence Analyst told us that no one in the FBI had every asked him to segregate records obtained in response to community of interest [redacted] requests or asked any questions about the pracitce.

Page 73: The report goes on to admit that if

there was not reason to connect these numbers with an authorized investigation, they violated ECPA.

Page 74: Some details about COI volume.

> One Company A analyst estimated that he may have used the community of interest [redacted] for up to 25 percent of the [redacted] he [redacted]. Company A records show that from 2004 to 2007, Company A analysts used its community of interest [redacted] to review records in its database for 10,070 [redacted] telephone numbers. We believe that most of these numbers were [redacted] by Company A analysts without community of interest requests from the FBI but did not generate records that were provided to the FBI. A Company A attorney told us, based on information provided to him, that the majority of the community of interest [redacted] by the on-site Compnay A analysts did not result in disclosure of any data to the FBI.

Page 86: The details of the August 28, 2007 request to OLC. (Note this was filed not long after PAA was approved).

Page 88: In discussion of communities of interest, it appears that Company A was both providing information in response to requests, and performing some kind of service which might include communities of interest.

> As noted above, we believe that most of Company A's community of interest [redacted] without requests from the FBI as part of Company A's [redacted] service, and records were not provided to the FBI.

Page 115: The IG Report makes it clear that FBI did not tell the reporters all details about the collection of their calls (presumably, that it came through onsite collaboration with the

telecoms).

Page 130: In the description of the third attempt to get a reporter's call data suggests that the process was driven by the Company A (AT&T) employee. The Company A employee actually looked at the content of the reporters' calls, and after he found there were no calls in question (effectively showing that the person in question was not the source for the reporter), they didn't pursue it any further. As the description continues, however, it makes it clear that Company A analyst of his own initiative (apparently) went to the two other Companies' analysts to get them to check their databases for contacts involving the reporter.

Page 137: Note the date of the notice to FISA: August 2008. Which may be in response to the DOJ IG Report on the warrantless wiretap program. (Though the fourth, on page 140, was dated November 2008).

Pae 141: FBI told IG that in February 2006, they instituted new process to make sure FISA applications were accurate. This would have been in aftermath of revelation of illegal program.

Page 184: In the first blanket NSL, 39 of 192 numbers were associated with "domestic terrorism investigations" (but NSLs can only be used for international terrorism investigations).

Page 185: The January 16, 2009 OLC opinion pertained at least in part to whether an Acting DAD could sign an NSL.

Page 187: The July 5, 2006 blanket NSL included 7 numbers that were associated with domestic terrorism investigations.

Page 188: 134 of the numbers on the September blanket NSL were domestic terrorism and criminal investigations.

Page 276: FBI makes a new assertion about not needing any backup to get these records.