PCLOB REPORT, WORKING THREAD

The report is here. I will do a running update of my comments. Page references will be to the report page numbers, not PDF.

(4) Note PCLOB had access to "various inspector general reports."

(6) Note the dates when WH got these conclusions.

(9) PCLOB confirms what I was the first to point out: this program operated without a legal opinion until July 2013. Told ya so.

(10) One of four reasons the program is illegal is bc 215 is written for FBI, not NSA. Also says it violates ECPA.

(11) PCLOB says FBI would have found Moalin w/o the dragnet. Remember, they were investigating his hawala and had a tap on Ayro.

(14) PCLOB confirms only two cases (info sharing/minimization and Yahoo) ever got to FISCR.

(15) On the govt's so-called transparency:

> However, to date the official disclosures relate almost exclusively to specific programs that had already been the subject of leaks, and we must be careful in citing these disclosures as object lessons for what additional transparency might be appropriate in the future.

(17) PCLOB provides several immediate relationships and notes that Obama doesn't need Congress to do them.

(19) Note PCLOB's reference to releasing opinions on programs that have been discontinued bc of continuing relevance. Suspect this refers to more than just the Internet dragnet.

(25) Note PCLOB says the data integrity analysts take out “other unwanted data” in addition to high volume numbers. I believe some sensitive numbers are purged at this step.

(30) PCLOB dances around saying that corporate store leads right to content.

> For instance, such calling records may be integrated with data acquired under other authorities for further analysis

(31) PCLOB notes FBI gets reports on the dragnet. It doesn’t mention CIA and NCTC or other agencies.

(32) CIA and NCTC have no minimization rules for data that comes from 215 reports:

> Other federal agencies also receive information from the NSA that was obtained through Section 215, but the FISA court’s orders do not establish rules for how those agencies must handle the information they receive.83 In addition, the government has informed the FISA court that it may provide telephone numbers derived from the program to “appropriate . . . foreign government agencies.”84

(33) PCLOB notes that FISC doesn’t say what kind of training the dragnet people must get. As a former training professional, their training sucks ass.

(34) Nice description of the monthly reports.

(40) The phrasing for the description of what happened with the Internet dragnet is very interesting.

> After several years of operation, which included significant incidents of noncompliance with the FISA court’s orders, the bulk collection of Internet metadata under FISA court approval was terminated. Upon concluding that the

> program's value was limited, the NSA did not seek to renew it.

(40) PCLOB points to the USA Today reporting on the phone dragnet program to explain the telecom urgency for a legal order. That was May 10, the first dragnet order was May 24. They did it in two weeks.

(41) PCLOB makes it clear the government was already planning on moving to Section 215 when the extension was passed in 2006.

> The collection of telephone records under the President's Surveillance Program was classified, however, and the government's plans to seek new legal authority for that collection were not made public. Thus, congressional debates about the terms on which Section 215 should be renewed included no public discussion of the fact that the executive branch was planning to place the NSA's bulk calling records program under the auspices of the reauthorized statute.

(43) Note reference to John Scott Redd.

(44) PCLOB distinguishes the phone dragnet from the Internet one bc the latter was only taking circuits commonly used by terrorist traffic.

(45) The reference to minimization procedures and 2702 in succession makes it clear that Walton's December 2008 response on 2702 was a response to Glenn Fine's IG Report.

(46) Note the [sic] on numbers in the footnote.

(47) PCLOB, like I did, points out the 2009 problems came from continuing features of the illegal program.

(54) Here's a list of the other violations in the phone dragnet. I suspect they're described in the orders the Admin is still withholding.

> The isolated incidents reported to the FISA court comprised the following violations: (1) The NSA inadvertently received a tiny amount of cell site location information from a provider on one occasion (the data was accessible only to technical personnel and was never available to intelligence analysts); (2) An analyst performed a query on a selection term whose RAS approval had expired earlier that month (the agency responded with technical modifications to prevent such incidents); (3) A RAS determination was made based on what was later discovered to be incorrect information (the resulting query results were destroyed, and no intelligence reports were issued based on the query); (4) On several occasions analysts shared the results of queries via email with NSA personnel who were not authorized to receive such information (the agency responded with new procedures for email distribution); (5) An analyst sent an email message containing information derived from the Section 215 data to the wrong person, due to a typographical error in the email address (the recipient reportedly deleted the message without reading it, recognizing the error); (6) Information about U.S. persons was on three occasions disseminated outside the NSA before any official made the determinations that are required for such disseminations (officials later concluded that the standards for dissemination were satisfied in each case); (7) The government filed nine reports with the FISA court that lacked certain information required to be in such reports (the missing information involved no wrongdoing or noncompliance, and it subsequently was furnished to the court); (8) The government filed a compliance report with the FISA court on

> a Monday, instead of on the deadline the previous Friday.
>
> The two other noncompliance incidents were more far-reaching, although both represented inadvertent violations. In one incident, NSA technical personnel discovered a technical server with nearly 3,000 files containing call detail records that were more than five years old, but that had not been destroyed in accordance with the applicable retention rules. These files were among those used in connection with a migration of call detail records to a new system. Because a single file may contain more than one call detail record, and because the files were promptly destroyed by agency technical personnel, the NSA could not provide an estimate regarding the volume of calling records that were retained beyond the five-year limit. The technical server in question was not available to intelligence analysts.
>
> In the other incident, the NSA discovered that it had unintentionally received a large quantity of customer credit card numbers from a provider. These related to cases in which a customer used a credit card to pay for a phone call. This problem, which involved cases in which customers used credit cards to pay for phone calls, resulted from a software change implemented by the provider without notice to the NSA. In response to the discovery, the NSA masked the credit card data so that it would not be viewable for intelligence analysis. It also asked providers to give advance notice of changes that might affect the data transmitted to the NSA. The agency later eliminated the credit card data from its analytic stores, although the data remained in the agency’s non-analytic online stores

> and in back-up tapes. Despite repeated efforts to attempt a technical fix, six months later the agency was still receiving a significant amount of credit card information from the provider. As a result of additional efforts, this was reduced to fewer than five credit card numbers per month, and the provider continued to work to eliminate such production entirely.

(58) My favorite line so far:

> Notably, Section 215 requires that records sought be relevant to 'an' authorized investigation.

(61) The PCLOB smackdown on the legal logic behind the dragnet is delightful (is anyone here familiar enough w/Wald's judicial style to tell me whether this is all her?). The passage on "necessity" is important because it pushes back on underlying claims in OLC memos.

(65) We keep talking about the scope of the data NSA gets. This suggests it's closer to "all."

> As to that type of record, however, the government seeks access to virtually everything.

(69) Ow. I always suspected the White Paper citations on civil discovery were manufactured. PCLOB rips it to shreds.

(73) FN 267 argues Govt has a burden to show relevance. Somewhere, FISC even argued they were presumed regular.

(74) Note reference to House Report on PATRIOT debate—govt was looking for administrative subpoenas.

(80) Reading PCLOB's discussion of the need to have a belief makes me realize that belief was used as the same kind of dodge in the 215 argument as it was in the torture context.

(82) PCLOB calls the phone dragnet "an ongoing surveillance tool." Someone alert DiFi.

(94) PCLOB notes that NSL standards for phone metadata are actually higher than 215 standards. Given my suspicion FBI uses bulk NSLs for subscribe info, I find that partiularly interesting.

(96) I believe I've made this point too: given that there was no judicial opinion that approved the dragnet before it was reauthorized, Congress cannot be said to have authorized it.

(96) I like this:

> Applying the reenactment doctrine to legitimize the government's interpretation of Section 215, therefore, is both unsupported by legal precedent and unacceptable as a matter of democratic accountability.

(97) PCLOB is unaware that the Executive had not complied w/FAA requirements to share legal opinions on at least some of the Section 215 materials. (98) Hahaha! PCLOB did, at least, note that HPSCI did not pass on the 2011 notice to Congress. (99) PCLOB again suggests that the dragnet is designed to collect all call data.

> While the briefing paper explains that the NSA's program operates "on a very large scale" and involves "substantially all" of the calling records generated by "certain" telephone companies, it does not make explicit that the program is designed to collect the records of essentially all telephone calls.

(103) A novel idea:

> And we recommend as a policy matter that all three branches of government, in developing and assessing data collection programs, look beyond the application of cases decided in a very different environment and instead consider how to

> preserve the underlying constitutional principles in the face of modern communications technology and surveillance capabilities.

(133) PCLOB suggests the only thing protecting the dranget (in, for example, Amnesty v Clapper) from a First Amendment review is standing.

> However, in the cases decided so far, the Court has not reached the underlying question of whether the First Amendment has been violated, because the Court has found that the individuals challenging the surveillance program are not legally entitled to do so because they are unable to show that they are directly affected by the monitoring.

(140) PCLOB associates the Exigent Letters IG Report to this program. Says AT&T provided 2 hops on community of interest. Note the observation that AT&T could do 2 hops is new and not in unredacted text.

(144) PCLOB makes clear what I've been saying: the phone dragnet leads to the content.

> Any attempt to assess the value of the NSA's telephone records program must be cognizant of a few considerations. First, the information that the NSA obtains through Section 215 is not utilized in a vacuum. Rather, it is combined with information obtained under different legal authorities, including the Signals Intelligence that the NSA captures under Executive Order 12333, traditional wiretaps and other electronic surveillance of suspects conducted under FISA court authority, the interception of telephone calls and emails authorized by the FISA Amendments Act of 2008, the collection of communications metadata through FISA's pen register and trap and trace

> provision, physical surveillance, and the development of informants. The intelligence community views the NSA's Section 215 program as complementing and working in tandem with these and other intelligence sources, enabling analysts to paint a more comprehensive a picture when examining potential national security threats.

(155) PCLOB raises a point I have: why didn't the dragnet find the other unsuccessful attacks?

> Yet, it is worth noting that the program supplied no advance notice of attempted attacks on the New York City subway, the failed Christmas Day airliner bombing, or the failed Times Square car bombing.

(182) Note PCLOB met with John Bates. Interesting that neither PCLOB nor the Review Group were very sympathetic to FISC concerns.

(193) Mike Rogers has been warned.

> We expect to return to transparency in our future work.

(205) On 12333

> Our suggestions here focus on FISA authorities and are also relevant to National Security Letters. Our recommendations do not address reporting of activities under Executiv e Order 12333. It has become clear in recent months that E.O. 12333 collection poses important new questions in the age of globalized communications networks, but the Board has not yet attempted to address those issues.

(210) One of Brand's excuses for why PCLOB shouldn't weigh in on law?

> This legal question will be resolved by

> the courts, not by this Board, **which does not have the benefit of traditional adversarial legal briefing** and is not particularly well – suited to conducting de novo review of long – standing statutory interpretations