THE FBI PRTT DOCUMENTS: THE PARAGRAPH 31 PCTDD TECHNIQUE

I've been working my way through a series of documents in EPIC's FOIA for FISA PRTT documents. This is the last of a series of posts where I unpack the Internet dragnet documents. This post tracks what the reports to Congress reveal (largely about the language the government used to hide programs). And this post shows that the government probably used combined PRTT and Section 215 orders to get real-time cell location. The last chunk of documents withheld pertain to what I'll call "the Paragraph 31" technique, after the entirely redacted paragraph in the first David Hardy declaration describing it. The technique is some application of what gets treated as Post Cut-Through Dialed Digits (PCTDD), those digits a person enters after being connected to a phone number, which might include phone tree responses, credit card information, or password information.

The PCTDD DIOG section withheld

We know Paragraph 31 pertains to PCTDD because one of the documents withheld — described as document 1 in the first Hardy declaration — is a section of the Domestic Investigations and Operations Guide that pertains to PCTDD.

> The first document is comprised of pages 186-189 of the DIOG. The DIOG is a manual used by FBI Special Agents in conducting and carrying out investigations. This particular excerpt of the DIOG provides a step-by-step guide in assisting Special Agents in determining whether to utilize a

> specific method in collecting information such as (1) when to use the method and technique; (2) factors to consider when making this determination; (3) how to go about using the specific method and technique; and (4) the type of information that can be gleaned from it

The paragraph cites paragraph 31, so we know it's the same method. As reflected by the Vaughn Index, the pages in question appear to be from the 2008 DIOG, not the 2011 one. The pagination of the two documents reinforces that. There's no way to work the pagination of the 2011 DIOG to land in the PRTT section, whereas those page numbers do point to the PRTT section in the 2008 DIOG. The section in question starts at PDF 79. The key unredacted part reads,

> The definition of both a pen register device and a trap and trace device provides that the information collected by these devices "shall not include the contents of any communication." See 18 U.S.C. § 3127(3) and (4). In addition, 18 U.S.C. § 3121(c) makes explicit the requirement to "use technology reasonably available" that restricts the collection of information "so as not to include the contents of any wire or electronic communications." "Content" includes any information concerning the substance, purport, or meaning of a communication. See 18 U.S.C. §2510(8). When the pen register definition is read in conjunction with the limitation provision, however, it suggests that although a PR/TT device may not be used for the express purpose of collecting content, the incidental collection of content may occur despite the use of "reasonably available" technology to minimize, to the extent feasible, any possible over collection while still allowing the device to collect all of

> the dialing and signaling information authorized.
>
> In addition to this statutory obligation, DOJ has issued a directive in [redacted half line in 2011 DIOG] to all DOJ agencies requiring that no affirmative investigative use may be made of PCTDD incidentally collected that constitutes content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security.

The criminal context of FBI's PCTDD FISA usage

As with the "hybrid" use of PRTT and toll record orders, the concern about PCTDD may have had some tie to criminal proceedings.

On May 24, 2002, Deputy Attorney General Larry Thompson issued a directive on "avoiding collection and investigative use of content in the operation of Pen Registers." It explicitly said that FISA was "outside the scope of this Memorandum."

In 2006 and 2007, the government applied for Pen Registers in EDNY, including PCTDD. The magistrate judge denied the request for PCTDD as content, which led to a process of reconsideration and further briefing, including amicus briefs from EFF and Federal Defenders of NY. [Update: I've been reliably informed that Kollar-Kotelly's request was a response to a MJ Stephen Smith ruling issued in Texas in July 2006.]

During this period, on August 7, 2006, Colleen Kollar-Kotelly ordered briefing in docket PRTT 06-102 on how FBI was fulfilling its obligation, apparently under the 2002 DOJ directive FBI maintained did not apply to FISA, not to affirmatively use PCTDD for any investigative purpose. PDF 39-40

> Judge Kotelly has ordered the FBI to submit a report no later than September 25 (2006). This report must contain:
>
> (1) an explanation of how the FBI is implementing its obligation to make no affirmative investigative use, through pen register authorization, of post-cut-through digits that do not constitute call dialing, routing, addressing or signaling information, except in a rare case in order to prevent an immediate danger of death, serious physical injury or harm to the National Security, addressing in particular: a) whether post-cut-through digits obtained via FISA pen register surveillance are uploaded into TA, Proton, IDW, EDMS, TED, or any other FBI system; and b) if so what procedures are in place to ensure that no affirmative investigative use is made of postcut-through digits that do not constitute call dialing, routing, addressing or signaling information, including whether such procedures mandate that this information be deleted from the relevant system.
>
> (2) an explanation of what procedures are in place to ensure that the Court is notified, as required pursuant to the Courts Order in the above captioned matter, whenever the government decides to make affirmative investigative use of post-cut-through digits that do not constitute call dialing, routing, addressing or signaling information in order to prevent an immediate danger of death, serious physical injury, or harm to the national security.

At the time, at least some of FBI's lawyers believed that for FISA Pen Registers, FBI retained all the PCTDD. PDF 38

> When DSC 3000 is used for a FISA collection, doesn't the DCS 3000 pass

> all to the [redacted](DSC 5000) including the PCTDD—in other words for FISAs the DCS3000 does NOT use the default of not recoding [sic] the PCTTD???? [sic]

This report — dated September 25, 2006 — appears to be the report Kollar-Kotelly requested. It implores her not to follow [redacted], which ~~appears to~~ is a reference ~~the EDNY court~~ Texas decision.

That report is followed by this one — which was submitted on November 1, 2006 — which appears to propose new procedures to convince her to permit the FBI to continue to collect and retain PCTDD.

In other words, during the early part of the period when the FBI was bumping up against a criminal standard prohibiting the retention of PCTDD under protection of minimization procedures, Judge Kollar-Kotelly required FBI to prove its existing (and new) minimization procedures to ensure they were strong enough to comport with the law.

The original PCTDD question was still burbling away in EDNY, however, and in November 2008 Judge Nicholas Garaufis mooted the question of PCTDD based on the government's representation that it would delete the information when it received it.

> On June 11, 2008, the Government applied to Judge Orenstein for authorization to install and use a pen register and trap and trace device on two wireless telephones (the "SUBJECT WIRELESS TELEPHONES"). (Gov. Br. at 5.) The Government requested, *inter alia,* an Order authorizing the recording of post-cut-through dialed digits ("PCTDD") via pen register. PCTDD are digits dialed from a telephone after a call is connected or "cut through." *In the Matter of Applications,* 515 F.Supp.2d

> 325515F.Supp.2d325, 328 (E.D.N.Y.2007) *204 ("Azrack Opinion"). Because PCTDD sometimes transmit information such as bank account numbers and Social Security numbers which constitutes "contents of communications," and because the Pen Register Statute defines a pen register as "a device or process which *records or decodes* dialing … or signaling information… provided, however, that *such information shall not include the contents of any communication,"* 18 U.S.C. § 3127(3) (emphasis added), Judge Orenstein denied the Government's request for authorization to record PCTDD. The Government subsequently appealed Judge Orenstein's denial of its request to this court, asking this court to authorize it to record PCTDD.
>
> On September 23, 2008, in response to the court's request for clarification of the specifics of its request for pen register data, the Government informed the court that the law enforcement agency involved in the investigation of the SUBJECT WIRELESS TELEPHONES will configure its computers so as to immediately delete all PCTDD received from the provider. (Government's September 23, 2008 letter to the court.) Therefore, as the pen registers sought by the Government in this application will not "record" or "decode" content within the meaning of the Pen Register Statute, the legal question presented by the Government in its appeal is moot.[3] As the Government is entitled to the information it now seeks, the court directs the Magistrate Judge to issue, if still necessary, an order authorizing the installation of the pen registers on the SUBJECT WIRELESS TELEPHONES that is consistent with the representations in the Government's letter of September 23,

> 2008.

Note that Garaufis also embraced the hybrid theory other judges had started rejecting in 2005, which I believe lies behind the BRPR orders.

Behind the scenes, there appear to have been changes to the way the government dealt with PCTDD information under FISA collection. This August 17, 2009 Memo of Law appears to revisit the issue (perhaps in light of the final ruling in EDNY in 2008 and/or as part of the PRTT review of that year). It argues over some of the same Pat Leahy language as the other documents do. It appears to refer to the November 2006 document. It discusses the May 24, 2002 over-collection directive as applying only to the criminal context.

But it also describes some changes implemented in July and December 2008 (it's possible there are references to revisions to the DIOG in this section).

That's one reason why several changes between the 2008 and 2011 DIOG are of interest. In addition to the redacted passage on DOJ's 2002 directive (above) probably affirmatively asserting now that the directive does not apply to FISA, there are two other changes in the Pen Register that are unclassified between the two DIOGs. First, the 2011 one reflects a 2010 change in FISC procedure (see Procedure 15 and Section 18 .6.9.5.1.4), no longer permitting (or requiring) the sequestration of over-collected information at FISC. In addition, the 2011 DIOG appears to show an extra use of PCTDD collection (showing 7 total across subsections A and B, as compared to 6).

What becomes clear reviewing the public records (these reports say this explicitly) is that the 2002 DOJ directive against retaining PCTDD applies to the criminal context, not the FISA context. When judges started challenging FBI's authority to retain PCTDD that might include

content under criminal authorities, FBI fought for and won the authority to continue to treat PCTDD using minimization procedures, not deletion. And even the standard for retention of PCTDD that counts as content permits the affirmative investigative use of incidentally collected PCTDD that constitutes content in cases of "harm to the national security."

Whateverthefuck that is.

Which is, I guess, how FBI still has 7 uses of PCTDD, including one new one since 2008.

The details on the withheld documents

Which brings us to the remaining documents on Paragraph 31 the FBI is withholding. In addition to the DIOG and a Westlaw print out (which I would guess is the opinion in the criminal case), there are 4 memoranda and one report described in the first Hardy Declaration, as well as a PRBR motion to retain data that I wouldn't be surprised if FBI used to request the authority to retain, under FISA authority, the materials it said it wouldn't obtain in the EDNY case (in any case, it requested approval to retain some data collected under a hybrid PRBR order). One of the documents in that bunch includes both electronic surveillance (the collection of content) and the use of a pen register (ostensibly non-content). The second Hardy declaration includes 9 FISC orders pertaining to the method, along with a District Court order pertaining to it (which might be that 2008 opinion).

Significantly, 4 of those orders are Primary Orders, suggesting multiple Secondary Orders to providers of some sort, and a program of some bulk. And those documents are only the ones that got shared with Congress, so only the ones that reflected some significant decision.

The declarations don't tell us much about how they're using this PCTDD information. Here are the most informative passages (some of which

show up in both).

> The ability to conduct electronic surveillance through the installation and use of pen registers and trap and trace devices has proven to be an indispensable investigative tool and continues to serve as a building block in many of the FBI's counterterrorism and counterintelligence investigations. The specific type of electronic surveillance has resulted in numerous benefits by providing the FBI valuable substantive information in connection with national security investigations. The information gathered has either confirmed prior investigative information or has contributed to the development of additional investigative information, and has been invaluable in providing investigative leads.
>
> [snip]
>
> [T]he release of such information would reveal actual intelligence activities and methods used by the FBI against specific targets who are the subject of foreign counterintelligence investigations or operations; identify a target of a foreign counterintelligence investigation; or disclose the intelligence gathering capabilities of the activities or methods directed at specific targets.
>
> [snip]
>
> The information protected under this [7(E)] exemption contain details about sensitive law enforcement techniques used by the FBI in gathering valuable intelligence information in current and prospective criminal, counterintelligence, and national security investigations.

What I find most interesting about these

declarations, however, is the near total (maybe even total) silence about terrorism. These are used for “national security” and “counterintelligence” investigations, but nothing explicitly described as a counterterrorism investigation.

While I can see some especially useful applications of PCTDD information in the CI context — imagine how valuable it would be to know the voicemail passwords of Chinese targets, for example — I also wonder whether the FBI is using this stuff primarily for cyber targets. Whatever it is, the government has apparently argued for and maintained the authority to retain PCTDD data in the FISA context, with the ability to use actual content in the event of possible harm to national security.