HOT NUMBERS AND THE 2009 TROUBLES

Starting in 2007, DOJ's Inpector General Glenn Fine did a series of reports on the FBI's use of National Security Letters and Exigent Letters. In response (and as the FBI tried to clean up the mess from its inappropriate use of those tools), in 2007 the government asked OLC for an interpretation on the Electronic Communications Privacy Act. That opinion, which was issued on November 8, 2008, ruled that ECPA barred telecom providers from responding to certain kinds of requests without legal process.

> Finally, you have asked whether a provider, in answer to an oral request before service of an NSL, may tell the FBI whether a particular account exists. This information would be confined to whether a provider serves a particular subscriber or a particular phone number. We believe that ECPA ordinarily bars providers from complying with such requests.

In the last of his IG Reports on NSLs and Exigent Letters, Fine argued that that OLC opinion made two of FBI's practices with exigent letters — "sneak peeks" and "hot numbers" — illegal.

> [T]he Department's Office of Legal Counsel concluded, and we agree, that the ECPA ordinarily bars communications service providers from telling the FBI, prior to service of legal process, whether a particular account exists. We also concluded that if that type of information falls within the ambit of "a record or other information pertaining to a subscriber to or customer of such service" under 18 USC 2702(a)(3), so does the existence of calling activity by particular hot telephone numbers,

> absent a qualifying emergency under 18 USC 2702(c)(4).
>
> [snip]
>
> Therefore, we believe that the practice of obtaining calling activity information about how numbers in these matters without service of legal process violated the ECPA.
>
> [snip]
>
> We believe the FBI should carefully review the circumstances in which FBI personnel asked the on-site communications service providers [redacted] "hot numbers" to enable the Department to determine if the FBI obtained calling activity information under circumstances that trigger discovery or other obligations in any criminal investigations or prosecutions.

The "hot number" practice is functionally equivalent to the "alert list" the NSA used on the Section 215 dragnet database, in which it checked daily incoming calls to see if there had been any US contact with both approved and unapproved identifiers; if there was activity in both cases, it would spark further investigation.

The practice Fine focused on in this report was the requests FBI would get onsite telecom providers to fill without a subpoena. But at the same time Fine was working on that series of reports (the last one wasn't issued until 2010) he was also working on a report on the FBI's 2006 use of Section 215 (issued in March 2008), which included two classified appendices on bulk collection programs including (presumably) the phone dragnet from May until December 2006, and the 2009 Joint IG Report on the illegal wiretap program (which would have covered the dragnet program through May 2006).

We now know that both the pre May 2006 dragnet

program and the post May 2006 dragnet program included a practice that, in wake of that OLC opinion (and perhaps before), Fine would find required some legal attention (the Pen Register equivalent in a grand jury context might put the post May 2006 practice in good stead, the 2008 opinion would seem to make the use of alerts earlier illegal, along with everything else).

Which may be why the government asked Judge Reggie Walton to consider whether the dragnet program complied with ECPA for his December 12, 2008 opinion.

That's just a hypothesis (though the December 2008 would have been the first dragnet application after the OLC memo).

But if it's right, it makes the NSA"s "discovery" of the alert process the following month all the more ridiculous. The alert process had been in place for years. FBI was being scolded for an equivalent practice (that ended in 2006) within FBI. And yet NSA somehow didn't think to tell Walton about it until he had ruled ECPA did not present a problem for the dragnet more generally.

These three programs — the illegal program and the exigent letters, which both became the early dragnet in 2006 — are all closely related. Once you read them in tandem, though, it makes NSA"s claims to ignorance completely incredible.

Which brings me back to a reminder I've made several times. In the wake of the 2009 discoveries, Pat Leahy tried to mandate a DOJ review of the ongoing Section 215 activity, an effort the Administration thwarted. Fine agreed to do one anyway … then left. His replacement, Michael Horowitz, keeps claiming he's still working on that investigation (but only covering the activities through 2009). That investigation has been going on 1,191 days now.

Update: Another interesting timing detail. According to the White Paper, the Intelligence and Judiciary Committees had all received the initial application and Primary Order on the

dragnet by December 2008. So did they wait until the Walton opinion? Or did they know the Judiciary Committees would get them as part of DOJ IG reports?