ABOUT THAT MAY 2007 FISC OPINION

Update, March 11: Docket 07-449 is not an Internet dragnet one (those all have a PR/TT preface). This is one of the bulk collection programs approved in early 2007.

The other day, I pointed to a passage from the October 3, 2011 John Bates opinion,

> The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers"). Insofar as the discrete, wholly domestic "about" communications at issue here are communications between non-target accounts that contain the name of the targeted facility, the same conclusion applies to them.

And suggested the May 31, 2007 order in question was probably the Primary Order for the Internet Dragnet program.

> Given the description, it likely was a primary order for the purportedly defunct Internet dragnet program; if so, it would represent the application of an opinion about metadata to collection including content.

Timewise, that might make sense. Colleen Kollar-Kotelly signed the first Pen Register/Trap &

Trace order for Internet metadata on July 14, 2004. Accounting for some margin of error in reapplications and the 5 days earlier 90-day authorizations would be each year, a May 31 order 3 years after that first order is not far off what you'd expect.

But the description of the opinion — which pertains to messages identified because they contain information "about" a target — seems to refer to content, not metadata (though packets would blur this issue).

> The Court has effectively concluded that certain communications containing a reference to a targeted selector are reasonably likely to contain foreign intelligence information, including communications between non-target accounts that contain the name of the targeted facility in the body of the message. See Docket No. 07-449, May 31, 2007 Primary Order at 12 (finding probable cause to believe that certain "about" communications were "themselves being sent and/or received by one of the targeted foreign powers").

Moreover, this order would have been issued during the period when two FISC orders allowed the collection of content. And those orders — as the 2009 Draft NSA IG Report explains — formalized the claim that a targeted "facility" could consist of a switch carrying general traffic rather than a specific phone number or IP address.

> Ultimately, DoJ decided to pursue a FISC order for content collection wherein the traditional FISA definition of a "facility" as a specific telephone number or email address was changed to encompass the gateway or cable head that foreign targets use for communications. Minimization and probable cause standards would then be applied. As with the PRTT and Business Records orders,

> NSA collaborated with DoJ to prepare the application and declarations and provided the operational requirements needed to continue effective surveillance.
>
> (TS/ lSI! INF) After 18 months of concerted effort and coordination, the FISC ultimately accepted the theory for foreign selectors but rejected it for domestic selectors. Consequently, on 10 January 2007, the FISC signed two separate orders: the Foreign Content Order and the Domestic Content Order.

Yet, not long after these orders were signed — probably in March 2007 (though NSA's IG Report doesn't describe this at all) — another FISC judge sharply curtailed these efforts, ruling some of this collection illegal.

> The judge, whose name could not be learned, concluded early this year that the government had overstepped its authority in attempting to broadly surveil communications between two locations overseas that are passed through routing stations in the United States, according to two other government sources familiar with the decision.
>
> The decision was both a political and practical blow to the administration, which had long held that all of the National Security Agency's enhanced surveillance efforts since 2001 were legal. The administration for years had declined to subject those efforts to the jurisdiction of the Foreign Intelligence Surveillance Court, and after it finally did so in January the court ruled that the administration's legal judgment was at least partly wrong.
>
> The practical effect has been to block the NSA's efforts to collect information

> from a large volume of foreign calls and e-mails that passes through U.S. communications nodes clustered around New York and California.
>
> [snip]
>
> The effect of the judge's decision to curtail some of that surveillance was to limit the flow of information about possible terrorism suspects, according to congressional staffers briefed on the ruling. Last week, McConnell told the Center for Strategic and International Studies that the government faces "this huge backlog trying to get warrants for things that are totally foreign that are threatening to this country."
>
> Gaining access to the foreign communications at issue would allow the NSA to tap into the huge volume of calls, faxes and e-mails that pass from one foreign country to another by way of fiber-optic connections in the United States.

Then Director of National Intelligence started pushing for new legislation in March and April, and the Senate Intelligence Committee held its first hearing on what would become Protect America Act on May 1. At it, Bill Nelson alluded to some of what the FISC judge had rejected; Keith Alexander and Mike McConnell seemed to present a very different notion of the issue than reported by the WaPo.

> SEN. BILL NELSON: Let's go back to your second — General, your second answer.
>
> LTG ALEXANDER: If you know both ends — where the call is going to go to before he makes the call, then you know that both ends were foreign; if you knew that ahead of time, you would not need a warrant.
>
> SEN. NELSON: If you knew that.

> LTG ALEXANDER: If you knew that.
>
> SEN. NELSON: If you did not know that the recipient of the call in the U.S. is foreign, then you would have to have a FISA order.
>
> LTG ALEXANDER: If you collected it in the United States. If you collected it overseas, you would not.
>
> [snip]
>
> SEN. NELSON: I understand that, but — now, I got two different answers to the same question from you, Mr. Director, and from you, General.
>
> MR. McCONNELL: It depends on where the target is and where you collect it. That's why you heard different answers.
>
> SEN. NELSON: So if you're collecting the information in the United States —
>
> MR. McCONNELL: It requires a FISA.
>
> SEN. NELSON: Okay. Under the current law, the president is allowed 72 hours in which he can go ahead and collect information and, after the fact, go back and get the FISA order. Why was that suspended before in the collection of information?
>
> LTG ALEXANDER: Sir, I think that would best be answered in closed session to give you exactly the correct answer, and I think I can do that.
>
> SEN. NELSON: And — well, then, you can acknowledge here that is — it was in fact suspended.
>
> SEN. ROCKEFELLER: I would hope that that would be — we would leave this where it is.

But it seems to suggest that FISC held that collection of communications within the US

involving two foreigners required a warrant, but collection overseas in which only the target was foreign did not require a warrant.

Whatever that ruling though, within weeks of that exchange, the NSA had requested and won a decision holding that conversations about a target met a probable cause standard (and therefore, presumably, did not require a warrant). Particularly given the way Bates uses it, it seems to suggest even in the middle of this dispute, FISC was expanding "about" collection beyond what FISC had authorized for other content. "About" communications met probable cause by their very nature.

Meanwhile, if that opinion is anything like what Bates makes it seem, and presuming Bates was already read into the collection from switches authorized earlier in 2007, then how can he claim to be unaware the government was collecting "about" information?

I don't know what the answers are. But this opinion — issued at a remarkable moment in the transition from illegal to court-sanctioned collection — seems to reflect a rather timely use of "about" collection to bypass limits on domestic surveillance.