THE GOVERNMENT USES FISCR FAST TRACK TO PUT DOWN JUDGES' REBELLION, EXPAND CONTENT COLLECTION

Since it was first proposed, I've been warning (not once but twice!) about the FISCR Fast Track, a part of the USA Freedom Act that would permit the government to immediately ask the FISA Court of Review to review a FISC decision. The idea was sold as a way to get a more senior court to review dodgy FISC decisions. But as I noted, it was also an easy way for the government to use the secretive FISC system to get a circuit level decision that might preempt traditional court decisions they didn't like (I feared they might use FISCR to invalidate the Second Circuit decision finding the phone dragnet to be unlawful, for example).

Sure enough, that's how it got used in its first incarnation — not just to confirm that the FISC can operate by different rules than criminal courts, but also to put down a judges rebellion.

As I noted back in 2014, the FISC has long permitted the government to collect Post Cut Through Dialed Digits using FISA pen registers, though it requires the government to minimize anything counted as content after collection. PCTDD are the numbers you dial after connecting a phone call — perhaps to get a particular extension, enter a password, or transfer money. The FBI is not supposed to do this at the criminal level, but can do so under FISA provided it doesn't use the "content" (like the banking numbers) afterwards. FISC reviewed that issue in 2006 and 2009 (after magistrates in the criminal context deemed PCTDD to be content that was impermissible).

At least year's semiannual FISC judges'

conference, some judges raised concerns about the FISC practice, deciding they needed to get further briefing on the practice. So when approving a standing Pen Register, the FISC told the government it needed further briefing on the issue.

> On October 29, 2015, in conjunction with entertaining the immediately prior application for [redacted] the Court ordered the Government to submit a brief addressing, among other things, the lawfulness of acquiring post-cut-through digits under PR/TT orders. See Docket No. PR/TT 2015-78, Supplemental Order issued on Oct. 29, 2015. That briefing order was issued after the FISC judges discussed the issues presented by post-cut-through digits at their semi-annual conference on October 27, 2015. Id. at 1. Following that discussion, it was the consensus of the judges that further briefing was warranted in view of concerns expressed by some judges about continuing to authorize the acquisition of post-cut-through digits under PR/TT orders.

The government didn't deal with it for three months until just as they were submitting their next application. At that point, there was not enough time to brief the issue at the FISC level, which gave then presiding judge Thomas Hogan the opportunity to approve the PRTT renewal and kick the PCTDD issue to the FISCR, with an amicus.

> Nevertheless, the Court did not appoint an amicus pursuant to § 1803(i)(2)(A) because it found that it was not appropriate to do so under applicable time constraints and in view of the requirement under § 1803(c) to proceed as expeditiously as possible. The prior PR/TT authorization for [redacted] was set to expire on January 22, 2016. See Docket No. PR/TT 15-78, Primary Order for Pen Register and Trap and Trace Device(s) issued on Oct. 29, 2015, at 7. Pursuant to FISC Rule of Procedure 9(a), the Government submitted its proposed application to continue this PR/TT collection on January 15, 2016 (the same date that it filed its most recent legal brief on post-cut-through digits).[6] Unless the Court had permitted authorization for all

This minimized the adversarial input, but put the question where it could carry the weight of a circuit court.

Importantly, when Hogan kicked the issue upstairs, he did not specify that this legal issue applies only to phone PRTTs.

Whether an order issued under 50 U.S.C. § 1842 may authorize the Government to obtain all post-cut-through digits, subject to a prohibition on the affirmative investigative use of any contents thereby acquired, when there is no technology reasonably available to the Government that would permit:

(1) a PR/TT device to acquire post-cut-through digits that are non-content DRAS information, while not acquiring post-cut-through digits that are contents of a communication; or

(2) the Government, at the time it receives information acquired by a PR/TT device, to discard post-cut-through digits that are contents of a communication, while retaining those digits that are non-content DRAS information.

At the FISCR, Mark Zwillinger got appointed as an amicus. He saw the same problem as I did. While the treatment of phone PCTDD is bad but, if properly minimized, not horrible, it becomes horrible once you extend it to the Internet.

[7] The amicus curiae contends that if the government's argument were applied to Internet pen registers, the government could collect information generated by a wide variety of activities on the Internet, including searching, uploading documents, and drafting emails. [redacted] Nonetheless, the amicus argues that the prospect of such collections indicates that the government's statutory construction must be wrong. We disagree. Even assuming that the government's statutory theory would apply in the same manner in that different technological setting, we would have to determine whether any technology is reasonably available to excise content. Moreover, the application of the government's theory in that setting, if it had the consequences argued by amicus curiae, might call for a different Fourth Amendment balancing of interests.

The FISCR didn't much care. They found the collection of content using a PRTT, then promising not to use it except to protect national security (and a few other exceptions to the rule that the government has to ask FISC permission to use this stuff) was cool.

We have reviewed the record and considered briefs from the government and from amicus curiae appointed by the court under 50 U.S.C. § 1803(i) to present argument in this matter. We conclude that section 1842 authorizes, and the Fourth Amendment to the Constitution of the United States does not prohibit, an order of the kind described in the FISC's certification. Read fairly and as a whole, the governing statutes evince Congress's understanding that pen registers and trap-and-trace devices will, under some circumstances, inevitably collect content information. Congress has addressed this difficulty by requiring the government to minimize the incidental collection of content through the employment of such technological measures as are reasonably available—not by barring entirely, as a form of prophylaxis, the use of pen registers and trap-and-trace devices simply because they might gather content incidentally.

Along the way, the FISCR laid out several other precedents that will have really dangerous implications. One is that content to a provider may not be content.

The amicus curiae argues that all post-cut-through digits are content with respect to the service provider, and that the interception of post-cut-through digits should never be authorized. That argument is unconvincing, as the definition of "contents" for purposes of pen registers is "information concerning the substance, purport, or meaning of [a wire, oral, or electronic] communication." 18 U.S.C. § 2510(8). That definition does not include dialing information, whether viewed from the perspective of the individual or the provider. The fact that the provider is not the one who uses that information for dialing purposes does not alter the fact that the information is dialing information. The FCC made that point in its decision on remand from *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000), cited by the amicus curiae. The FCC explained that whether particular information is call-identifying information has nothing to do with "whether a carrier uses the dialed digits as part of its own call processing." *In re Communications Assistance for Law Enforcement Act*, 17 F.C.C.R. 6896 (2002).

This is probably the issue that made the bulk PRTT dragnet illegal in the first place (and created problems when the government resumed it in 2010). Now, the problem of collecting content in packets is eliminated!

Along with this, the FISCR extended the definition of "incidental" to apply to a higher standard of evidence.

> Third, a pen register authorized in a FISA investigation is targeted at dialing information; the collection of any content information from post-cut-through digits is incidental to the purpose of the pen register. The incidental collection of constitutionally protected material does not render the authorized collection of unprotected material unlawful. *See In re Directives*, 551 F.3d at 1015 (citing *United States v. Kahn*, 415 U.S. 143 (1974), and *United States v. Schwartz*, 535 F.2d 160 (2d Cir. 1976) ("Incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful.")).

Thus, it becomes permissible to collect using a standard that doesn't require probable cause something that does, so long as it is "minimized," which doesn't always mean it isn't used.

Finally, FISCR certified the redefinition of "minimization" that FISC has long adopted (and which is crucial in some other programs). Collecting content, but then not using it (except for exceptions that are far too broad), is all good.

> [9] The term "minimization" has a familiar meaning in the context of interceptions of electronic communications. Section 2518(5) of title 18 directs that electronic surveillance must "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception." The requirement of minimization thus contemplates that some unauthorized interception will inevitably occur, but that the agency must take steps to keep that interception to a minimum.

In other words, FISCR not only approved the narrow application of using calling card data but not bank data and passwords (except to protect national security). But they also approved a bunch of other things that the government is going to turn around and use to resume certain programs that were long ago found problematic.

I don't even hate to say this anymore. I told privacy people this (including someone involved in this issue personally). I was told I was being unduly worried. This is, frankly, even worse than I expected (and of course it has been released publicly so the FBI can start chipping away at criminal protections too).

Yet another time my concerns have been not only borne out, but proven to be insufficiently cynical.