~~SECRET~~

THIS IS A COVER SHEET

FOR CLASSIFIED INFORMATION

ALL INDIVIDUALS HANDLING THIS INFORMATION ARE REQUIRED TO PROTECT IT FROM UNAUTHORIZED DISCLOSURE IN THE INTEREST OF THE NATIONAL SECURITY OF THE UNITED STATES.

HANDLING, STORAGE, REPRODUCTION AND DISPOSITION OF THE ATTACHED DOCUMENT WILL BE IN ACCORDANCE WITH APPLICABLE EXECUTIVE ORDER(S), STATUTE(S) AND AGENCY IMPLEMENTING REGULATIONS.

(This cover sheet is unclassified.)

~~SECRET~~

704-101
NSN 7540-01-213-7902

STANDARD FORM 704 (11-10)
Prescribed by NARA/ISOO
32 CFR PART 2001 EO 13526

Previous edition usable

~~SECRET~~

~~(U) UNDER SEAL~~
(X) Docket No. FISCR 16-01

United States Foreign Intelligence Surveillance Court of Review

MAR 31 2016
4:10 p
LeeAnn Flynn Hall, Clerk of Court

b6 Per FBI
b7C

(U) IN THE UNITED STATES
FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

(U) IN RE CERTIFIED QUESTION OF LAW

(S) ON CERTIFICATION FROM THE
UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT
~~(S)~~ DOCKET NUMBER PR/TT 16[redacted] (Hogan, Presiding Judge)

b1 Per FBI
b3
b7E

(U) REPLY BRIEF FOR THE UNITED STATES

JOHN P. CARLIN
Assistant Attorney General for National Security
STUART J. EVANS
J. BRADFORD WIEGMANN
Deputy Assistant Attorneys General
b6, b7C [redacted]
Deputy Chief, Operations Section
Office of Intelligence
b6, b7C [redacted]
Attorney
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
b6, b7C [redacted]

~~SECRET~~

(U) TABLE OF CONTENTS

(U) TABLE OF AUTHORITIES ii

(U) ARGUMENT 1

(U) I. (S) The Pen Register Statute Authorizes the Collection of Post-Cut-Through Dialing and Routing Information. 1

II. (U) The Proper Construction of the Statute Does Not Raise Constitutional Concerns. 8

(U) CONCLUSION 10

(U) CERTIFICATE OF COMPLIANCE 12

(U) CERTIFICATE OF SERVICE 13

(U) TABLE OF AUTHORITIES

Cases

[Redacted] *No. PR/TT* [Redacted] (FISC 2010) 7

City of Ontario v. Quon, 560 U.S. 746 (2010) 10

Director v. Peabody Coal Co., 554 F.2d 310 (7th Cir. 1977) 8

Illinois v. Lafayette, 462 U.S. 640 (1983) 10

In re Application of the United States, 622 F. Supp. 2d 411 (S.D. Tex. 2007) 3

In re Applications of the United States, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) 3

In re Directives, 551 F.3d 1004 (FISA Ct. Rev. 2008) 9

Panama R. Co. v. Johnson, 264 U.S. 375 (1924) 8

United States v. McKinnon, 721 F.2d 19 (1st Cir. 1983) 9

United States v. Miller, 425 U.S. 435 (1976) 10

Statutes

18 U.S.C. § 3121(c) 2, 3, 4, 5, 7, 8

18 U.S.C. § 3123(a)(3) 8

18 U.S.C. § 3127 7

18 U.S.C. § 3127(3) 1, 2, 5, 7, 8

18 U.S.C. § 3127(4) 1, 5

50 U.S.C. § 1841(2) 1, 7

50 U.S.C. § 1842 7

50 U.S.C. § 1842(h)(2) 4, 8

50 U.S.C. § 1845 3

Other Authorities

147 Cong. Rec. S11000 5

H.R. Rep. No. 103-827, pt. 1 (1994) 5

S. Rep. No. 103-402 (1994) 5

(U) ARGUMENT

I. (U) (S) The Pen Register Statute Authorizes the Collection of Post-Cut-Through Dialing and Routing Information.

(U) (S) The criminal pen register and trap and trace ("PR/TT") provisions authorize the collection of dialing and routing information both pre- and post-cut-through, and the FISA PR/TT provisions incorporate, and reinforce, that authority.

(U) **A.** (S) The linchpin of amicus' argument is that "a device that records contents, *even if only sometimes,* is not a pen register or trap and trace device." Amicus Br. 15 (emphasis added). On amicus' understanding, capturing a *single* instance of "content" while collecting dialing, routing, addressing or signaling ("DRAS") information instantaneously converts a PR/TT device into a wiretap. *See id.* at 16 ("If a device captures content, it is by definition not a pen register or a trap and trace device."). This absolutist interpretation of the PR/TT statute is incorrect, fails to harmonize the statutory scheme, and leads to anomalous results.

(U) **1.** (S) Title 18's definition of a "pen register" — a "device or process which records or decodes [DRAS] information . . . provided [ ] that such information shall not include the contents of any communication" — expressly allows the government to collect DRAS information and does not distinguish between the collection of DRAS pre-cut-through versus post-cut-through. 18 U.S.C. § 3127(3); *see id.* § 3127(4) (similar for trap and trace device); 50 U.S.C. § 1841(2)

(providing that FISA PR/TTs shall have the same "meaning" as Title 18 PR/TTs). The proviso that "such information" shall not include the "contents" of communications prevents the government from using pen registers purposefully to obtain content under the guise of collecting DRAS; the incidental, unavoidable collection of post-cut-through digits that may include content by a pen register targeting DRAS is not prohibited. This reading of the statutory language harmonizes the definition of section 3127(3) with 18 U.S.C. § 3121(c), giving both provisions meaning and rendering neither superfluous.

(U) (S) By contrast, amicus' interpretation of the criminal PR/TT scheme fails to make sense of the two provisions. Amicus construes section 3127(3) as establishing an absolute and categorical prohibition on decoding the "contents of any communication," including incidental collection of non-DRAS digits that may include content. Amicus then construes section 3121(c) as requiring the government to use "reasonably available" technology to avoid collecting the "contents of any communication." But amicus' construction of the two provisions renders section 3121(c) entirely superfluous. If section 3127(3) establishes an absolute prohibition, as amicus argues, Congress had no reason also to direct the government to use "reasonably available" technology to avoid such collection.

(U) (S) That is why several of the opinions on which amicus relies candidly

admit that amicus' interpretation creates an anomaly. *See In re Application of the United States*, 622 F. Supp. 2d 411, 420 (S.D. Tex. 2007) (remarking on the "contradiction inherent in the [pen register] statute"); *In re Applications of the United States*, 515 F. Supp. 2d 325, 332, 335 (E.D.N.Y. 2007) (magistrate judge opinion) (noting that "a contradiction arises" and that section 3121(c) "is superfluous if the ban on content acquisition is absolute"). This Court should not embrace an interpretation that leads to "contradiction" and "superflu[ity]" when the FISC's alternative construction harmonizes all of the statute's provisions.

(U) ~~(S)~~ To the extent there is any ambiguity in the *criminal* provisions, however, the *FISA* PR/TT statute's suppression and minimization provisions eliminate it. As amicus concedes, the existence of suppression and minimization provisions suggests that a statute (in amicus' words) "authorize[s] overcollection" and minimization. Amicus Br. 20. But amicus claims that "[u]nlike other surveillance statutes, Congress did not build a minimization or a suppression scheme into" the FISA PR/TT statute. *Id.*; *id.* at 11-12 ("the PR/TT statutes contain no mention of minimization or suppression"). This assertion is puzzling. As the government explained in its opening brief, the FISA PR/TT statute does contain a suppression remedy. *See* 50 U.S.C. § 1845; Gov't Br. 10-11.

(U) ~~(S)~~ Moreover, following amendments in 2015, FISA also authorizes the

FISC or the Attorney General to "impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device." 50 U.S.C. § 1842(h)(2). Amicus tries to distinguish section 1842(h)(2)'s express minimization authorization on three grounds, all unavailing. Amicus first notes that the provision only allows the FISC or Attorney General to impose "*additional*" procedures. Amicus Br. 21. That is true, but irrelevant, because all minimization techniques are "additional" in the sense that they *add* protections to those already specified by statute. Amicus next claims that section 1842(h)(2) authorizes the government to minimize only "the use of *non-content* data." Amicus Br. 21. But the provision does not distinguish between content and non-content information. Finally, amicus argues that section 1842(h)(2) "should not be read to *expand*" government FISA PR/TT authority. Amicus Br. 21. But that argument misses the point. Section 1842(h)(2) does not "expand" government authority, but rather confirms that the government may, using a FISA PR/TT, incidentally collect content, subject to appropriate minimization.

(U) **2.** (S) Amicus claims that section 3121(c) does not "authorize any governmental conduct," but rather "restricts conduct." Amicus Br. 19, 23-25. This dichotomy between statutes that "authorize" (or "expand") conduct and statutes that "limit" conduct, however, overlooks a third possibility: A statute can

accomplish two aims, at the same time, by *both* authorizing (or clarifying pre-existing authority) *and* limiting conduct. Section 3121(c) does precisely that — not by "expanding" the government's authority but by clarifying that sections 3127(3) and 3127(4) apply to the targeted, and not incidental, collection of content. At the same time, section 3121(c) limits the government's authority by requiring the government to use "reasonably available" technology in PR/TTs to avoid the collection of content when it can reasonably be separated from non-content DRAS.

(U) ~~(S)~~ The legislative history is consistent with this understanding. Amicus asserts that "[t]here is no indication in the legislative history that any incidental collection of content was authorized," Amicus Br. 10, and that Congress has "repeatedly amend[ed] the statute to make clear that the government *cannot* collect any content using PR/TT authority," *id.* at 25. These assertions ignore that Congress intended section 3121(c) to "require[] law enforcement to use reasonably available technology to *minimize* information obtained through pen registers." S. Rep. No. 103-402, at 18 (1994) (emphasis added); H.R. Rep. No. 103-827, pt. 1, at 17 (1994) (same). They also ignore the evidence that Congress was aware that pen registers may incidentally collect content. *See, e.g.*, 147 Cong. Rec. S11000 (remarks of Sen. Leahy) (noting that the statute "requires the government to use reasonably available technology" precisely because "pen register devices 'do

capture all electronic impulses . . . including such impulses transmitted after a phone call is connected to the called party'"). There is no inconsistency between Congress' goal to limit targeted collection of content, *see* Amicus Br. 5-10, 25-26, and Congress' intent that the government may accomplish that goal, where no "reasonably available" technology can prevent acquisition of content, by incidentally collecting, and then minimizing, content that is unavoidably obtained.

(U) (S) Amicus' other arguments are equally unavailing. Amicus argues that the government may "use existing technology" to avoid collecting both content and non-content post-cut-through digits. Amicus Br. 27-29. But that argument simply avoids the legal question certified to this Court. The government is authorized to collect non-content post-cut-through digits, and obligated to use "reasonably available" technology to avoid collecting content, rather than forgoing the collection of all post-cut-through DRAS information until technology improves. Amicus raises the specter of broad content collection on the Internet, but only by adopting the premise, without any basis in law or fact, that technology is unavailable to differentiate most content and non-content in that context. *See id.* at 29-31. And amicus claims that all post-cut-through digits, including those that are indisputably DRAS, ought to be considered content, because they are not used by the provider to route a call. *Id.* at 31-34. But those digits are used to route a call

by the calling card company, and the statute asks this Court to determine how they are functionally used, rather than who uses them. *See* [Redacted] *No. PR/TT* [Redacted] 52-53 (FISC 2010) ("dialing, routing, and addressing information are all types of information that, in the context of a communication, particularly relate to the transmission of the communication to its intended party"); *id.* at 34.

(U) **B.** (S) By defining a "pen register" to "have the meaning[] given [that] term[] in section 3127 of Title 18," 50 U.S.C. § 1841(2), Congress intended that the FISA PR/TT provisions be given the comprehensive "meaning" of the term "pen register" in Title 18. Section 3121(c) supplies a portion of the "meaning" of a criminal pen register, because section 3127(3) must be read in light of section 3121(c). *See* Certification 6 n.3 (finding that "there is no indication that Congress, having adopted for purposes of § 1842 the Title 18 definitions of 'pen register' and 'trap and trace device,' nevertheless intended PR/TT devices to operate differently under a § 1842 order"). To determine the "meaning" of "pen register" under the criminal PR/TT statute, in other words, one must look at the statute as a whole, rather than view a single provision's words in isolation.

(U) (S) In arguing to the contrary, amicus notes that FISA does not expressly cross-reference or incorporate section 3121(c). Amicus Br. 17-18. But an express cross-reference is not necessary when the statutory scheme, read in context,

achieves the same result. *See, e.g.*, *Panama R. Co. v. Johnson*, 264 U.S. 375, 391-92 (1924) (reasoning that a "generic reference" to another statute "serves to bring into the latter all that is fairly covered by the reference"); *Director v. Peabody Coal Co.*, 554 F.2d 310 (7th Cir. 1977). Amicus also claims that FISA does not incorporate other parts of the criminal PR/TT statute, such as the procedural aspects of 18 U.S.C. § 3123(a)(3). Amicus Br. 18 n.8; *see* 18 U.S.C. § 3123(a)(3) (establishing procedures for installing a pen register on a "packet-switched data network"). That is true enough, but the FISA PR/TT statute incorporates the "meaning" of, rather than the procedures for obtaining, a criminal "pen register."

~~(S)~~ At any rate, section 3121(c) is important because it reinforces the conclusion that a criminal pen register, as defined in section 3127(3), that targets non-content DRAS may incidentally collect non-DRAS digits that may include content, provided the government uses technology reasonably available to it to avoid collecting content and appropriate minimization techniques to handle any content non-DRAS digits it may unavoidably collect. In its 2015 amendments to FISA, Congress confirmed, by enacting section 1842(h)(2), that using such "minimization" techniques in the PR/TT context is entirely appropriate.

II. (U) The Proper Construction of the Statute Does Not Raise Constitutional Concerns.

~~(U)~~ ~~(S)~~ Amicus concedes that national security is a "special need" of the utmost

importance and that this Court's analysis should therefore be guided by Fourth Amendment reasonableness principles. Amicus Br. 36. But amicus' argument that the government's FISA PR/TT practices are unreasonable is incorrect.

(U) ~~(S)~~ Amicus contends that the acquisition of content post-cut-through digits should not be characterized as "incidental" because the government is "intentionally targeting and collecting" content. Amicus Br. 38-39. That is wrong. The government purposefully targets non-content and acquires content because the technical means to limit collection to non-content alone is not reasonably available. Such collection is properly considered "incidental" because it is the collateral result, given the available technology, of lawful collection. The fact that such collection is an *anticipated* by-product, rather than an unexpected accident, does not undermine the application of the incidental collection principle. *See United States v. McKinnon*, 721 F.2d 19, 22-23 (1st Cir. 1983) ("While an interception that is unanticipated is *a fortiori* incidental, the converse is not true: something does not have to be unanticipated in order to be incidental."); *In re Directives*, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).

(U) ~~(S)~~ Nor is the government's practice unreasonable because some of the content post-cut-through digits may contain personal information. A string of digits, even when it captures personal information, is unlikely to be revealing

without context, and the relevant databases mask those digits until an analyst establishes (by reviewing the pre-cut-through digits) that further examination of the post-cut-through digits is appropriate. Moreover, some of the examples on which amicus relies — such as financial account or social security numbers — involve circumstances where a person's expectation of privacy is diminished because he has transmitted those numbers electronically to a business, which may record the numbers to facilitate a transaction and later disclose those records to the government by subpoena. *See United States v. Miller*, 425 U.S. 435, 443 (1976).

(U) ~~(S)~~ Neither, contrary to amicus' suggestion, is the government's collection of post-cut-through digits unreasonable because the government may have alternative means of obtaining the same information. Amicus speculates about, but does not establish, practical alternatives. And the Supreme Court has "repeatedly refus[ed] to declare that only the 'least intrusive' search practicable can be reasonable." *City of Ontario v. Quon*, 560 U.S. 746, 763 (2010); *Illinois v. Lafayette*, 462 U.S. 640, 647 (1983) (reasonableness "does not necessarily or invariably turn on the existence of alternative 'less intrusive' means").

(U) CONCLUSION

(U) ~~(S)~~ For these reasons and those previously given, this Court should answer the certified question of law in the affirmative.

Respectfully submitted,

JOHN P. CARLIN
Assistant Attorney General for National Security
STUART J. EVANS
J. BRADFORD WIEGMANN
Deputy Assistant Attorneys General

b6, b7C [redacted]

Deputy Chief, Operations Section
Office of Intelligence
b6, b7C [redacted]
Attorney
National Security Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530
b6, b7C [redacted]

Dated: March 31, 2016

(U) CERTIFICATE OF COMPLIANCE

(U) 1. This brief complies with this Court's order dated March 11, 2016, because it is ten pages long, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

(U) 2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14 point font size and Times New Roman type style.

b6, b7C [redacted]

Deputy Chief, Operations Section
Office of Intelligence
National Security Division
U.S. Department of Justice

Dated: March 31, 2016

(U) CERTIFICATE OF SERVICE

(U) Pursuant to Foreign Intelligence Surveillance Court of Review Rules of Procedure 10(b) and 16, on March 31, 2016, I provided two copies of the Reply Brief for the United States in the above-captioned matter to the Litigation Security Group / Security and Emergency Planning Staff, to be made available to:

Marc Zwillinger
ZwillGen PLLC
1900 M Street, NW, Suite 250
Washington, DC 20036
Telephone: (202) 296-3585
Facsimile: (202) 706-5298

b6, b7C [redacted]

Deputy Chief, Operations Section
Office of Intelligence
National Security Division
U.S. Department of Justice

Dated: March 31, 2016