b6 Per FBI
b7C

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//ORCON/NOFORN~~

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

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

(U) (S) IN RE CERTIFIED QUESTION OF LAW

(S) ON CERTIFICATION FROM THE
UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT
DOCKET NUMBER PR/TT 1[redacted] (Hogan, Presiding Judge)

(U) (S) OPENING 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//ORCON/NOFORN~~

~~Classified by:~~ Chief, Operations Section, OI, NSD, DOJ
Derived from: ~~Multiple Sources~~
~~Declassify on:~~ 20410322

(U) TABLE OF CONTENTS

~~Classified by:~~ Chief, Operations Section, OI, ~~NSD, DOJ~~
Derived from: ~~Multiple Sources~~
~~Declassify on:~~ 20410322

(U) TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

(U) GLOSSARY OF ABBREVIATIONS

Communications Assistance for Law Enforcement Act	CALEA
Dialing, Routing, Addressing, or Signaling	DRAS
Domestic Investigations and Operations Guide	DIOG
Electronic Communications Privacy Act of 1986	ECPA
Foreign Intelligence Surveillance Act	FISA
Foreign Intelligence Surveillance Court	FISC
Foreign Intelligence Surveillance Court of Review	FISCR
Pen Register / Trap and Trace	PR/TT
Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015	USA FREEDOM Act
Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001	USA PATRIOT Act

(U) JURISDICTIONAL STATEMENT

(S) The United States Foreign Intelligence Surveillance Court ("FISC") had jurisdiction of the underlying pen register/trap and trace ("PR/TT") application in docket number PR/TT 16[redacted] pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1841-1846. On February 12, 2016, the Honorable Thomas F. Hogan, Presiding Judge of the FISC, certified a question of law to this Court pursuant to 50 U.S.C. § 1803(j). *See* Certification of Question of Law to the Foreign Intelligence Surveillance Court of Review, Docket No. PR/TT 1[redacted] (Feb. 12, 2016) ("Certification"). This Court has jurisdiction over the certified question of law pursuant to 50 U.S.C. § 1803(j).

b1 Per FBI
b3
b7E

(S)

(U) STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

(S) In its entirety, the FISC's certified question of law for review by this Court is as follows:

> 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 [dialing, routing, addressing or signaling (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.

Certification 14.

(U) STATEMENT OF THE CASE

b1 Per FBI
b3
b6
b7C
b7E

~~(S//OC/NF)~~ The certified question of law arises from a FISA pen register (S) application in docket number PR/TT 16[redacted] requesting authorization to use pen register and trap and trace devices targeted at [redacted] (S) *Application for Pen Register and Trap and Trace Device(s)*, Docket No. PR/TT (S) 16[redacted] (FISC filed Jan. 21, 2016) ("Application") (Index of the United States Foreign Intelligence Surveillance Court of Review Record ("FISCR Record"), Tab No. 1). Presiding Judge Hogan approved the pen register and, consistent with the uniform practice of the FISC for at least a decade, authorized the recording and decoding of "post-cut-through digits" — digits entered by a caller after the initial call set-up is completed. He then certified a question of law for this Court to address.

A. (U) Statutory and Legal Framework

(U) 1. *Criminal pen registers.* As part of the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, § 302, 100 Stat. 1848, Congress enacted a provision authorizing the federal government to obtain court orders authorizing a "pen register." As originally enacted, ECPA defined, in relevant part, a "pen register" as "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the

telephone line to which such device is attached." 18 U.S.C. § 3126(3) (1986); *cf. United States v. New York Tel. Co.*, 434 U.S. 159, 161 n.1 (1977) (finding, as understood in 1977, that "[a] pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released" and "does not overhear oral communications and does not indicate whether calls are actually completed"); *United States v. Giordano*, 416 U.S. 505, 549 n.1 (1974) (Powell, J., concurring in part and dissenting in part) (observing that a pen register is "usually installed at a central telephone facility [and] records on a paper tape all numbers dialed from [the] line").

(U) In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279 (1994). That Act added a "limitation" provision to the criminal pen register statute. *See* 18 U.S.C. § 3121(c). As originally enacted, this provision provided that a "government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing." CALEA, § 207, 108 Stat. at 4292.

(U) In 2001, both the definition of "pen register" in section 3127 and the "limitation" provision in section 3121(c) underwent significant amendments in the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), Pub. L. No. 107-56, § 216, 115 Stat. 272, 288, 290. Because section 3127 defined "pen register" in terms of outdated telephone technology (by referring to a "device" "attached" to a "telephone line"), *see, e.g.*, 147 Cong. Rec. S10,999 (daily ed. Oct. 25, 2001) (remarks of Sen. Leahy) ("[t]he language of the existing statute is hopelessly out of date and speaks of a pen register or trap and trace 'device' being 'attached' to a telephone 'line'"), Congress updated this definition in 2001 to define a "pen register" in pertinent part as:

> [A] device or process which records or decodes *dialing, routing, addressing, or signaling* information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . .

18 U.S.C. § 3127(3) (emphasis added); *see also* 18 U.S.C. § 3127(4) (defining "trap and trace device" in pertinent part as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to

identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication").

(U) These changes clarified that the pen register provision applies to an array of modern communications technologies — such as, for example, the Internet — and not simply traditional telephone lines. *See* H.R. Rep. No. 107-236(I), at 52-53 (2001) (discussing predecessor bill H.R. 2975); *see also* 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (section-by-section analysis by Sen. Leahy). The changes authorize the government to collect "dialing, routing, addressing, or signaling information" generally, rather than, as the prior version of section 3127 had provided, "the numbers dialed or otherwise transmitted on the telephone line." At the same time, the changes confirmed that a pen register could not be used to obtain the "contents" of a communication.

(U) In the USA PATRIOT Act, Congress also amended section 3121(c) to conform to the revised language of the pen register definition. The amended (and current) version reads:

> A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law *shall use technology reasonably available to it* that *restricts* the recording or decoding of electronic or other impulses *to the dialing, routing, addressing, and signaling information* utilized in the processing and transmitting of wire or electronic communications *so as not to include the contents of any wire or electronic communications.*

18 U.S.C. § 3121(c) (emphasis added). As with its changes to section 3127, Congress's changes to section 3121(c) clarified that the term "pen register" applies not only to traditional telephone lines, but to all manner of modern electronic communications — and that the purpose of a pen register is to collect "dialing, routing, addressing, and signaling information." At the same time, Congress did not disturb the background principle that the government need only use "technology reasonably available to it" to "restrict[] the recording or decoding" to solely those digits "utilized" in "processing and transmitting" wire or electronic communications.

(U) 2. *FISA pen registers.* In 1978, Congress enacted FISA "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes." S. Rep. No. 95-604, at 7 (1977); *see, e.g.*, 50 U.S.C. §§ 1801 (a)-(c), (e) (defining "foreign power," "agent of a foreign power," "international terrorism," and "foreign intelligence information"). In its original version, FISA did not contain a specific pen register provision, and authority for installation or use of a pen register or trap and trace device for foreign intelligence purposes would have been sought pursuant to subchapter I (electronic surveillance) of FISA.

(U) In 1998, however, Congress added subchapter III to FISA to specifically authorize and regulate the use of pen registers and trap and trace

devices for foreign intelligence and international terrorism investigations. *See* Intelligence Authorization Act of 1999, Pub. L. No. 105-272, Title VI, § 601(2), 112 Stat. 2396, 2404 (1998). From the start, the statute defined "pen register" to "have the meaning[] given [that] term[] in section 3127 of Title 18," the criminal analog to FISA's pen register provision. 50 U.S.C. § 1841(2). By giving a PR/TT obtained under FISA the "meaning" of a PR/TT obtained under Title 18, section 1841(2) also incorporates the gloss on the meaning of a PR/TT supplied by section 3121(c). *See* Certication 6 n.3 (noting 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 than under an order issued under 18 U.S.C. § 3123").

(U) Subsequently, in 2006, Congress clarified that the government may use a FISA pen register to obtain "the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including *any* temporarily assigned network address *or associated routing or transmission information.*" 50 U.S.C. § 1842(d)(2)(C)(i)(III) (emphasis added); *see id.* § 1842(d)(2)(C)(ii)(III) (requiring disclosure of the same "routing or transmission information" for the customer or subscriber of incoming and outgoing communications to or from the service covered by the order); *see also* USA

PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 128, 120 Stat. 192, 228-29 (2006). In doing so, Congress augmented the government's abilities by "authoriz[ing] the FISC to issue FISA pen register/trap and trace orders that also provide the Government . . . certain limited subscriber information associated with *routing* information captured by the surveillance devices." S. Rep. No. 109-85, at 25 (2005) (emphasis added).

(U) To obtain a FISA pen register order, the government must (in relevant part) "make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1842(a)(1); *cf. id.* § 1843 (setting forth alternative procedures for obtaining authorization during emergencies). A FISA pen register application must be made to a judge of the FISC or an appropriately designated magistrate judge. *See* 50 U.S.C. §§ 1842(b)(1)-(2). Upon receiving an application, the judge "shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements" of section 1842. 50 U.S.C. § 1842(d)(1). For pen registers in investigations to protect against

international terrorism or clandestine intelligence activities, the judge "shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days." 50 U.S.C. § 1842(e)(1); *see also id.* § 1842(e)(2) (authorizing a period not to exceed one year if the information likely to be obtained is foreign intelligence information not concerning a United States person).

(U) The Act specifies limitations on how information properly acquired from a FISA pen register may be used. *See* 50 U.S.C. § 1845(a)(1). Information may not be used or disclosed "except for lawful purposes," 50 U.S.C. § 1845(a)(2), and may be used in a criminal proceeding only "with the advance authorization of the Attorney General," 50 U.S.C. § 1845(b). When the United States "intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States" any FISA pen register information, it must notify "the aggrieved person and the court or other authority in which the information is to be disclosed or used." 50 U.S.C. § 1845(c); *see also id.* § 1845(d) (similar for State use or disclosure); *id.* § 1841(3) (defining "aggrieved person" for pen register provision). The Act also permits any "aggrieved person against whom" FISA pen register information is used to "move to suppress" such evidence, 50 U.S.C. § 1845(e)(1), and directs the district court to suppress such

evidence if it finds that the surveillance "was not lawfully authorized or conducted," 50 U.S.C. § 1845(g)(1).

(U) The statute establishes a robust scheme of congressional oversight. Specifically, on a semiannual basis, the Attorney General must inform the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of both chambers of Congress, "concerning all uses of pen registers and trap and trace devices" under section 1842. 50 U.S.C. § 1846(a); *see also id.* § 1846(b) (requiring a report setting forth, among other things, the number of FISA PR/TT applications during the reporting period and the FISC's resolution of such applications).

~~(U)~~ (S) These provisions supplement FISA's general requirement that the Executive Branch inform Congress about any "significant legal interpretations" of FISA, "including interpretations or pleadings filed with" the FISC. 50 U.S.C. § 1871(a)(4). Pursuant to this provision, in June 2010 and August 2010, the government produced to the Judiciary Committees of both chambers of Congress, the Senate Select Committee on Intelligence, and the House Permanent Select Committee on Intelligence three significant 2006 pleadings and a 2009 pleading filed with the FISC that describe the government's collection of post-cut-

through digits pursuant to FISA pen register authority and explain why obtaining post-cut-through digits using a FISA pen register is lawful. Br. in Resp. to the Court's Oct. 29, 2015 Supplemental Order, Docket No. PR/TT 15-78, at 2-3 nn.1 & 2 (FISC filed Jan. 15, 2016) (FISCR Record, Tab No. 2); United States of America Verified Memorandum of Law in Response to the Court's June 18, 2009 Supplemental Order, Docket Nos. PR/TT 09-36, 09-37, and 09-38 (FISC filed Aug. 17, 2009) (with attached exhibits A-F) ("2009 Memorandum") (FISCR Record, Tab No. 4).

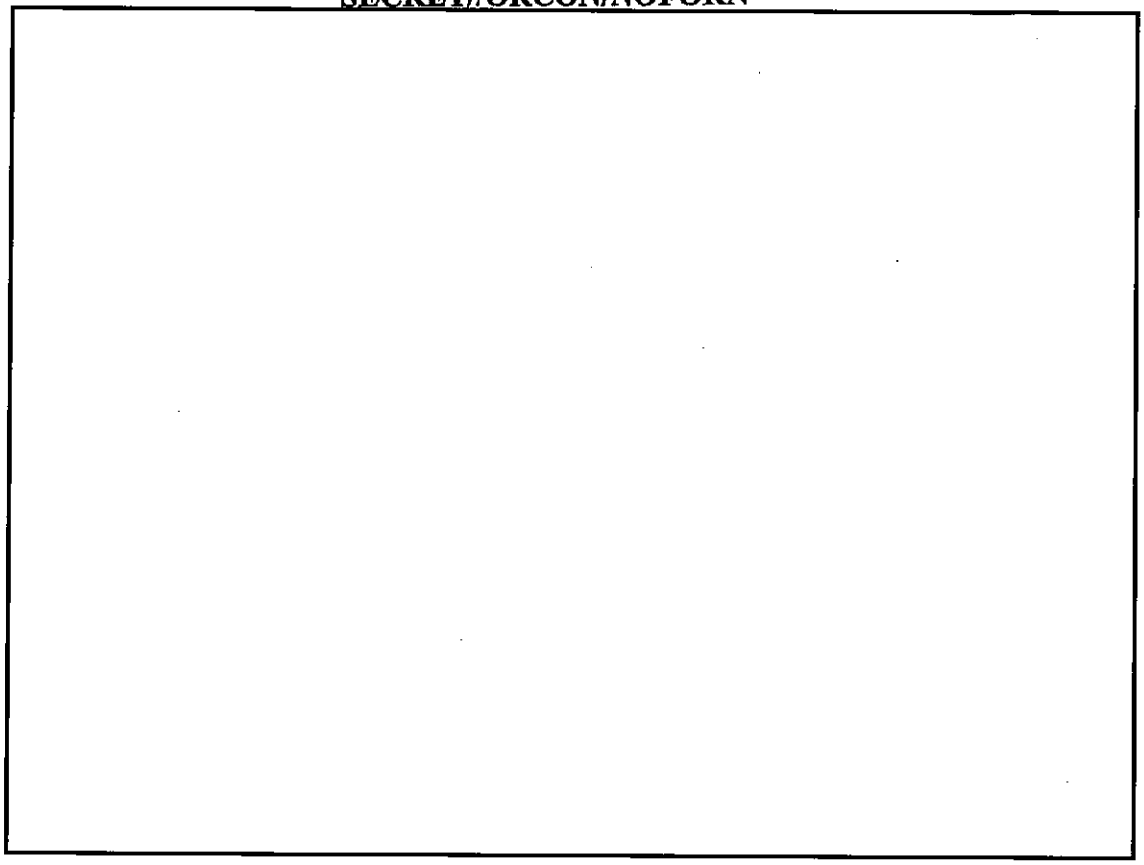
(U) Lastly, recent amendments have specifically codified the concept of minimization in the FISA pen register provision. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. No. 114-23, § 2, 129 Stat. 268 ("USA FREEDOM Act"). Those amendments added a section on privacy procedures that specifically states that the FISC or the Attorney General may "impose additional privacy or minimization procedures with regard to the installation or use of a pen register or trap and trace device." USA FREEDOM Act § 202, 129 Stat. at 278 (codified at 50 U.S.C. § 1842(h)(2)).

(U) 3. *Post-cut-through digits.* "Post-cut-through digits" is a term of art that refers to digits entered by a caller after the initial call set-up is completed or

"cut-through." Some post-cut-through digits are non-content call identifying information (dialing, routing, addressing, or signaling ("DRAS") information), such as when a caller dials a toll free number to connect to a service provider (*e.g.*, 1-800-CALLATT), then after the initial call is connected to the service provider, ultimately enters another phone number, which is in fact the ultimate call destination. *See* Certification 3; Application 22-24 (FISCR Record, Tab No. 1). Other post-cut-through digits may constitute content, such as when a caller phones and is connected to an automated system, such as a financial institution or pharmacy, and, in response to prompts, enters digits that signify transferring funds from one account number to another or a prescription number. Certification 3. In either case, the digits are sequences of numbers. *See generally U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 462 (D.C. Cir. 2000).

[redacted]

b3 Per FBI
b7E Per FBI



b3 Per FBI
b7E

(U) (S) In addition to the foregoing, two facts about the collection of post-cut-through digits are relevant to this case. First, as the government has explained to the FISC, and as the certified question of law presented to this Court acknowledges, there is "no reasonably available technology to distinguish non-content pen register data from content." Submission Regarding Post-Cut-Through Digits, Docket No. PR/TT 15-53, at 20 (FISC filed Oct. 1, 2015) ("2015 Submission"); *see also* Supplemental Order, Docket No. PR/TT 15-53 (FISC July 8, 2015) (Eagan, J.) (directing the government to brief this issue); Supplemental

Order, Docket Nos. PR/TT 09-36, 09-37, 09-38 (FISC June 18, 2009) (Hogan, J.)

(similar). [redacted] b3 Per FBI b7E

[redacted]

(U) [redacted]

b3 Per FBI
b7E

(U)

[redacted]

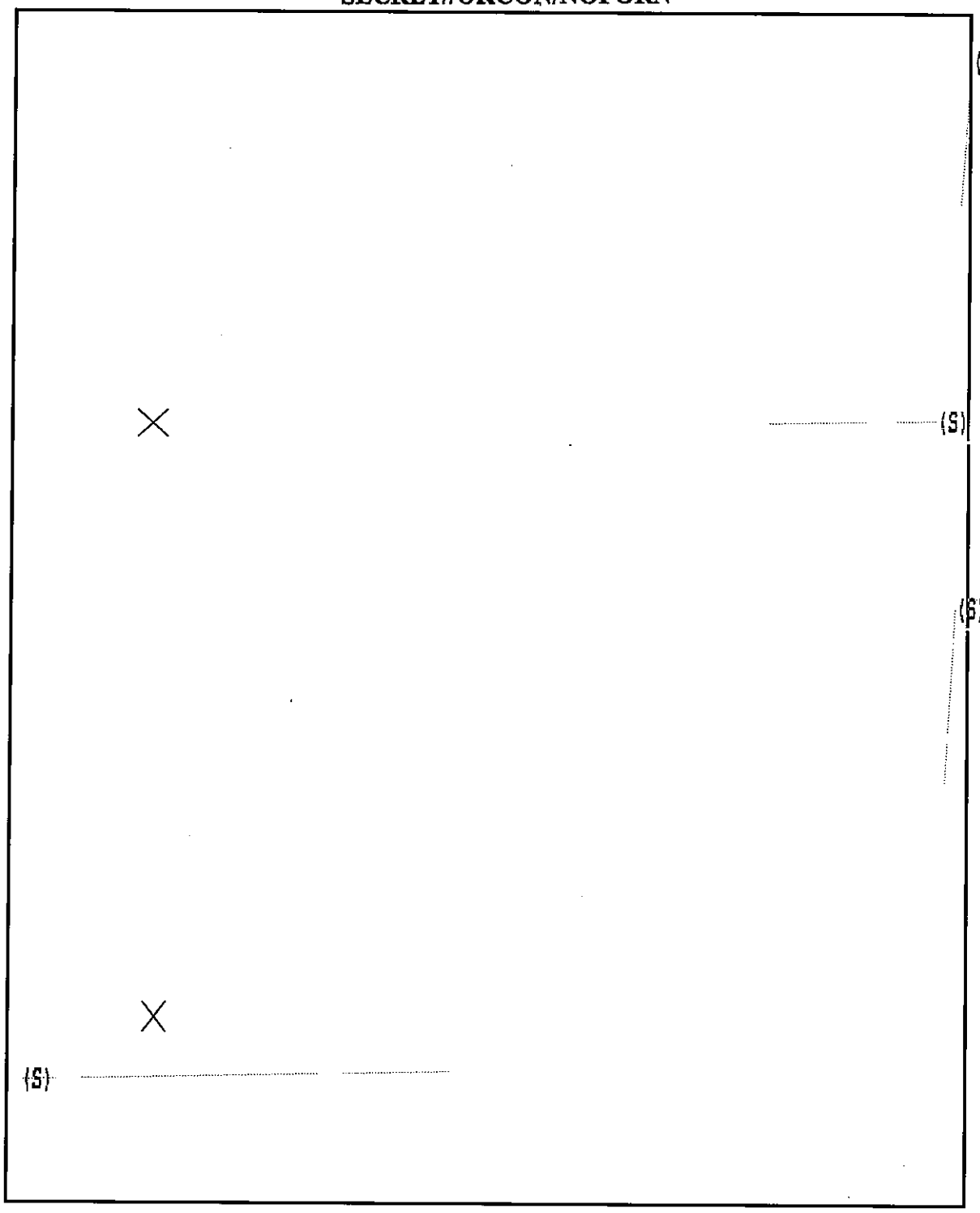
b3 Per FBI
b7E

B. (U) Factual Background

(S) ~~(S//OC/NF)~~ 1. [redacted] On January 21, 2016, the government requested renewal of FISA PR/TT orders relating to [redacted] (S) [redacted] (S) who is also a United States person within the meaning of FISA. [redacted]

b1 Per FBI
b3
b6
b7C
b7E

[redacted] (S)



b1 Per FBI
b3
b6
b7C
b7E

[redacted]

b3 Per FBI
b7E

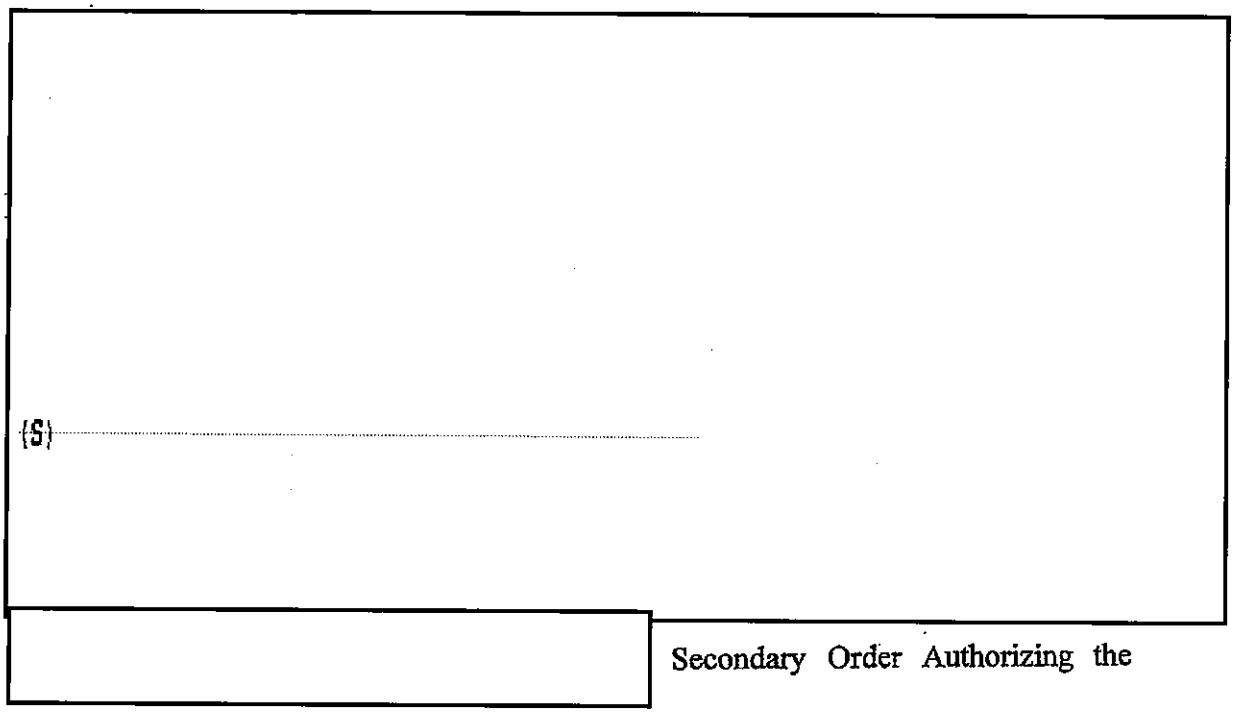
C. (U) Procedural History

~~(S//OC/NF)~~ 1. *The FISC approves the Application.* On January 21, 2016, the FISC approved the Application, finding that it conformed to FISA's requirements. *See* Primary Order for Pen Register and Trap and Trace Device(s) (S) ("Primary Order"), Docket No. PR/TT 16[redacted] at 1-2 (FISC Jan. 21, 2016) (FISCR Record, Tab No. 1). The Primary Order authorizes the installation and use of PR/TT devices [redacted] (S)

b1 Per FBI
b3
b7E

[redacted] (S)

[redacted]



b1 Per FBI
b3
b7E

(S)

Secondary Order Authorizing the Installation and Use of Pen Register and Trap and Trace Device(s) ("Secondary Order"), Docket No. PR/TT 16 at 2-3 (FISC Jan. 21, 2016) (FISCR Record, Tab No. 1).

(U) ~~(S)~~ The Primary and Secondary Orders expire on April 19, 2016. Primary Order 7; Secondary Order 5.

(U) ~~(S//OC/NF)~~ 2. *The FISC certifies a question of law to this Court.* On February 12, 2016, the FISC issued a "certification of question of law" to this Court pursuant to 50 U.S.C. § 1803(j). The FISC noted in its Certification that its approval of the government's application "was consistent with prior FISC practice," and that, since (at least) 2006, FISC judges have issued PR/TT orders

under 50 U.S.C. § 1842 authorizing, at the government's request, acquisition of all post-cut-through digits while prohibiting the use of content post-cut-through digits unless additional authorization is obtained from the FISC. Certification 2. Although "[t]o date, FISC judges have been uniform in their handling of the principal issues presented by post-cut-through digits" and have authorized their acquisition, the Certification noted that some FISC judges have recently expressed "concerns" about continuing to authorize the acquisition of post-cut-through digits under FISA PR/TT orders. *Id.* at 13. The Certification cited two federal district court and four magistrate judge decisions from the 2006 to 2008 timeframe that denied government requests, in the criminal context, to acquire post-cut-through digits in applications for the installation and use of PR/TT devices. Certification 9-11 & n.4, 13.

(U) (S) The FISC Certification stated that in authorizing the collection of all post-cut-through digits pursuant to FISA PR/TT orders, with a prohibition on the use of post-cut-through digits constituting content, the FISC judges "have accepted the Government's principal statutory argument, which hinges on 18 U.S.C. § 3121(c)." Certification 6. As the FISC's certified question of law acknowledges, there is no "technology reasonably available" to the government under section 3121(c) that would permit a PR/TT device at the time of acquisition

to distinguish between non-content post-cut-through digits that are DRAS information used in processing a phone call (*e.g.*, digits dialed after connection to a service provider) from post-cut-through digits that may be content unrelated to processing a call (*e.g.*, bank account information), nor is there reasonably available technology that at acquisition, without further analysis, could discard the digits that constitute content and retain only the non-content DRAS information. Certification 6-7. On the reading proposed by the government and accepted by the FISC judges, "Section 3121(c) permits the Government to obtain all post-cut-through digits in the absence of such reasonably available technology," at least when use of content post-cut-through digits is prohibited without further authorization from the FISC. *Id.* at 7.

~~(U)~~ ~~(S//OC/NF)~~ 3. *This Court appoints an* amicus curiae. On February 17, 2016, this Court issued an order appointing an *amicus curiae* pursuant to 50 U.S.C. § 1803(i)(1) and establishing a briefing schedule in this matter. *See* Order Appointing an *Amicus Curiae* and Briefing Order (Feb. 17, 2016).

(U) SUMMARY OF THE ARGUMENT

(U) (S) The acquisition of all post-cut-through digits — accompanied by a prohibition on the use of all content post-cut-through digits — is authorized by the relevant statutory provisions and is consistent with constitutional requirements. This Court should affirm the FISC's longstanding practice of authorizing government collection of post-cut-through digits under FISA's pen register provisions.

(U) (S) I. The relevant FISA (and criminal) provisions authorize the collection of "dialing, routing, addressing, or signaling information" through a pen register, whether such information is collected pre- or post-cut-through. 18 U.S.C. § 3127(3). Non-content post-cut-through digits — for example, telephone numbers that happen to be dialed after a call is connected — are information of this nature, because they are conveyed to a third party in order to effectuate "dialing, routing, addressing, or signaling."

(U) (S) In collecting non-content post-cut-through digits authorized by the pen register statute, the government must use "technology reasonably available to it" to avoid the collection of the "contents" of a telephone call. 18 U.S.C. § 3121(c). As explained at length in the FISC, and as reflected in the certified question, there is no technology reasonably available to the government that permits the collection of

only non-content post-cut-through digits. [redacted] b3 Per FBI b7E

[redacted]

[redacted] The FISC has approved the collection of post-cut-through digits on this basis for nearly a decade, consistent with the plain text of section 3121(c), with the statute's drafting and legislative history, and with government practice under comparable statutory provisions that authorize the use of minimization techniques in the national-security and criminal contexts.

(U) (S) The contrary district court and magistrate judge decisions noted in the FISC Certification, Certification 9-11 & n.4, which denied requests for the collection of post-cut-through digits in the context of criminal pen register applications, do not provide a basis for denying the collection of post-cut-through digits under FISA pen register orders. Those decisions, which come from only three judicial districts, are not binding on this Court, fail to harmonize all of the statutory language, and do not take into account the FISA authorities and practice applicable here.

(U) (S) II. The government's collection of post-cut-through digits under FISA's pen register provision also complies with the Fourth Amendment. Accordingly,

there is no basis for construing any portion of the statutory scheme contrary to its plain language.

(U) (S) The collection of non-content post-cut-through digits is not a "search" within the meaning of the Fourth Amendment. Under *Smith v. Maryland*, 442 U.S. 735 (1979), the collection of telephone numbers using a pen register is not a Fourth Amendment search. There is no basis for drawing an artificial distinction between telephone numbers collected pre- and post-cut-through in this context.

(U) (S) As for any content post-cut-through digits that may be incidentally collected and then minimized in connection with FISC-authorized pen registers, the ultimate Fourth Amendment test is reasonableness. The scheme adopted by Congress in the pen register definition and in section 3121(c), which allows the incidental collection of content post-cut-through digits to the extent that no filtering technology is reasonably available to the government, is reasonable under the Fourth Amendment, particularly in the FISA context, because the balance of harms and benefits weighs decisively in favor of collection.

(U) (S) Here, the intrusion into privacy — recording and decoding the digits dialed into a targeted telephone after the initial call is "cut through" — is slight, especially in light of the extensive policy and technological restrictions on government agents seeking access to post-cut-through digits. On the other hand,

the government's interest in collecting post-cut-through digits that may contain DRAS is great. Targets of FISA pen registers are subjects of national security investigations, and "the interest in national security . . . is of the highest order of magnitude." *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). [redacted] b3 Per FBI b7E

[redacted]

[redacted] As this Court has found, "[i]f the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions." *Id.*

(U) STANDARD OF REVIEW

(U) (S) The question of law before this Court was certified by the FISC pursuant to 50 U.S.C. § 1803(j) as a question that warrants review because of a need for uniformity or because consideration by this Court would serve the interests of justice. Upon certification of a question of law under 50 U.S.C. § 1803(j), this Court "may give binding instructions or require the entire record to be sent up for decision of the entire matter in controversy." 50 U.S.C. § 1803(j). This Court reviews questions of law de novo. *In re Directives*, 551 F.3d at 1009.

(U) ARGUMENT

(U) (S) The FISC's longstanding, uniform practice of authorizing the recording and decoding of post-cut-through digits pursuant to FISA pen register orders, with a prohibition on the use of any such digits that constitute content, is lawful and should continue. The acquisition of post-cut-through digits in this context is authorized by the applicable statutory provisions and is consistent with the Fourth Amendment.

I. (U) (S) Under the Plain Language of the Pen Register Statute, the Government Has the Authority To Collect All Post-Cut-Through Digits.

(U) (S) The relevant FISA (and criminal) provisions authorize the collection of "dialing, routing, addressing, or signaling" information through a pen register, and those provisions make no distinction between collecting such information pre- or post-cut-through. 18 U.S.C. § 3127(3). [redacted] b3 Per FBI b7E

[redacted]

[redacted] Under the relevant statutory provisions, the government shall accomplish collection using "technology reasonably available to it" to avoid the collection of the contents of a telephone call. 18 U.S.C. § 3121(c). As the government explained at length in the FISC, and as the question certified to this

Court acknowledges, there is no technology reasonably available to the government that permits the collection of only non-content post-cut-through digits. Under current technology reasonably available to the government, the government must collect all post-cut-through digits to obtain the DRAS information authorized by the statute. The government then uses strict technological and policy measures to prevent the use of any content post-cut-through digits incidentally collected. *See* 2015 Submission (FISCR Record, Tab No. 3). As the FISC has long recognized, such collection is consistent with the plain meaning of the pen register statute.

(U) A. (S) The Government May Collect Non-Content Post-Cut-Through Digits Because They Are "Dialing, Routing, Addressing, or Signaling Information" under the Pen Register Statute.

(U) The statutory definition of a "pen register," as incorporated into FISA at 50 U.S.C. § 1841(2), refers to

> a device or process which records or decodes *dialing, routing, addressing, or signaling* information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . . .

18 U.S.C. § 3127(3) (emphasis added). The statute, accordingly, authorizes the recording or decoding of "*dialing, routing, addressing, or signaling* information," but not "the contents of any communication." On its face, the provision draws a

distinction between non-content "dialing, routing, addressing, or signaling" information and the "contents" of a communication.

(U) [redacted] b3 Per FBI b7E

[redacted] Section 3127(1) adopts the definition of "contents" contained in 18 U.S.C. § 2510(8), which defines the term as "any information concerning the substance, purport, or meaning" of a "wire, oral, or electronic communication." Under these definitions, post-cut-through dialed telephone numbers clearly constitute non-content "*dialing, routing, addressing, or signaling* information" rather than "information concerning the substance, purport, or meaning" of a communication.

(U) Section 3127 makes no mention of the concept of "cut-through" at all. That is not accidental. As discussed above, in amending section 3127(3) in the USA PATRIOT Act, Congress intended to authorize the government to obtain, through a pen register device, all non-content information — "dialing, routing, addressing, or signaling information" — for new and modern technology, not merely for telephone calls. Reading a "pre-cut-through" requirement into section 3127 would revert the provision back to its pre-modern status. Congress's broad

authorization of the collection of "dialing, routing, addressing, or signaling" information through pen registers includes the collection of dialed phone numbers, whether collected "pre-" or "post-cut-through." *See In re Commc'ns Assistance for Law Enforcement Act*, 17 F.C.C.R. 6896, 6925 (F.C.C. Apr. 11, 2002) (reasoning that many post-cut-through digits "simply route the call to the intended party and are, therefore, unquestionably call-identifying information even under a narrow interpretation of that term"); [Redacted] *No. PR/TT* [Redacted] 33 (FISC 2010) ("*some* digits dialed after a call has been connected, or 'cut through,' can constitute 'contents' . . . . Courts accordingly have described post-cut-through digits as dialing information, *some* of which also constitutes contents") (emphasis added) ("*2010 FISC Opinion*"), *available at* http:www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf; *cf. In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 137-38 (3d Cir. 2015).

(U) (S) The 2006 amendment to the FISA pen register provision bolsters this conclusion. That amendment specifies that the government may obtain "the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including *any* temporarily assigned network address *or associated routing or transmission information.*" 50 U.S.C. § 1842(d)(2)(C)(i)(III) (emphasis added); *see also id.* § 1842(d)(2)(C)(ii)(III). Congress's purpose in

enacting this provision was to "authorize[] the FISC to issue FISA pen register/trap and trace orders that also provide the Government . . . certain limited subscriber information associated with *routing* information captured by the surveillance devices." S. Rep. No. 109-85, at 25 (emphasis added).

b1 Per FBI
b3
b7E

(S)

(S)

(U) [redacted]

b1 Per FBI
b3
b7E

(U) **B. (S) The Government May Collect Content Post-Cut-Through Digits Incidental to the Collection of DRAS.**

(U) 1. *Statutory text.* Pursuant to section 3121(c):

> A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law *shall use technology reasonably available to it* that *restricts* the recording or decoding of electronic or other impulses *to the dialing, routing, addressing, and signaling information* utilized in the processing and transmitting of wire or electronic communications *so as not to include the contents of any wire or electronic communications.*

18 U.S.C. § 3121(c). Accordingly, the pen register statute authorizes the government to "use technology reasonably available to it" to collect "dialing, routing, addressing, and signaling information" and to avoid collecting the "contents" of communications. By its terms, section 3121(c) recognizes the potential for pen register devices to collect "content," and the statute requires the government to use "technology reasonably available" to it to mitigate that possibility, rather than requiring the government to avoid the possibility altogether. Section 3121(c)'s text, in other words, recognizes the likelihood that "dialing, routing, addressing, and signaling information" and "contents" may be

intermingled — requiring the government to use "technology reasonably available" to address the issue, rather than prohibiting the collection of content altogether. Section 3121(c) thus balances the government's need for non-content post-cut-through digits with the possibility that content post-cut-through digits will be collected incidentally.

(U) (S) As a matter of plain statutory text, any reading that absolutely prohibits the government from collecting post-cut-through digits that may later be determined to include "content" would render Congress's use of the "technology reasonably available" language superfluous. Such a reading would violate the bedrock rule of statutory construction that all words of a statute must, if possible, be given meaning. *See, e.g., TRW, Inc. v. Andrews*, 534 U.S. 19, 31 (2001) ("It is a cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant."); *King v. St. Vincent's Hosp.*, 502 U.S. 215, 221 (1991) (referring to the "cardinal rule that a statute is to be read as a whole since the meaning of the statutory language, plain or not, depends on context") (citation omitted).

(U) 2. *Comparable provisions.* This interpretation of section 3121(c) is consistent with how Congress has approached similar problems in other statutory

provisions. For example, under well-established precedents, the criminal wiretap provisions do "not forbid the interception of all nonrelevant conversations, but rather instruct[] the [government] to conduct the surveillance in such a manner as to minimize the interception of such conversations." *Scott v. United States*, 436 U.S. 128, 140 (1978) (emphasis omitted). Thus, 18 U.S.C. § 2518(5) requires that electronic surveillance "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception."

(U) Similarly, for example, each application for electronic surveillance submitted by the government under Title I of FISA must contain a statement of the government's proposed minimization procedures. 50 U.S.C. § 1804(a)(4). FISA defines "minimization procedures," in pertinent part, as "specific procedures . . . that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1801(h)(1). FISA's minimization procedures take into account the realities of foreign intelligence collection, where the activities of individuals engaged in clandestine intelligence activities or international terrorism are often not obvious

on their face, and investigations often develop over long periods of time. *See, e.g.*, *United States v. Rahman*, 861 F. Supp. 247, 253 (S.D.N.Y. 1994) (rejecting the notion that the "wheat" could be separated from the "chaff" while the "stalks were still growing"), *aff'd on other grounds*, 189 F.3d 88 (2d Cir. 1999); S. Rep. No. 95-701, at 40 (1978) ("[P]rimarily for technological reasons, it may not be possible to avoid acquiring all conversations. In these situations, minimizing retention and dissemination becomes most important.").

(U) (S) In using the "technology reasonably available" language in section 3121(c), Congress incorporated a similar principle. Congress made clear its intent that the government may incidentally acquire information that may fall outside the scope of a pen register (*i.e.*, content), when such recording or decoding is a necessary incident of capturing call processing information, because the government lacks "reasonably available technology" to avoid the collection of content post-cut-through digits. Minimization of this non-pen-register information, once it is identified after acquisition, is consistent with other FISA authorities. *See* 50 U.S.C. § 1842(h)(2) (authorizing 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"); *see also id.* §§ 1801(h), 1805(c)(2)(A), 1821(4), 1824(c)(2)(A), 1861(c)(1).

(U) 3. *Legislative history*. The legislative history of section 3121(c) points in the same direction. Committee reports from both the House of Representatives and the Senate confirm that Congress intended to permit the government to incidentally record and decode post-cut-through digits that may turn out to be content. Both reports state that section 3121(c) is intended to "require[] law enforcement to use reasonably available technology to *minimize* information obtained through pen registers." *See* S. Rep. No. 103-402, at 18 (1994) (emphasis added); H.R. Rep. No. 103-827, pt. 1, at 17 (1994) (same). Before the enactment of section 3121(c) in 1994, the term "minimize" had acquired specific legal meaning under the electronic surveillance laws of both Title III of the Omnibus Crime Control and Safe Streets Act, enacted in 1968, and FISA, enacted in 1978.

(U) In addition, Senator Leahy, the primary architect of section 3121(c), characterized the provision as requiring "government agencies installing and using pen register devices to use, *when reasonably available*, technology that restricts the information captured by such device to the dialing or signaling information necessary to direct or process a call, excluding any further communications conducted through the use of dialed digits that *would otherwise be captured*." 140 Cong. Rec. S11,062 (daily ed. Aug. 9, 1994) (emphasis added). Senator Leahy thus indicated that the government was required to apply filtering technology to

avoid acquiring content *only when* such technology is reasonably available. And both the Senate and the House of Representatives committee reports accompanying CALEA adopted Senator Leahy's remarks verbatim. *See* S. Rep. No. 103-402, at 31; H.R. Rep. No. 103-827, pt. 1, at 32.

(U) (S) In short, Congress deliberately chose to make the reasonable availability of filtering technology the cornerstone of section 3121(c), knowing that the existence of such technology was by no means assured. As long as filtering technology to distinguish content and non-content post-cut-through digits is not reasonably available, Congress authorized the government to record and to decode all post-cut-through digits, including incidentally recording and decoding content post-cut-through digits, subject to appropriate minimization procedures.

(U) C. (S) Contrary District Court and Magistrate Judge Decisions in Criminal Cases Are Neither Binding Nor Persuasive.

(U) (S) In its Certification, the FISC noted that, although all FISC judges to rule on the issue since 2006 have uniformly and consistently authorized acquisition of post-cut-through digits pursuant to FISA pen register orders, resolution of the issue before this Court was warranted. Between 2006 and 2008, two district judges and four magistrate judges in three districts denied requests to acquire such information in the context of criminal pen registers. Certification 9-11 & n.4.

(U) (S) Those district court and magistrate judge decisions, of course, are not

binding on this Court. Indeed, judges in other districts have continued to authorize the acquisition of post-cut-through digits in criminal pen register orders, albeit in unpublished orders that are typically filed under seal. *See, e.g.*, Order, *In re Application of the United States*, Misc. No. 3:15-mc (W.D.N.C. Nov. 30, 2014) (unsealed on Mar. 21, 2016) (attached as Exhibit A). Although it is not clear whether the judges in these cases specifically considered the legality of collecting post-cut-through digits by PR/TT, it is clear that the FISC is not the only court to have authorized such collection. *Compare* Certification 10 (suggesting that "the FISC may be the only court to have" authorized collection of post-cut-through digits under a PR/TT order).

(U) In any event, the district and magistrate judge decisions denying authority to collect post-cut-through digits were incorrectly reasoned and decided. They rest, as explained below, on four significant flaws.

(U) *First*, none of the decisions analyzes the text of section 3127(3) to determine whether non-content post-cut-through digits — such as telephone numbers dialed after "cut-through" to a calling card number — are "dialing, routing, addressing, or signaling information." 18 U.S.C. § 3127(3). That omission is a serious one: If non-content post-cut-through digits are in fact DRAS under section 3127(3), then it follows from the definition included in the criminal

and FISA pen register statutes that the government is *expressly* authorized to collect such digits. The decisions, however, do not grapple with this threshold, yet important, point. *See 2010 FISC Opinion* 53 ("there is no reason to think Congress intended to compel an agency deploying a PR/TT device to try to avoid acquiring data that would constitute DRAS information under the definitions of 'pen register' and 'trap and trace device'").

(U) *Second*, the decisions incorrectly analyze the pen register statute's prohibition on collecting "the contents of any communication," 18 U.S.C. § 3127(3), and the import of section 3121(c). Thus, for example, the sole published district court decision rests its analysis in large part on the repeated claim that the pen register statute "contains an express and clear statement that information collected by a pen register 'shall not include the contents of any communication.'" *In re Application of the United States*, 622 F. Supp. 2d 411, 421 (S.D. Tex. 2007) (quoting 18 U.S.C. § 3127(3)); *see also id.* ("The prohibition on the collection of content is clear."); *id.* at 422 (statute "contains an affirmative obligation *not* to collect content in the first place"); *id.* ("Under the clear language of the statute, the Government is precluded from collecting content at all, even if it would be prevented from obtaining some non-content that would otherwise be authorized."); *id.* ("The Pen Register Statute expressly prohibits the collection of

content."). The only other district court decision to have addressed this issue, as well as the four relevant magistrate judge decisions, also rest in principal part on this theory. *See In re Application of the United States*, No. 6:06-mj-1130, slip op. at *5 (M.D. Fla. June 20, 2006) (finding that the "statute seems plain . . . that information intercepted by pen registers and trap/trace devices 'shall not include the contents of any communication'" and referring to the "clear prohibition on the interception of content") (FISCR Record, Tab No. 4, Exhibit F), *aff'g*, No. 6:06-mj-1130 (M.D. Fla. May 23, 2006) (opinion of magistrate judge) (FISCR Record, Tab No. 4, Exhibit E); *In re Application of the United States*, No. 08-MC-595(JO), 2008 WL 5255815 (E.D.N.Y. Dec. 16, 2008) (opinion of magistrate judge); *In re Applications of the United States*, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (opinion of magistrate judge), *summarily aff'd*, Nos. 06-mc-547, 06-mc-561, 07-mc-120, 07-mc-400 (E.D.N.Y. Dec. 17, 2007); *In re Application of the United States*, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (opinion of magistrate judge).

(U) These claims about the plain language of section 3127(3) are correct in a limited sense, but they are incorrect in a more relevant sense. Section 3127(3) prohibits the *targeted* collection of the "contents of any communication." That prohibition on *targeted* collection, however, says nothing about the lawfulness of *incidental* collection of such "contents" during the *targeted* collection of non-

content DRAS. The way to harmonize the "no content" prohibition and the "reasonably available technology" permission, taken together, is to understand that the statute prohibits targeted collection of "content" but permits incidental collection of "content" when the government collects DRAS information.

(U) In interpreting section 3121(c) differently, the judges in these cases recognized that they were creating a problematic construction. Thus, for example, the district judge in the Southern District of Texas remarked that there is a "contradiction inherent in the [pen-register] statute." *Application of the United States*, 622 F. Supp. 2d at 420. That "contradiction," in the court's view, gives rise to a strange situation where the statute provides that "once the Government obtains authorization to use a pen register (which, by definition, cannot be used to collect contents), it must use all reasonably available technology to prevent collection of content." *Id.* at 421. Likewise, a magistrate judge in the Eastern District of New York claimed that "a contradiction arises: if no content can be collected, then what is the purpose of the reasonably available technology requirement?" and worried that section 3121(c) "is superfluous if the ban on content acquisition is absolute." *In re Applications of the United States*, 515 F. Supp. 2d at 332, 335.

~~(U)~~ ~~(S)~~ But the notion that there is a "contradiction" in the pen-register statute is mistaken. If the statute is interpreted consistent with other comparable provisions,

the prohibition on collection of "contents" applies only to targeted collection of contents rather than incidental collection. An effort to harmonize these two statutory provisions leads to the conclusion that content post-cut-through digits may be incidentally collected, subject to appropriate minimization.

(U) *Third*, the opinions either fail to recognize the significant parallels between section 3121(c) and the other provisions that authorize collection subject to minimization procedures, or they draw the wrong inference from those parallels. In *Application of the United States*, for example, the district court placed significant weight on the fact that section 3121(c) does not expressly use the terms "minimize" or "minimization." 622 F. Supp. 2d at 422. Comparing the pen register statute with the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, the court observed that the Wiretap Act "allows the Government to intercept both relevant and irrelevant communications but requires that irrelevant communications be minimized." 622 F. Supp. 2d at 422; *see* 18 U.S.C. § 2518(5); *Scott v. United States*, 436 U.S. 128, 140 (1978) ("The [wiretap] statute does not forbid the interception of all nonrelevant conversations, but rather instructs the agents to conduct the surveillance in such a manner as to 'minimize' the interception of such conversations."). But the court then concluded that the pen register statute was different because it "does not contain an obligation to minimize the collection of

the content of communications." 622 F. Supp. 2d at 422.

(U) This analysis fails to acknowledge that Congress *did* invoke the concept of "minimization" when it enacted section 3121(c), as is clear from the relevant legislative history. *See* S. Rep. No. 103-402, at 18 (describing section 3121(c) as requiring "law enforcement to use reasonably available technology to *minimize* information obtained through pen registers") (emphasis added); H.R. Rep. No. 103-827, pt. 1, at 17 (same). In any event, there is no requirement that Congress use a particular talismanic term — "minimization" — rather than a different term to express the same concept, namely, "technology reasonably available." A court's contrary analysis elevates terminology over substance. Moreover, the FISA pen register provision has been recently amended to refer expressly to the use of "minimization procedures." *See* 50 U.S.C. § 1842(h)(2).

(U) *Fourth*, some of the decisions appear to take issue with the concept of minimization procedures altogether. For example, the district judge in the Middle District of Florida found that section 3127(3) precludes collection of post-cut-through digits because "the determination of whether post-cut-through digits represent signaling information or communication cannot be made until the data is analyzed, post-interception," thereby making it "impossible to ascertain in advance whether any particular post-cut-through digits represent communications content."

post-cut-through digits, *see Application of the United States*, 441 F. Supp. 2d at 837; *Applications of the United States*, 515 F. Supp. 2d at 335, 339, those concerns are misguided. The statutory scheme, as described above, is clear and does not give rise to an ambiguity that warrants application of the canon of constitutional avoidance.

(U) ~~(S)~~ In any event, the acquisition of post-cut-through digits by pen register does not violate the Fourth Amendment. The touchstone for review of government action under the Fourth Amendment is whether a search is "reasonable." *See, e.g., Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 652 (1995); *In re Sealed Case*, 310 F.3d 717, 737, 742, 746 (FISA Ct. Rev. 2002) (emphasizing reasonableness as critical factor in reviewing constitutionality of foreign intelligence surveillance). The collection of non-content DRAS information accompanied by the incidental collection of numbers entered into a phone that may include content, given that no filtering technology is reasonably available to the government, is reasonable under the Fourth Amendment, particularly in the foreign intelligence context.

(U) A. ~~(S)~~ The Collection of Non-Content Post-Cut-Through Digits Is Not a "Search" Within the Meaning of the Fourth Amendment.

(U) ~~(S)~~ The government's collection of a telephone number that a person dials into a phone is not a "search" within the meaning of the Fourth Amendment. *Smith v. Maryland*, 442 U.S. 735 (1979). The logic of *Smith* applies with equal

force to telephone numbers dialed "post-cut-through," for example when the dialer uses a calling card or a third-party call service. *Cf. United States v. Miller*, 425 U.S. 435 (1976). The collection of such non-content "post-cut-through digits" is not a search under the Fourth Amendment — and the incidental collection of content post-cut-through digits is "reasonable" under the Fourth Amendment when subject to appropriate minimization.

(U) In *Smith*, the Court held that the installation and use of a pen register to collect dialed telephone numbers was not a "search" within the meaning of the Fourth Amendment. 442 U.S. at 741-42. The facts of the case involved a person who, in the Court's telling, "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business." *Id.* at 744; *see also id.* at 737-38.

(U) The Court held that a person had no "'legitimate expectation of privacy' regarding the numbers he dialed on his phone." *Smith*, 442 U.S. at 742 ("we doubt that people in general entertain any actual expectation of privacy in the numbers they dial"); *compare Katz v. United States*, 389 U.S. 347 (1967) (addressing applicability of Fourth Amendment where government agents intercept the *contents* of a telephone conversation). In doing so, the *Smith* Court reasoned:

> All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company

> switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

Smith, 442 U.S. at 742; *see id.* at 743 (finding that telephone users "typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes"). In this respect, the Court noted, "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications." *Id.* at 741; *see also United States v. New York Tel. Co.*, 434 U.S. 159, 167-68 (1977) (observing that pen registers "do not hear sound," but rather "disclose only the telephone numbers that have been dialed — a means of establishing communication," and that "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers").

(U) This analysis applies with equal force to phone numbers that are dialed "post-cut-through" as it does to phone numbers that are dialed "pre-cut-through." In both circumstances, the number is "convey[ed]" to a third-party company — the telephone or calling card company — for the purpose of allowing the call to be completed. In both circumstances, moreover, the third-party company maintains

"facilities for making permanent records" of the dialed numbers and generally allows a customer to "see a list of their long-distance (toll) calls."

(U) Other Supreme Court cases make clear that *Smith* is not artificially limited to pre-cut-through digits alone. *Smith* rests on a broader principle that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" for the third party's use in the ordinary course of business. 442 U.S. at 743-44. Thus, in *Miller*, the Court held that a bank depositor has no "legitimate 'expectation of privacy'" in financial information "voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business." 425 U.S. at 442. That was so because, as the Court explained, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." *Id.* at 443.

(U) (S) For that reason, courts have repeatedly applied *Smith* and *Miller* to other kinds of information conveyed to third parties in the ordinary course of business, including where technological changes have given rise to new types of information that were not foreseeable in 1976 (when the Court decided *Miller*) or 1979 (when the Court decided *Smith*). In *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), for example, the Ninth Circuit held that *Smith* applied to email "to/from" and Internet Protocol addressing information. *Id.* at 510-11. In *Quon v. Arch*

Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), *rev'd on other grounds*, 560 U.S. 746 (2010), the Ninth Circuit also applied *Smith* to text message address information. *Id.* at 905. And in *Guest v. Leis*, 255 F.3d 325 (6th Cir. 2001), the Sixth Circuit applied *Smith* to subscriber information, such as names, addresses, birthdates, and passwords, communicated to systems operators and Internet service providers. *Id.* at 335-36. This case is more straightforward. The post-cut-through phone numbers and DRAS information that the government seeks to obtain are the *same kind* of information at issue in *Smith*.

(U) **B. (S) The Government May Incidentally Collect Content Post-Cut-Through Digits.**

(U) (S) The government may collect post-cut-through digits that may constitute content incidental to its collection of non-content post-cut-through digits, subject to appropriate minimization, without violating the Fourth Amendment. The touchstone for lawfulness under the Fourth Amendment is "reasonableness," and it is reasonable for the government to collect, and then minimize, Fourth Amendment-protected information incidental to the collection of non-protected information. *See, e.g.*, *In re Directives*, 551 F.3d at 1015 ("incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful"); *see also United States v. Kahn*, 415 U.S. 143, 156-57 (1974); *United States v. White*, 401 U.S. 745, 751-53 (1971). In this context,

that conclusion is bolstered by the important national-security interests at issue in this case. *See In re Terrorist Bombings of U.S. Embassies*, 552 F.3d 157, 174 (2d Cir. 2008) (discussing "manifest need to investigate possible threats to national security" under reasonableness test).

(U) 1. *"Special needs" analysis.* The Supreme Court has held on several occasions that it is reasonable for the government to conduct a Fourth Amendment "search" without a warrant where doing so serves a "special need." *See Vernonia Sch. Dist.*, 515 U.S. at 653; *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444, 450-51 (1990) (no Fourth Amendment violation where safety interests served by drunk driving checkpoints outweighed motorists' interests in driving without being stopped).

(U) It cannot be disputed that national security — the interest in preventing terrorist attacks by identifying and tracking operatives, preventing acts of espionage, and preventing other acts contrary to the national-security interests of the United States — is a "special need" of the utmost importance. In *United States v. United States District Court (Keith)*, 407 U.S. 297 (1972), the Supreme Court declined to extend the Fourth Amendment warrant requirement to the surveillance of foreign powers or their agents for foreign intelligence purposes. *Id.* at 321-22; *see also Katz*, 389 U.S. at 358 n.23. And as this Court has put it, "the relevant

governmental interest — the interest in national security — is of the highest order of magnitude." *In re Directives*, 551 F.3d at 1012; *In re Sealed Case*, 310 F.3d at 742; *see also Haig v. Agee*, 453 U.S. 280, 307 (1981) ("no governmental interest is more compelling" than national security); *Cassidy v. Chertoff*, 471 F.3d 67, 82 (2d Cir. 2006) ("the prevention of terrorist attacks on [ferries] . . . constitutes a 'special need'"); *MacWade v. Kelly*, 460 F.3d 260, 271 (2d Cir. 2006) ("preventing a terrorist from bombing the subways constitutes a special need"); *Hartness v. Bush*, 919 F.2d 170, 172-73 (D.C. Cir. 1990); H.R. Rep. No. 95-1283, pt. 1, at 17-21 (1978).

X

b1 Per FBI
b3
b6
b7C
b7E

(S)

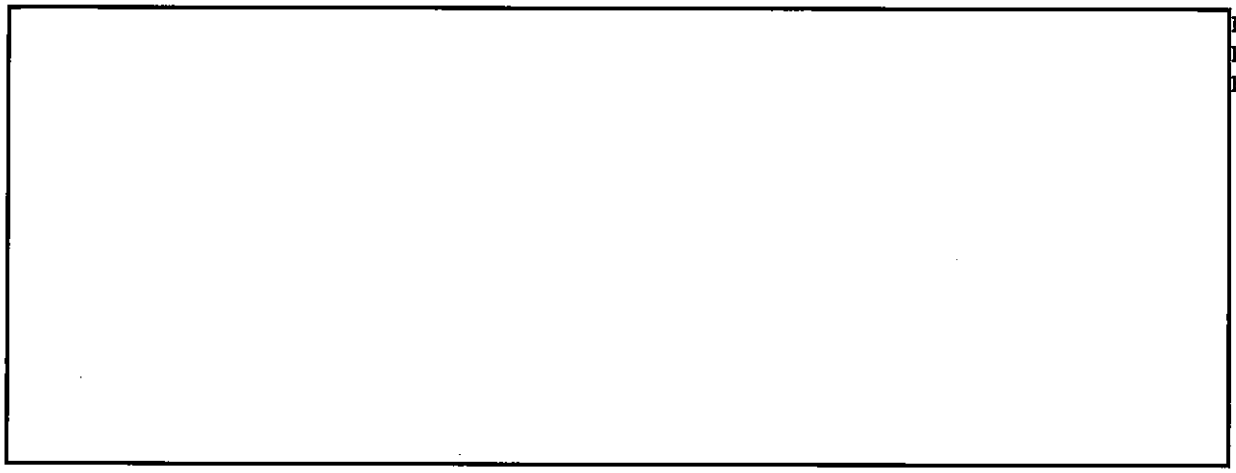
[redacted]

b3 Per FBI
b7E

(U) 2. *"Reasonableness" analysis.* To determine the reasonableness of a search under the Fourth Amendment, courts rely on a balancing test "by assessing, on the one hand, the degree to which [a search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (quoting *Wyoming v. Houghton*, 526 U.S. 295, 300 (1999)); *see also Maryland v. King*, 133 S. Ct. 1958, 1970 (2013) (reasonableness requires balancing "the promotion of legitimate governmental interests against the degree to which [a search] intrudes upon an individual's privacy") (internal quotation marks and citation omitted).

b3 Per FBI
b7E

[redacted]



b1 Per FBI
b3
b7E

(U) ~~(S)~~ In addition, the reasonableness of the collection of post-cut-through digits is bolstered by the government's extensive procedures to minimize access to, and prohibit use of, any post-cut-through digits that may constitute content. The Supreme Court has recognized the relevance of procedures aimed at minimization in assessing the lawfulness of Fourth Amendment searches in a variety of contexts. For example, in upholding post-arrest DNA collection against a Fourth Amendment challenge, the Court found that the government had installed safeguards limiting DNA analysis to identification information alone, thereby reducing any intrusion into privacy. *See King*, 133 S. Ct. at 1979-80. And the Court found that the government's restriction on the testing of student athletes' urine — for illegal drugs and not for any medical condition — was relevant to the Fourth Amendment analysis of a student athlete drug testing program. *See Board of Educ. v. Earls*, 536 U.S. 822, 826, 833-34 (2002).

(U) Protective procedures of this kind are especially salient in the national-security context. In the words of this Court, "[i]f the protections that are in place for individual privacy interests are sufficient in light of the governmental interest at stake, the constitutional scales will tilt in favor of upholding the government's actions." *In re Directives*, 551 F.3d at 1012.

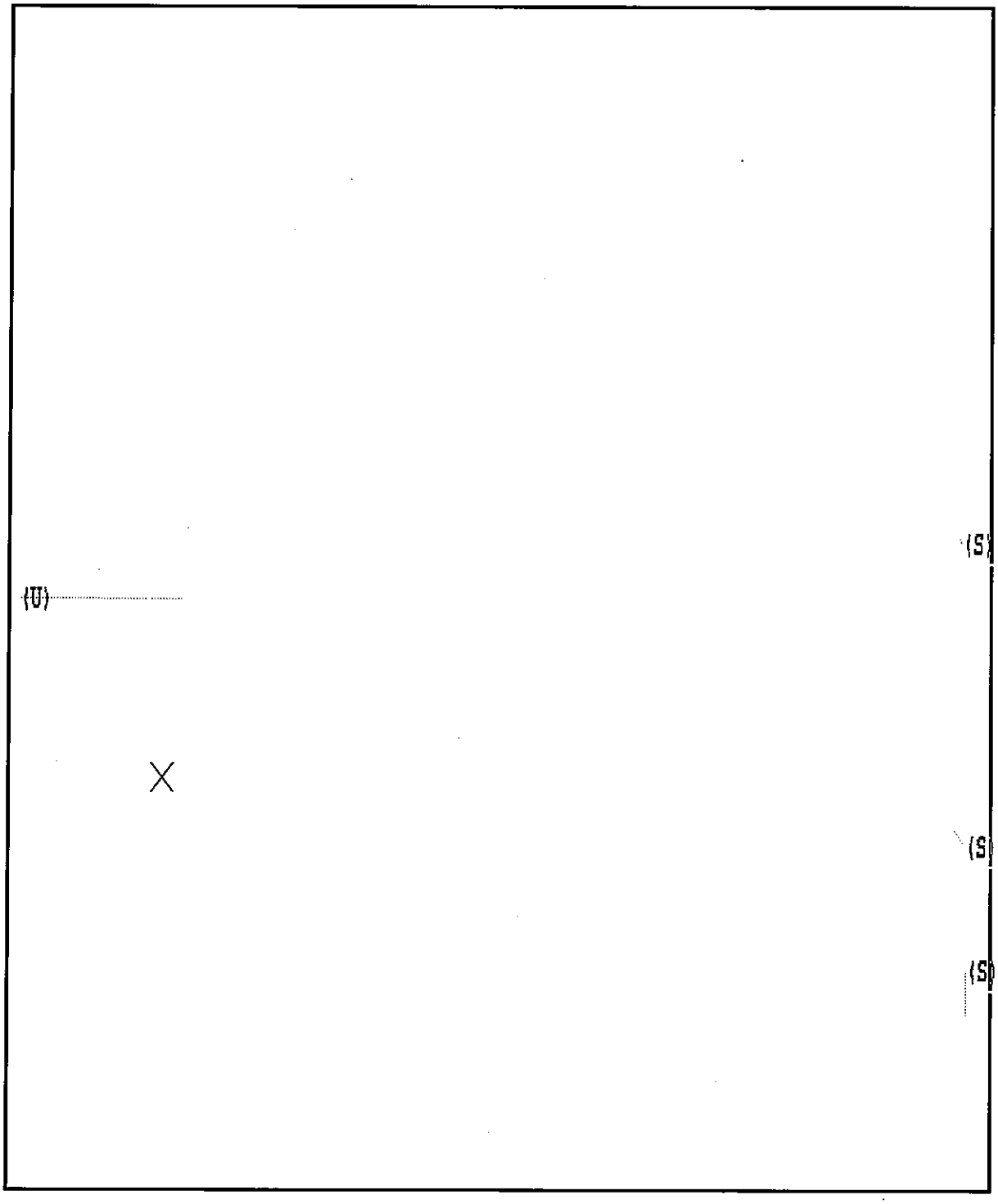
(U) ~~(S)~~ Here, the government's procedures to ensure against the use of, or even access to, content post-cut-through digits are robust. [redacted] b3 Per FBI b7E

[redacted]

b3 Per FBI
b7E

(U) X

X



b1 Per FBI
b3
b6
b7C
b7E

(S)

(S)

b1 Per FBI
b3
b6
b7C
b7E

(U) CONCLUSION

(S) For these reasons, and those stated in rulings by the FISC, this Court should answer the certified question of law in the affirmative. The government's acquisition of post-cut-through digits pursuant to FISA pen register orders is lawful under the relevant statutory language and does not offend the Fourth Amendment.

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 22, 2016

(U) CERTIFICATE OF COMPLIANCE

(U) 1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B), because it contains 12,254 words, 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 22, 2016

(U) CERTIFICATE OF SERVICE

(S) Pursuant to Foreign Intelligence Surveillance Court of Review Rules of Procedure 10(b) and 16, on March 22, 2016, I provided two copies of the Opening 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:

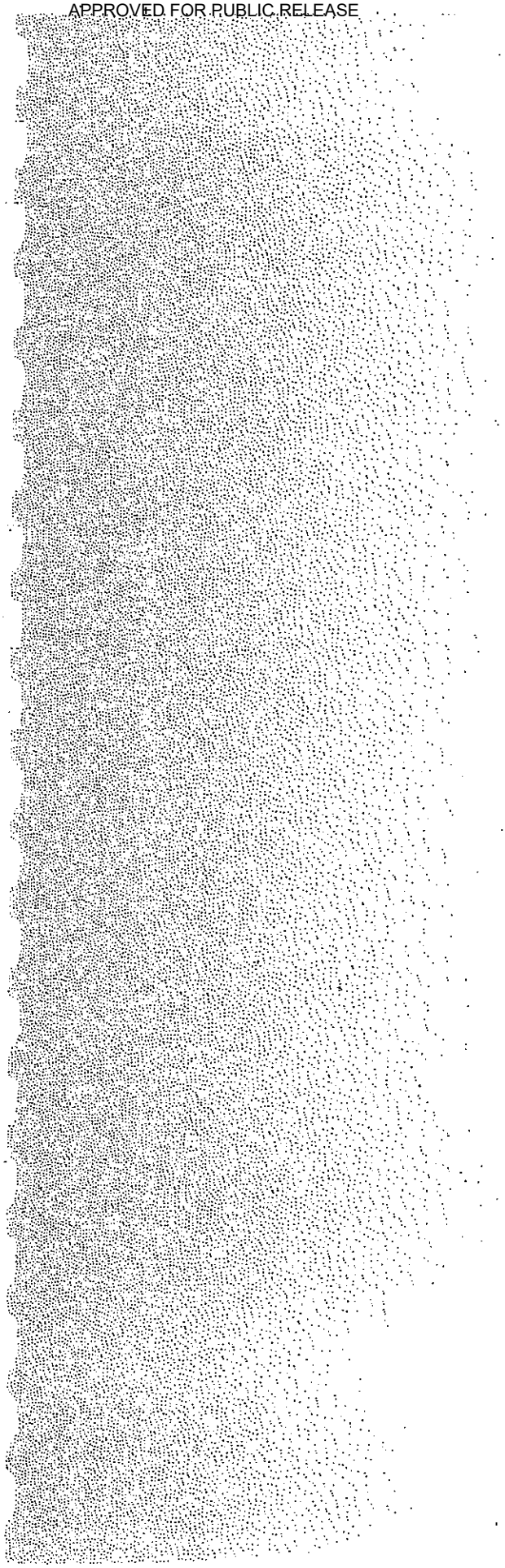
Marc Zwillinger
ZwillGen PLLC
1900 M Street, NW, Suite 250
Washington, DC 20036
Telephone: (202) 296-3585
Facsimile: (202) 706-5298

b6, b7C [redacted]

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

Dated: March 22, 2016

b6 Per FBI
b7C



(U) STATUTORY ADDENDUM

(U) CONTENTS

(U) 18 U.S.C. § 2510
(U) Definitions

As used in this chapter--

(1) "wire communication" means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;

(2) "oral communication" means any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation, but such term does not include any electronic communication;

. . .

(8) "contents", when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication;

. . .

(12) "electronic communication" means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include--

(A) any wire or oral communication;

(B) any communication made through a tone-only paging device;

(C) any communication from a tracking device (as defined in section 3117 of this title); or

(D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

. . .

(U) 18 U.S.C. § 3121

(U) General prohibition on pen register and trap and trace device use; exception

(a) In general.--Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception.--The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

(c) Limitation.--A government agency authorized to install and use a pen register or trap and trace device under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.

(d) Penalty.--Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

(U) 18 U.S.C. § 3127
(U) Definitions for chapter

As used in this chapter--

(1) the terms "wire communication", "electronic communication", "electronic communication service", and "contents" have the meanings set forth for such terms in section 2510 of this title;

(2) the term "court of competent jurisdiction" means--

(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that--

(i) has jurisdiction over the offense being investigated;

(ii) is in or for a district in which the provider of a wire or electronic communication service is located;

(iii) is in or for a district in which a landlord, custodian, or other person subject to subsections (a) or (b) of section 3124 of this title is located; or

(iv) is acting on a request for foreign assistance pursuant to section 3512 of this title; or

(B) a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device;

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication, but such term does not

include any device or process used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device or process used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business;

(4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication;

(5) the term "attorney for the Government" has the meaning given such term for the purposes of the Federal Rules of Criminal Procedure; and

(6) the term "State" means a State, the District of Columbia, Puerto Rico, and any other possession or territory of the United States.

(U) 50 U.S.C. § 1841
(U) Definitions

As used in this subchapter:

(1) The terms "foreign power", "agent of a foreign power", "international terrorism", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", and "State" shall have the same meanings as in section 1801 of this title.

(2) The terms "pen register" and "trap and trace device" have the meanings given such terms in section 3127 of Title 18.

(3) The term "aggrieved person" means any person--

(A) whose telephone line was subject to the installation or use of a pen register or trap and trace device authorized by this subchapter; or

(B) whose communication instrument or device was subject to the use of a pen register or trap and trace device authorized by this subchapter to capture incoming electronic or other communications impulses.

(4)(A) The term "specific selection term"--

(i) is a term that specifically identifies a person, account, address, or personal device, or any other specific identifier; and

(ii) is used to limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device.

(B) A specific selection term under subparagraph (A) does not include an identifier that does not limit, to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose for seeking the use of the pen register or trap and trace device, such as an identifier that--

(i) identifies an electronic communication service provider (as that term is defined in section 1881 of this title) or a provider of remote computing service (as that term

is defined in section 2711 of Title 18), when not used as part of a specific identifier as described in subparagraph (A), unless the provider is itself a subject of an authorized investigation for which the specific selection term is used as the basis for the use; or

(ii) identifies a broad geographic region, including the United States, a city, a county, a State, a zip code, or an area code, when not used as part of a specific identifier as described in subparagraph (A).

(C) For purposes of subparagraph (A), the term "address" means a physical address or electronic address, such as an electronic mail address or temporarily assigned network address (including an Internet protocol address).

(D) Nothing in this paragraph shall be construed to preclude the use of multiple terms or identifiers to meet the requirements of subparagraph (A).

(U) 50 U.S.C. § 1842
(U) Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations

(a) Application for authorization or approval

(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

(2) The authority under paragraph (1) is in addition to the authority under subchapter I of this chapter to conduct the electronic surveillance referred to in that paragraph.

(b) Form of application; recipient

Each application under this section shall be in writing under oath or affirmation to-

-

(1) a judge of the court established by section 1803(a) of this title; or

(2) a United States Magistrate Judge under chapter 43 of Title 28 who is publicly designated by the Chief Justice of the United States to have the power to hear applications for and grant orders approving the installation and use of a pen register or trap and trace device on behalf of a judge of that court.

(c) Executive approval; contents of application

Each application under this section shall require the approval of the Attorney General, or a designated attorney for the Government, and shall include--

(1) the identity of the Federal officer seeking to use the pen register or trap and trace device covered by the application;

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution; and

(3) a specific selection term to be used as the basis for the use of the pen register or trap and trace device.

(d) Ex parte judicial order of approval

(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the installation and use of a pen register or trap and trace device if the judge finds that the application satisfies the requirements of this section.

(2) An order issued under this section--

(A) shall specify--

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is

listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied; and

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order;

(B) shall direct that--

(i) upon request of the applicant, the provider of a wire or electronic communication service, landlord, custodian, or other person shall furnish any information, facilities, or technical assistance necessary to accomplish the installation and operation of the pen register or trap and trace device in such a manner as will protect its secrecy and produce a minimum amount of interference with the services that such provider, landlord, custodian, or other person is providing the person concerned;

(ii) such provider, landlord, custodian, or other person--

(I) shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person unless or until ordered by the court; and

(II) shall maintain, under security procedures approved by the Attorney General and the Director of National Intelligence pursuant to section 1805(b)(2)(C) of this title, any records concerning the pen register or trap and trace device or the aid furnished; and

(iii) the applicant shall compensate such provider, landlord, custodian, or other person for reasonable expenses incurred by such provider, landlord, custodian, or other person in providing such information, facilities, or technical assistance; and

(C) shall direct that, upon the request of the applicant, the provider of a wire or electronic communication service shall disclose to the Federal officer using the pen register or trap and trace device covered by the order--

(i) in the case of the customer or subscriber using the service covered by the order (for the period specified by the order)--

(I) the name of the customer or subscriber;

(II) the address of the customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of the customer or subscriber, including any temporarily assigned network address or associated routing or transmission information;

(IV) the length of the provision of service by such provider to the customer or subscriber and the types of services utilized by the customer or subscriber;

(V) in the case of a provider of local or long distance telephone service, any local or long distance telephone records of the customer or subscriber;

(VI) if applicable, any records reflecting period of usage (or sessions) by the customer or subscriber; and

(VII) any mechanisms and sources of payment for such service, including the number of any credit card or bank account utilized for payment for such service; and

(ii) if available, with respect to any customer or subscriber of incoming or outgoing communications to or from the service covered by the order--

(I) the name of such customer or subscriber;

(II) the address of such customer or subscriber;

(III) the telephone or instrument number, or other subscriber number or identifier, of such customer or subscriber, including any temporarily assigned network address or associated routing or transmission information; and

(IV) the length of the provision of service by such provider to such customer or subscriber and the types of services utilized by such customer or subscriber.

(e) Time limitation

(1) Except as provided in paragraph (2), an order issued under this section shall authorize the installation and use of a pen register or trap and trace device for a period not to exceed 90 days. Extensions of such an order may be granted, but only upon an application for an order under this section and upon the judicial finding required by subsection (d) of this section. The period of extension shall be for a period not to exceed 90 days.

(2) In the case of an application under subsection (c) where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a United States person, an order, or an extension of an order, under this section may be for a period not to exceed one year.

(f) Cause of action barred

No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance under subsection (d) of this section in accordance with the terms of an order issued under this section.

(g) Furnishing of results

Unless otherwise ordered by the judge, the results of a pen register or trap and trace device shall be furnished at reasonable intervals during regular business hours for the duration of the order to the authorized Government official or officials.

(h) Privacy procedures

(1) In general

The Attorney General shall ensure that appropriate policies and procedures are in place to safeguard nonpublicly available information concerning United States persons that is collected through the use of a pen register or trap and trace device installed under this section. Such policies and procedures shall, to the maximum extent practicable and consistent with the need to protect national security, include privacy protections that apply to the collection, retention, and use of information concerning United States persons.

(2) Rule of construction

Nothing in this subsection limits the authority of the court established under section 1803(a) of this title or of 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.

(U) 50 U.S.C. § 1843
(U) Authorization during emergencies

(a) Requirements for authorization

Notwithstanding any other provision of this subchapter, when the Attorney General makes a determination described in subsection (b) of this section, the Attorney General may authorize the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution if--

(1) a judge referred to in section 1842(b) of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and

(2) an application in accordance with section 1842 of this title is made to such judge as soon as practicable, but not more than 7 days, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.

(b) Determination of emergency and factual basis

A determination under this subsection is a reasonable determination by the Attorney General that--

(1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is

not conducted solely upon the basis of activities protected by the first amendment to the Constitution before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title; and

(2) the factual basis for issuance of an order under such section 1842 of this title to approve the installation and use of the pen register or trap and trace device, as the case may be, exists.

(c) Effect of absence of order

(1) In the absence of an order applied for under subsection (a)(2) of this section approving the installation and use of a pen register or trap and trace device authorized under this section, the installation and use of the pen register or trap and trace device, as the case may be, shall terminate at the earlier of--

(A) when the information sought is obtained;

(B) when the application for the order is denied under section 1842 of this title; or

(C) 7 days after the time of the authorization by the Attorney General.

(2) In the event that an application for an order applied for under subsection (a)(2) of this section is denied, or in any other case where the installation and use of a pen register or trap and trace device under this section is terminated and no order under section 1842 of this title is issued approving the installation and use of the pen register or trap and trace device, as the case may be, no information obtained or evidence derived from the use of the pen register or trap and trace device, as the case may be, shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from the use of the pen register or trap and trace

device, as the case may be, shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(d) Privacy procedures

Information collected through the use of a pen register or trap and trace device installed under this section shall be subject to the policies and procedures required under section 1842(h) of this title.

(U) 50 U.S.C. § 1844

(U) Authorization during time of war

Notwithstanding any other provision of law, the President, through the Attorney General, may authorize the use of a pen register or trap and trace device without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed 15 calendar days following a declaration of war by Congress.

(U) 50 U.S.C. § 1845
(U) Use of information

(a) In general

(1) Information acquired from the use of a pen register or trap and trace device installed pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the provisions of this section.

(2) No information acquired from a pen register or trap and trace device installed and used pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Disclosure for law enforcement purposes

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(c) Notification of intended disclosure by United States

Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States against an aggrieved person any information obtained or derived from the use of a pen register or trap and trace device pursuant to this subchapter, the United States shall, before the trial, hearing, or the other proceeding or at a reasonable time before an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(d) Notification of intended disclosure by State or political subdivision

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the State or political subdivision thereof against an aggrieved person any information obtained or derived from the use of a pen register or trap and trace device pursuant to this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

(1) Any aggrieved person against whom evidence obtained or derived from the use of a pen register or trap and trace device is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, or a State or political subdivision thereof, may move to suppress the evidence obtained or derived from the use of the pen register or trap and trace device, as the case may be, on the grounds that--

(A) the information was unlawfully acquired; or

(B) the use of the pen register or trap and trace device, as the case may be, was not made in conformity with an order of authorization or approval under this subchapter.

(2) A motion under paragraph (1) shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the aggrieved person concerned was not aware of the grounds of the motion.

(f) In camera and ex parte review

(1) Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to the use of a pen register or trap and trace device authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from the use of a pen register or trap and trace device authorized by this subchapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law and if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the use of the pen register or trap and trace device, as the case may be, as may be necessary to determine whether the use of the pen register or trap and trace device, as the case may be, was lawfully authorized and conducted.

(2) In making a determination under paragraph (1), the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the use of the pen register or trap and trace device, as the case may be, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the use of the pen register or trap and trace device, as the case may be.

(g) Effect of determination of lawfulness

(1) If the United States district court determines pursuant to subsection (f) of this section that the use of a pen register or trap and trace device was not lawfully authorized or conducted, the court may, in accordance with the requirements of

law, suppress the evidence which was unlawfully obtained or derived from the use of the pen register or trap and trace device, as the case may be, or otherwise grant the motion of the aggrieved person.

(2) If the court determines that the use of the pen register or trap and trace device, as the case may be, was lawfully authorized or conducted, it may deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Binding final orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that the use of a pen register or trap and trace device was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the installation and use of a pen register or trap and trace device shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(U) 50 U.S.C. § 1846
(U) Congressional oversight

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate, and the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate, concerning all uses of pen registers and trap and trace devices pursuant to this subchapter.

(b) On a semiannual basis, the Attorney General shall also provide to the committees referred to in subsection (a) of this section and to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

(1) the total number of applications made for orders approving the use of pen registers or trap and trace devices under this subchapter;

(2) the total number of such orders either granted, modified, or denied;

(3) the total number of pen registers and trap and trace devices whose installation and use was authorized by the Attorney General on an emergency basis under section 1843 of this title, and the total number of subsequent orders approving or denying the installation and use of such pen registers and trap and trace devices;

(4) each department or agency on behalf of which the Attorney General or a designated attorney for the Government has made an application for an order authorizing or approving the installation and use of a pen register or trap and trace device under this subchapter; and

(5) for each department or agency described in paragraph (4), each number described in paragraphs (1), (2), and (3).

Exhibit A

b6 Per FBI
b7C