

~~SECRET//ORCON//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW

WASHINGTON, D.C.

U.S. COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA
SURVEILLANCE COURT
2016 FEB 19 PM 4:58
CLERK OF COURT
b6 Per FBI
b7C

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

Docket Number: FISCR 16-01
UNDER SEAL

**WRITTEN NOTICE IN RESPONSE TO ORDER APPOINTING AN AMICUS
CURIAE AND BRIEFING ORDER**

~~(S//OC/NF)~~ The United States respectfully submits this written notice in response to this Court's Order Appointing an *Amicus Curiae* and Briefing Order (Order) in the above-captioned docket, dated February 17, 2016. That Order stated that the Court has determined that the materials identified in Exhibit A thereto are relevant to the duties of the amicus appointed in that Order. Order at 2. It further stated that the Court believes that in this matter, the amicus's access to classified information (the materials identified in Exhibit A) is consistent with the national security of the United States, "[i]f, however, the government believes otherwise, it shall provide written notice and explanation to the Court by February 19, 2016." Order at 2. The government respectfully submits that while it has determined that the provision of the materials identified in Exhibit A to the Order to the amicus is generally consistent with national

~~SECRET//ORCON//NOFORN~~

~~Classified by: Chief, Operations Section, OI, NSD, DOJ
Derived from: Multiple Sources
Declassify on: 20410219~~

~~SECRET//ORCON/NOFORN~~

security, certain limited information therein is not relevant to the legal issues being briefed or the ability of the amicus to brief such issues, and therefore the amicus does not have a need to know and making that information available to him would not be consistent with the national security. In particular, target names not yet released to the amicus, and not relevant to his duties, should be redacted.¹ Such redactions would apply to the Supplemental Order in docket number PR/TT 2015-0053, the Submission Regarding Post-Cut-Through Digits in docket number PR/TT 2015-0053, the Supplemental Order in docket numbers PR/TT 2009-0036, PR/TT 2009-0037, and PR/TT 2009-0038, and the Verified Memorandum of Law in Response to the Court's June 18, 2009 Supplemental Order in docket numbers PR/TT 2009-0036, PR/TT 2009-0037, and

¹ ~~(S//OC/NF)~~ The Government understands that [REDACTED] was shared with the amicus for conflict purposes. Therefore, that name has not been redacted from the relevant materials identified in Exhibit A. In addition, under the facts of this particular case and due to the intersection between those facts and some of the legal issues to be briefed, the government believes that in this case providing the amicus with the factual predication of the investigation of the target set forth in docket number [REDACTED] is consistent with national security.

b3 Per FBI
b7E

~~SECRET//ORCON/NOFORN~~

~~SECRET//ORCON//NOFORN~~

PR/TT 2009-0038, and would be limited to the target names in the captions. Those four documents with the above-described redactions are attached hereto at Tabs A through D.

Respectfully submitted,

b6, b7C

Deputy Chief, Operations Section
Office of Intelligence

National Security Division
U.S. Department of Justice

Dated: February 19, 2016

~~SECRET//ORCON//NOFORN~~

TAB A

Filed
United States Foreign
Intelligence Surveillance Court

JUL 08 2015

LeeAnn Flynn Hall, Clerk of Court

~~SECRET//NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

IN RE [redacted]
[redacted]

Docket Number: PR/TT

15-53

SUPPLEMENTAL ORDER

On this date, the Court has issued a Primary Order authorizing the government to conduct pen register/trap and trace surveillance in the above-captioned matter. The Court's Order includes the following provision:

[redacted] this authority includes the authority to record and decode all post-cut-through digits, as described in the Government's Verified Memorandum of Law Regarding the Collection of Post-Cut-Through Digits Through Telephone Pen Register Surveillance Under the Foreign Intelligence Surveillance Act, filed with the Court on August 17, 2009, in Docket Numbers PR/TT 09-36, PR/TT 09-37 and PR/TT 09-38. The Government shall not make any affirmative investigative use of post-cut-through digits acquired through pen register authorization that do not constitute call dialing, routing, addressing or signaling information, unless separately authorized by this Court.

b3 Per FBI
b7E

The government extensively briefed the issue of post-cut-through digits in its Verified Memorandum of Law that was filed with the FISC on August 17, 2009 (Memorandum). In that filing, the government represented that there was no technology reasonably available to the government that could distinguish between content and non-content post-cut-through digits at the time of acquisition. Memorandum at 7-9.

b3 Per FBI
b7E

[Large redacted area]

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

Id. at 26 n. 17.



b3 Per FBI
b7E

The government shall make a written submission to the Court either at the time of submission of a proposed renewal application for the above-captioned matter [redacted] of the issuance of this Supplemental Order, whichever is sooner. This submission shall include:

(1) A description of whether and to what extent technology that is now reasonably available to the government can distinguish between content and non-content post-cut-through digits prior to acquisition; and what efforts the government is making to develop such technology if it does not currently exist.

(2) An updated description of the procedures the government is using to prevent the unauthorized use of post-cut-through digits that constitute "content" and are acquired pursuant to FISC pen register/trap and trace orders.

(3) A description of the volume of post-cut-through digits acquired pursuant to the Court's order in this matter and an explanation of how any post-cut through digits acquired were stored and handled, and what steps the government took to prevent the use of any post-cut-through digits that constituted "content."

(4) A report on the status of the FBI's efforts to implement the technical enhancements described in the Memorandum.

ENTERED this 8th day of July, 2015 in Docket No. PR/TT 15-53

Claire V. Eagan
CLAIRE V. EAGAN
Judge, United States Foreign
Intelligence Surveillance Court

b6, b7C [redacted] Chief Deputy Clerk,
FISC, certify that this document is a
true and correct copy of the original

b6, b7C

~~SECRET//NOFORN~~

APPROVED FOR PUBLIC RELEASE

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 09-08-2021 BY NSICG

b6 Per FBI
b7C

TAB B

~~SECRET//NOFORN~~

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

UNITED STATES

2015 OCT -2 AM 10:30

FOREIGN INTELLIGENCE SURVEILLANCE COURT
LEAHN FLYNN HALL
CLERK OF COURT

WASHINGTON, D.C.

~~(S)~~ IN RE [redacted]
[redacted]

Docket Number: PRTT 2015-0053

(U) SUBMISSION REGARDING POST-CUT-THROUGH DIGITS

~~(S//NF)~~ The United States respectfully submits this report in response to this Court's Supplemental Order in the above-captioned docket, dated July 8, 2015, directing the government to make a written submission regarding the acquisition of post-cut-through digits pursuant to pen register orders under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq. (FISA), including: (1) A description of whether and to what extent technology that is now reasonably available to the government can distinguish between content and non-content post-cut-through digits prior to acquisition, and what efforts the government is making to develop such technology if it does not currently exist; (2) An updated description of the procedures the government is using to prevent the unauthorized use of post-cut-through digits that constitute

~~SECRET//NOFORN~~

~~Classified by: Chief, Operations Section, OI/NSD, DOJ
Derived from: Multiple Sources
Declassify on: 20400930~~

~~SECRET//NOFORN~~

"content" and are acquired pursuant to FISC pen register/trap and trace orders; (3) A description of the volume of post-cut-through digits acquired pursuant to the Court's order in this matter and an explanation of how any post-cut-through digits acquired were stored and handled, and what steps the government took to prevent the use of any post-cut-through digits that constituted "content"; and (4) A report on the status of the FBI's efforts to implement the technical enhancements described in the Government's Verified Memorandum of Law on post-cut-through digits filed with this Court on August 17, 2009. This submission addresses the information requested by the Court.

I. (U) BACKGROUND

(S) On May 23, 2006, the government filed with this Court, in docket number

[REDACTED]

a Verified Memorandum of Law (May 2006 Memorandum) advising the

Court about the government's collection of post-cut-through digits through pen register surveillance under FISA and explaining why such collection is necessary and lawful.¹

On August 17, 2009, the government filed, in docket numbers PR/TT 09-36, PR/TT 09-37, and PR/TT 09-38, a Verified Memorandum of Law extensively briefing the issue of post-cut-through digits (2009 Memorandum).

(S) In response to the Court's Orders, the Government also filed submissions with further legal analysis on post-cut-through digits on [REDACTED] in docket number

[REDACTED]

b3 Per FBI
b7E

b3 Per FBI
b7E

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

(U) As explained in the May 2006 and 2009 Memoranda, a pen register, defined in pertinent part, is "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) (incorporated into FISA at 50 U.S.C. § 1841(2)). "Post-cut-through digits" is a term of art that refers to digits dialed from a targeted telephone number 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 information), such as when a caller dials a toll free number to connect to a service provider (e.g., 1-800-CALL ATT), then after the initial call is connected to the service provider, enters another phone number, which is the ultimate call destination. 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 enters a bank account or prescription number. In either case, the digits are sequences of numbers.

(S) In the May 2006 and 2009 Memoranda, the government advised the Court that no technology exists that would permit the FBI to distinguish, at the acquisition point, between content and non-content post-cut-through digits, and then record or

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

decode only the non-content digits.² In the May 2006 and 2009 Memoranda, the government also reported that it would make no affirmative investigative use of any incidentally captured content post-cut-through digits, except in rare cases in order to prevent an immediate danger of death, serious physical injury, or harm to the national security. As a longstanding practice, this Court's Orders for pen registers authorizing collection of all post-cut-through digits specifically state, "The Government shall not make any affirmative investigative use of post-cut-through digits acquired through pen register authorization that do not constitute call dialing, routing, addressing or signaling information, unless separately authorized by this Court."

II. (U) THERE IS NO TECHNOLOGY REASONABLY AVAILABLE TO THE GOVERNMENT THAT CAN DISTINGUISH BETWEEN CONTENT AND NONCONTENT POST-CUT-THROUGH DIGITS AT ACQUISITION.

(U) There continues to be no reasonably available technology that permits a service provider to identify and segregate content post-cut-through digits prior to delivery to the government. There is also no reasonably available technology that permits the government, upon receipt of this information and without further analysis,

² (U) The so-called pen register limitation provision states that "[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). This limitation provision applies to FISA pen registers because FISA adopts the pen register and trap and trace definitions in section 3127 of Title 18.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

to determine whether the acquired digits represent content. The government believes that it is unlikely that such technology will be available in the foreseeable future.

(U) As described in detail in the 2009 Memorandum, the current architecture and complexity of the global telecommunications network creates tremendous challenges for separating content post-cut-through digits from non-content dialing, routing, addressing and signaling information in real time.

b3 Per FBI
b7E

(U)

b3 Per FBI
b7E

³ (U) Call-identifying information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2).

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~b3 Per FBI
b7E

III. (U) PREVENTION OF UNAUTHORIZED USE OF POST-CUT-THROUGH DIGITS THAT CONSTITUTE CONTENT

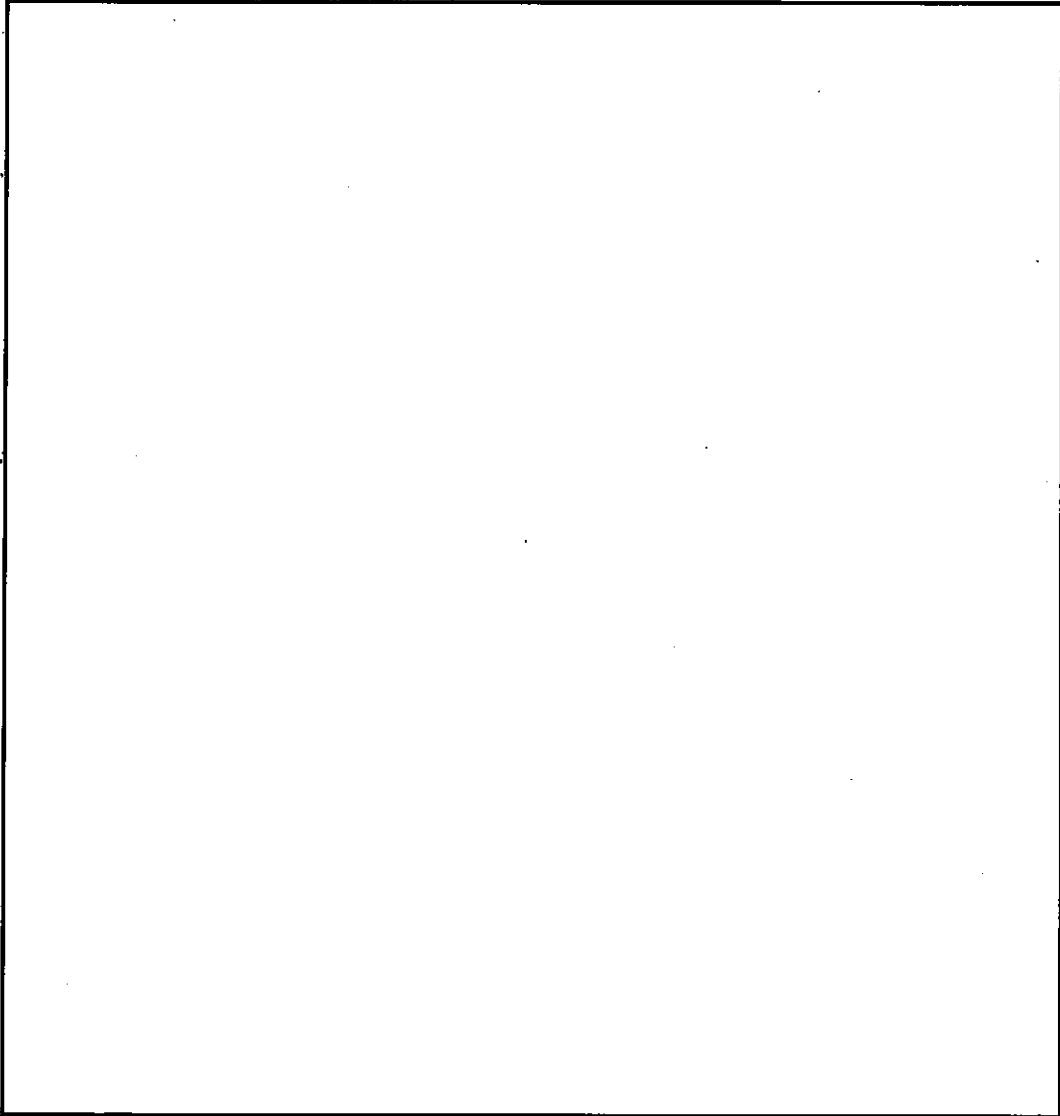
(U) The government recognizes the concerns regarding the collection of content through the operation of pen registers and has continued to take extraordinary steps to restrict the collection and/or use of content post-cut-through digits. As described in the 2009 Memorandum, on May 24, 2002, then Deputy Attorney General Larry D. Thompson issued a memorandum (the "DAG Memo" (attached thereto as Ex. A)) to all Department of Justice components setting forth the Department's policy regarding the avoidance of "over-collection" in the use of pen registers and trap and trace devices that are deployed under the authority of 18 U.S.C. § 3121, *et seq.*⁴ The memorandum requires that reasonably available technology be used to avoid over-collection and, if over-collection does occur despite the use of reasonably available technology, no affirmative investigative use be made of that information except to prevent immediate

⁴ (U) The DAG Memo specifically states, "The authorities granted by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, *et seq.*, are outside the scope of this Memorandum." DAG Mem. at 1, n.1. As discussed below, the FBI has since enacted policies that apply the principles of the DAG Memo to post-cut-through digits collected pursuant to a pen register authorized under FISA.

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

danger of death, serious physical injury, or harm to the national security. These principles continue to reflect the policy of the government regarding the collection and use of post-cut-through digits.



b3 Per FBI
b7E

~~SECRET//NOFORN~~

APPROVED FOR PUBLIC RELEASE

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-14-2021 BY NSICC

b6 Per FBI
b7C

TAB C

b6 Per FBI
b7C

~~SECRET//ORCON,NOFORN~~

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

IN RE [redacted]
[redacted]

Docket No. PR/TT 09-36

IN RE [redacted]
[redacted]

Docket No. PR/TT 09-37

IN RE [redacted]
[redacted]

Docket No. PR/TT 09-38

SUPPLEMENTAL ORDER

On June 17, 2009, in Docket Nos. PR/TT 09-36 and PR/TT 09-37, and on June 18, 2009, in Docket No. PR/TT 09-38, the Court granted pen register/trap-and-trace authority on the terms requested in the government's applications. Those authorizations included the following provision:

[T]his authority includes the authority to record and decode all post-cut-through digits,¹ as described in the Government's Verified Memorandum of Law Regarding the Collection of Post-Cut-Through Digits Through Telephone Pen Register Surveillance Under the Foreign Intelligence Surveillance Act, filed with the Court on May 23, 2006, in Docket Number PR/TT 06-79. The Government shall not make any affirmative investigative use, through pen register authorization, of post-cut-through digits that do not constitute call dialing, routing, addressing or signaling information, unless separately authorized by this Court.

Docket No. PR/TT 09-36, Primary Order at 3-4; Docket No. PR/TT 09-37, Primary Order at 3; Docket No. PR/TT 09-38 at 3-4.

[redacted]

b3 Per FBI
b7E

¹ "Post-cut-through digits" are numbers dialed on a telephone after an initial connection is made (i.e., after the call is "cut through").

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

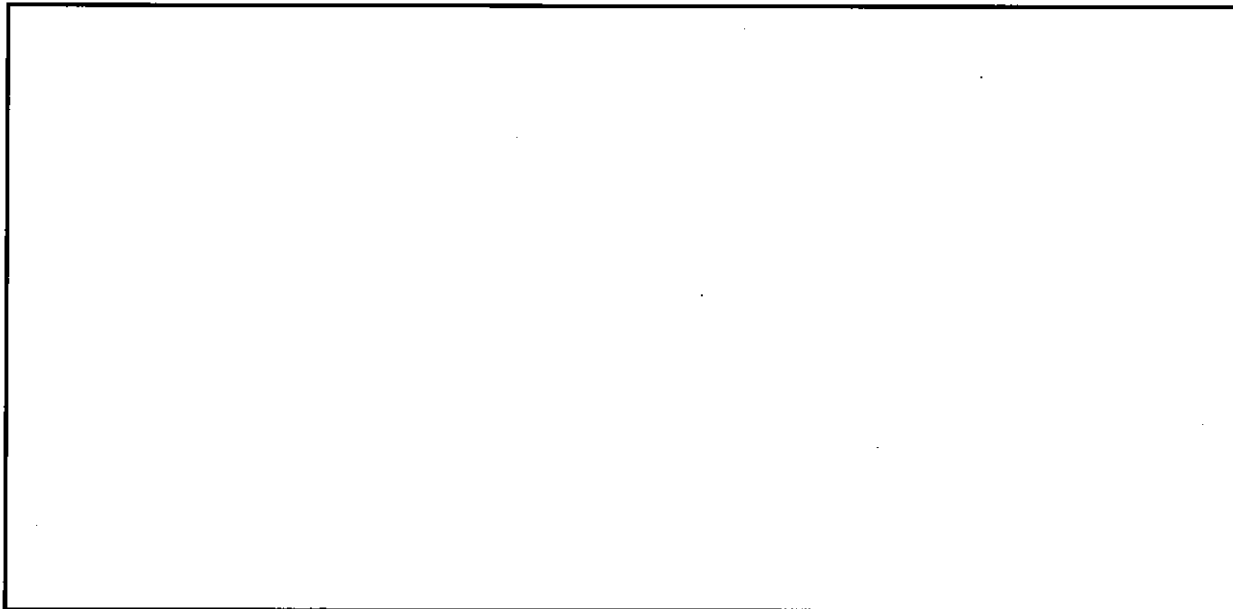


b3 Per FBI
b7E

In view of these circumstances, and the likelihood that the issue of acquiring post-cut-through digits will continue to be presented in pen register applications presented to the FISC, it is hereby ORDERED as follows:

On or before August 17, 2009, the government shall make a written submission to the FISC regarding the acquisition of post-cut-through digits under pen register orders. This submission shall include:

- (1) A description of whether and to what extent technology that is now reasonably available to the government can distinguish between content and non-content post-cut-through digits prior to acquisition, to include an explanation of whether such capabilities vary from case to case (e.g., depending on the provider or the nature of the service used by the target). If such technology does not currently



b3 Per FBI
b7E

~~SECRET//ORCON,NOFORN~~

~~SECRET//ORCON,NOFORN~~

exist, the submission shall include a description of what efforts are being made by the government to develop such technology.

(2) A discussion of the legal issues presented, in light of the current technology and the opinions cited in footnote 3 above.

ENTERED this 18th day of June, 2009 in Docket Nos. PR/TT 09-36, PR/TT 09-37, and PR/TT 09-38.


THOMAS F. HOGAN
Judge, United States Foreign
Intelligence Surveillance Court

~~SECRET//ORCON,NOFORN~~

b6, b7C [redacted] Deputy Clerk
[redacted] SC, certify that this document
is a true and correct copy of
the original. b6, b7C [redacted]

APPROVED FOR PUBLIC RELEASE

ALL INFORMATION CONTAINED
HEREIN IS UNCLASSIFIED
DATE 10-14-2021 BY NSICG

b6 Per FBI
b7C

TAB D

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

~~SECRET~~

UNITED STATES

2009 AUG 17 PM 4:17

FOREIGN INTELLIGENCE SURVEILLANCE COURT

CLERK OF COURT

WASHINGTON, D.C.

IN RE [redacted]	:	Docket No.: PR/TT 09-36
[redacted]	:	
IN RE [redacted]	:	Docket No.: PR/TT 09-37
[redacted]	:	
IN RE [redacted]	:	Docket No.: PR/TT 09-38
[redacted]	:	
[redacted] ⓧ	:	

VERIFIED MEMORANDUM OF LAW IN RESPONSE TO
THE COURT'S JUNE 18, 2009 SUPPLEMENTAL ORDER

~~SECRET~~

~~Classified by: David S. Kris, Assistant Attorney
General, NSD, DOJ~~
Reason: ~~1.4(e)~~
Declassify on: ~~17 August 2034~~

~~SECRET~~

TABLE OF CONTENTS

I. BACKGROUND: THE 2006 MEMORANDA AND REPORT (U) 2

II. STATEMENT OF FACTS CONCERNING POST-CUT-THROUGH DIGITS (U) 7

 A. There is No Technology Reasonably Available to the Government That Can Distinguish Between Content and Non-Content Post-Cut-Through Digits Prior to Acquisition. (U) 7

 B. Because of the Limitations of Available Technology, the Government Has Developed Policies and Procedures to Restrict the Collection and Unauthorized Use of Post-Cut-Through Digit Content. (U) 23

III. ANALYSIS OF LAW (U) 30

 A. The Plain Text of the Pen Register Statute Authorizes the Government Incidentally to Record or Decode Content Post-Cut-Through Digits In Order to Collect Call Processing Information. (U) 32

 1. As Originally Adopted, 18 U.S.C. Sections 3127(3) and 3121(c) Contemplated the Collection of All Post-Cut-Through Digits. (U) 32

b3 Per FBI
b7E Per FBI

~~SECRET~~

~~SECRET~~

- 2. Amendments to 18 U.S.C. Sections 3127(3) and 3121(c) by the PATRIOT Act Further Support the Collection of All Post-Cut-Through Digits. (U) 34
- 3. The Opinions Denying Collection of Post-Cut-Through Digits Under the Criminal Pen Register Statute Interpret the Definition of Pen Register in Isolation, Resulting In a Strained "Plain Meaning" of the Text. (U) 38
- B. The Legislative History of the Criminal Pen Register Statute Confirms that Congress Intended to Allow the Incidental Recording or Decoding of Content Post-Cut-Through Digits. (U) 43
 - 1. Legislative History Regarding the Enactment of 18 U.S.C. Section 3121(c) Confirms that Congress Intentionally Created a Technology-Driven Minimization Scheme. (U) 43
 - 2. The Legislative History of Section 216 of the PATRIOT Act Confirms that Congress Intended to Preserve the Post-Cut-Through Digits Minimization Scheme Created in 1994. (U) 48
 - 3. The Opinions Denying Collection of Post-Cut-Through Digits Under the Criminal Pen Register Statute Misread the Legislative History. (U) 52
- C. Congress Has Provided Additional Authority to Allow the Government to Collect Post-Cut-Through Digits Under FISA. (U) 59
- D. The Canons of Statutory Construction Favor the Government's Authority to Record or Decode Post-Cut-Through Digits, Particularly in the FISA Context. (U) 61
 - 1. No Clause or Word Should be Rendered Superfluous. (U) 62
 - 2. The Doctrine Against Implied Repeals (U) 65
 - 3. The Canon of Constitutional Avoidance (U) 67

~~SECRET~~

~~SECRET~~

E. The Recording and Decoding of Post-Cut-Through
Digits, With a Restriction on the Use of Content
Digits Except in Rare, Emergency Circumstances, is
Reasonable Under the Fourth Amendment. (U) 70

IV. CONCLUSION (U) 75

VERIFICATION (U) 76

~~SECRET~~

~~SECRET~~

The United States respectfully submits this Memorandum of Law in response to this Court's Supplemental Order, dated June 18, 2009, directing the government to make a written submission regarding the acquisition of post-cut-through digits pursuant to pen register orders under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 et seq. (FISA), including: (1) a description of whether and to what extent technology that is now reasonably available to the government can distinguish between content and non-content post-cut-through digits prior to acquisition, to include an explanation of whether such capabilities vary from case to case; and, if such technology does not currently exist, a description of what efforts are being made by the government to develop such technology; and (2) a discussion of the legal issues presented in light of current technology and several opinions cited in footnote 3 of the Court's Order. Docket No. PR/TF 09-36, 37, 38, Order at 2 n. 3. This verified memorandum of law addresses the information requested by the Court and provides the Court with additional information regarding enhanced protections

[Redacted]

b3 Per FBI
b7E

The government respectfully requests that this Court continue to authorize the recording and decoding of post-cut-

~~SECRET~~

through digits pursuant to FISA pen register orders because: (1) the plain language and legislative history of the relevant statutory provisions compel the conclusion that the government is permitted to acquire post-cut-through digits through a FISA pen register order; (2) cases denying the recording and decoding of post-cut-through digits in connection with a pen register are based on flawed analyses and have been decided under the criminal pen register statute rather than FISA, which includes even broader statutory authorization to acquire associated routing or transmission information; (3) the relevant canons of statutory construction support an interpretation of the pen register statute allowing the recording and decoding of post-cut-through digits; and (4) the recording and decoding of post-cut-through digits, with a restriction on the use of incidentally-acquired content digits except in rare, emergency circumstances, is reasonable under the Fourth Amendment. ~~(S)~~

I. **BACKGROUND: THE 2006 MEMORANDA AND REPORT** ~~(S)~~

On May 23, 2006, the government filed with this Court, a Verified Memorandum of Law (May 2006 Memorandum) advising the Court about the government's collection of post-cut-through digits through pen register surveillance under FISA and explaining why such collection is necessary and

b3 Per FBI
b7E

~~SECRET~~

~~SECRET~~

lawful.¹ In that memorandum, the government advised the Court that no technology exists that would permit the FBI to distinguish, at the acquisition point, between content and non-content post-cut-through dialed digits, and then record or decode only the non-content digits. See May 2006 Mem. at 3. The government asserted that the definition section of the criminal pen register statute, 18 U.S.C. section 3127(3), authorizes the government to collect non-content dialing, routing, addressing, or signaling digits dialed by a targeted telephone, and that the limitation provision, 18 U.S.C. section 3121(c), allows the government, in light of its technological limitations, to incidentally collect digits that may be dialed to transmit content.² May 2006 Mem. at 6-9. The government also reported

¹ "Post-cut-through digits" is a term of art that refers to digits dialed from a targeted telephone number 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 information), such as when a caller dials a toll free number to connect to a service provider (e.g., 1-800-CALL-ATT), then after the initial call is connected to the service provider, enters an account number and another phone number, which is the ultimate call destination. 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 enters a bank account or prescription number. In either case, the digits are sequences of numbers. See May 2006 Mem. at 1-2: (S)

² As explained in the government's May 2006 Memorandum, FISA authorizes the Court to issue orders approving the installation and use of pen registers and provides that "the term[] 'pen register' . . . ha[s] the meaning[] given such term[] in Section 3127 of Title 18, United States Code." 50 U.S.C. § 1841(2). Section 3121(c) applies

~~SECRET~~

~~SECRET~~

that it would make no affirmative investigative use of any incidentally captured content post-cut-through digits, except in rare cases in order to prevent an immediate danger of death, serious physical injury, or harm to the national security. May 2006 Mem. at 11-13. (S)

Shortly after the government filed its May 2006 Memorandum, on July 19, 2006, the Honorable Steven Wm. Smith, a Magistrate Judge from the Southern District of Texas, denied an application to acquire post-cut-through digits through the use of a criminal pen register under 18 U.S.C. section 3127(3). In re Application of the United States, 441 F. Supp. 2d 816 (S.D. Tex. 2006). Noting that the legal analysis in the government's May 2006 Memorandum rested in part on reasoning rejected by Magistrate Judge Smith, on July 27, 2006, the Honorable Colleen Kollar-Kotelly, then-presiding judge of this Court, ordered the government to submit a written brief "discussing how, if at all, Magistrate Judge Smith's opinion affects the government's analysis of this issue as set forth in its [May 26, 2006] Memorandum." Docket No. PR/TT 06-79, Order at 2 (FISA Ct. July 27, 2006). In response, on September 25, 2006, the government

in the FISA context because FISA pen registers are authorized under "this chapter," i.e., Chapter 206 of Title 18, 18 U.S.C. § 3121(a). May 2006 Mem. at 6, 9. (S)

~~SECRET~~

~~SECRET~~

provided a legal analysis (September 2006 Memorandum) of Magistrate Judge Smith's opinion, describing its misreading of statutory plain language and legislative history and its misapplication of various canons of statutory construction. The government submitted that this Court should decline to follow Magistrate Judge Smith's opinion, and noted that it has no precedential value for this Court.³ Following the filing of the September 2006 Memorandum, this Court continued to approve pen register applications including requests for authority to record and decode all post-cut-through digits. (S)

On August 7, 2006, Judge Kollar-Kotelly ordered the government to submit a report discussing: (1) how the government is implementing its obligation to make no affirmative investigative use of post-cut-through digits that do not constitute call dialing, routing, addressing or signaling information, except in a rare case to prevent an immediate danger of death, serious physical injury, or harm to the national

³ See Sept. 2006 Mem. at 7, n. 4. See, e.g., Browne v. McCain, 611 F. Supp. 2d 1062, 1072 (C.D. Cal. 2009) (case from another district factually distinguishable and does "not have binding precedential effect"); Irvine v. 233 Skydeck, LLC, 597 F. Supp. 2d 799, 803 (N.D. Ill. 2009) (a published case from another district "is not controlling authority and decisions of other district courts are entitled to no more weight than their intrinsic persuasive merits.") (internal quotations and citation omitted). Likewise, the other opinions cited in footnote 3 of this Court's June 18, 2009, Order also are not binding on this Court. (S)

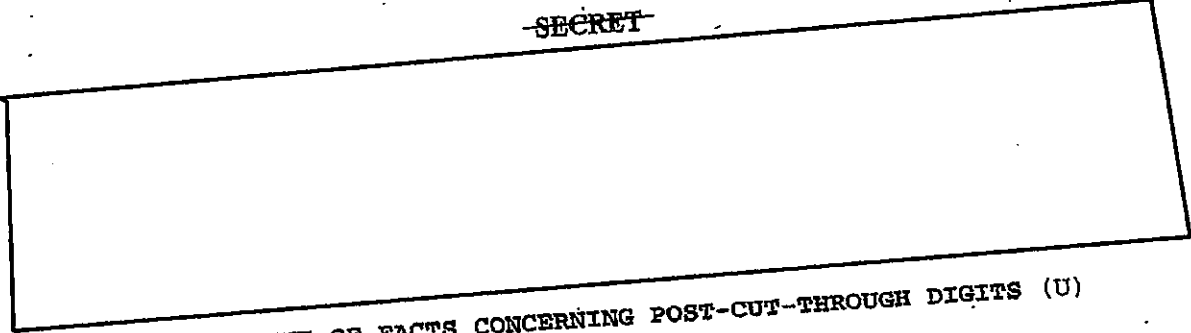
~~SECRET~~

~~SECRET~~

b3 Per FBI
b7E Per FBI

security

~~SECRET~~

~~SECRET~~b3 Per FBI
b7E
II. STATEMENT OF FACTS CONCERNING POST-CUT-THROUGH DIGITS (U)

The government submits that there continues to be no reasonably available technology that permits a service provider to identify and segregate content post-cut-through digits prior to delivery to the government. There is also no reasonably available technology that permits the government, upon receipt of this information and without further analysis, to determine whether the acquired digits represent content. The government believes that it is unlikely that such technology will be available in the foreseeable future. Therefore, the government has continued to develop policies and procedures to restrict the collection and improper use of any incidentally collected content post-cut-through digits. ~~(S)~~

A. There is No Technology Reasonably Available to the Government That Can Distinguish Between Content and Non-Content Post-Cut-Through Digits Prior to Acquisition. (U)

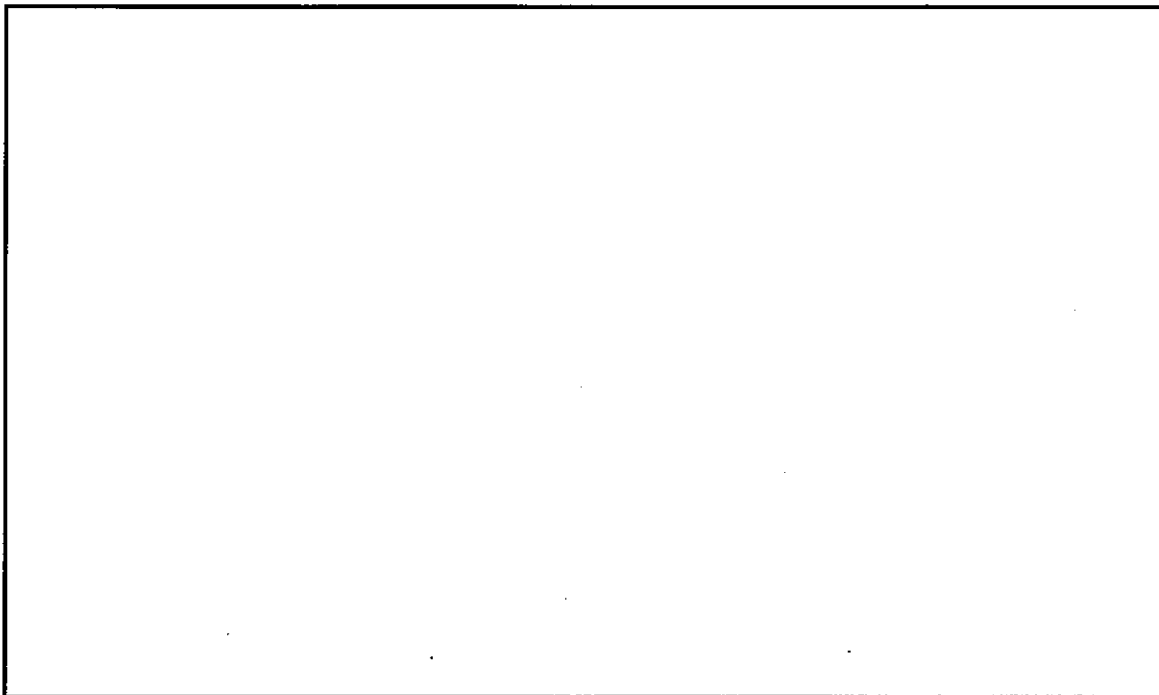
The current architecture and complexity of the global telecommunications network creates tremendous challenges for separating content post-cut-through digits from non-content

~~SECRET~~

~~SECRET~~

dialing, routing, addressing and signaling information in real
time.

b3 Per FBI
b7E



⁴ Call-identifying information is defined as "dialing or signaling information that identifies the origin, direction, destination, or termination of each communication generated or received by a subscriber by means of any equipment, facility, or service of a telecommunications carrier." 47 U.S.C. § 1001(2). (U)

⁵ The Communications Assistance for Law Enforcement Act of 1994, Pub.L. No. 103-414, 108 Stat. 4279 (1994) (hereinafter CALEA) was enacted to ensure that law enforcement maintained its interception capabilities in light of emerging technologies and the changing competitive telecommunications market. Overall, CALEA sought to balance three key policies: (1) to preserve a capability for law enforcement agencies to carry out properly authorized intercepts; (2) to protect privacy in the face of increasingly powerful and personally revealing technologies; and (3) to avoid impeding the development of new communications services and technologies. See H.R. Rep. No. 103-827(I) (1994), reprinted in 1994 U.S.C.C.A.N. 3489. (U)

~~SECRET~~

~~SECRET~~b3 Per FBI
b7E Per FBI

B. Because of the Limitations of Available Technology, the Government Has Developed Policies and Procedures to Restrict the Collection and Unauthorized Use of Post-Cut-Through Digit Content. (U)

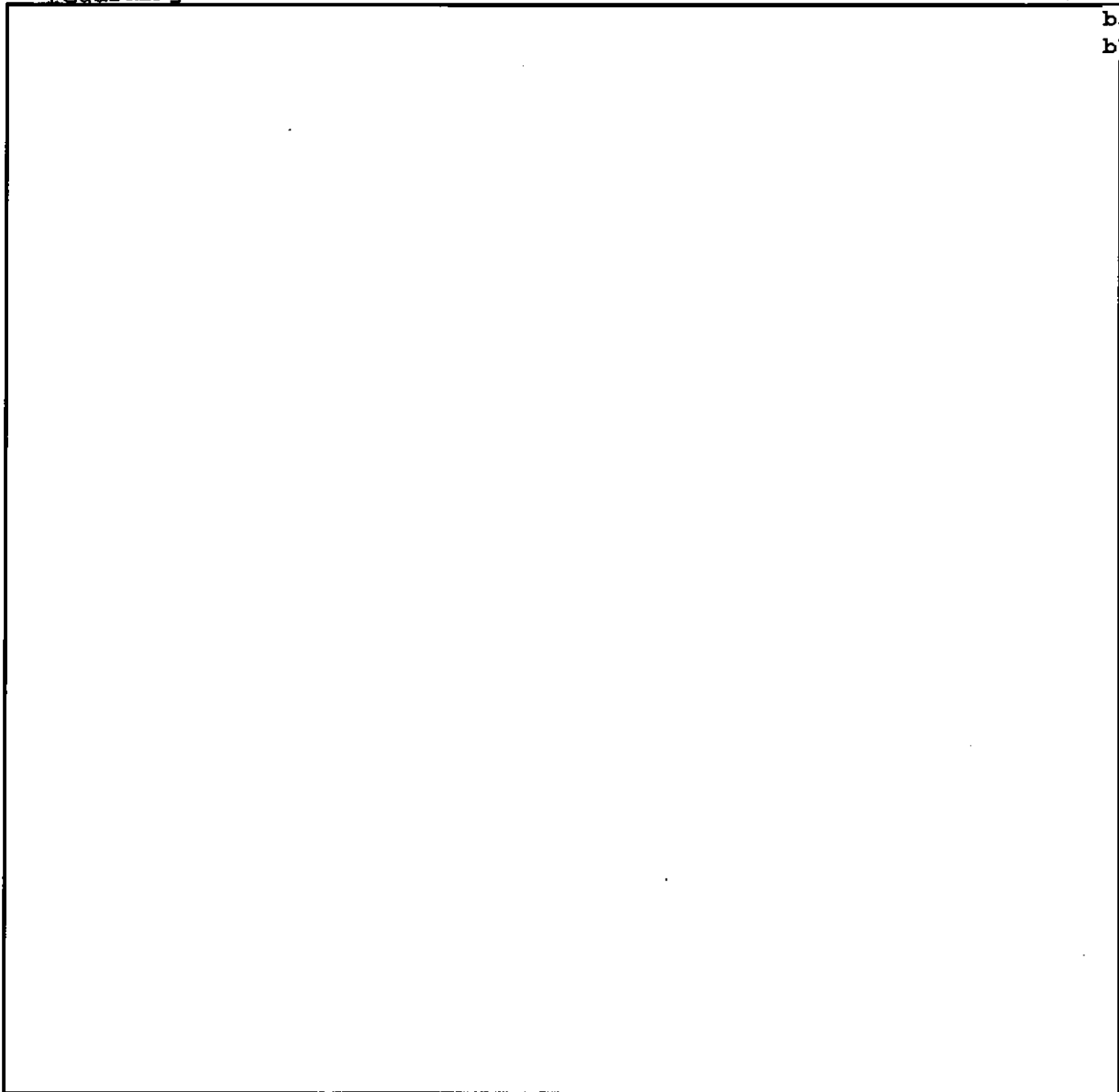
The government recognizes the concerns regarding the collection of content through the operation of pen registers and has taken extraordinary steps to restrict the collection and use of content post-cut-through digits. On May 24, 2002, then Deputy Attorney General Larry D. Thompson issued a memorandum (the "DAG Memo" (attached hereto as Ex. A)) to all Department of Justice components setting forth the Department's policy regarding the avoidance of "over-collection" in the use of pen registers and trap and trace devices that are deployed under the authority of 18 U.S.C. § 3121, et seq.¹⁵ The memorandum requires that reasonably available technology be used to avoid over-collection and, if over-collection does occur despite the use of reasonably available technology, no affirmative investigative use be made of that information except to prevent immediate danger of death.

¹⁵ The DAG Memo specifically states, "The authorities granted by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, et seq., are outside the scope of this Memorandum." DAG Mem. at 1, n. 1. As discussed below, the FBI has since enacted policies that apply the principles of the DAG Memo to post-cut-through digits collected pursuant to a pen register authorized under FISA. (U)

~~SECRET~~

~~SECRET~~

serious physical injury, or harm to the national security. These principles continue to reflect the policy of the government regarding the collection and use of post-cut-through digits. (U)

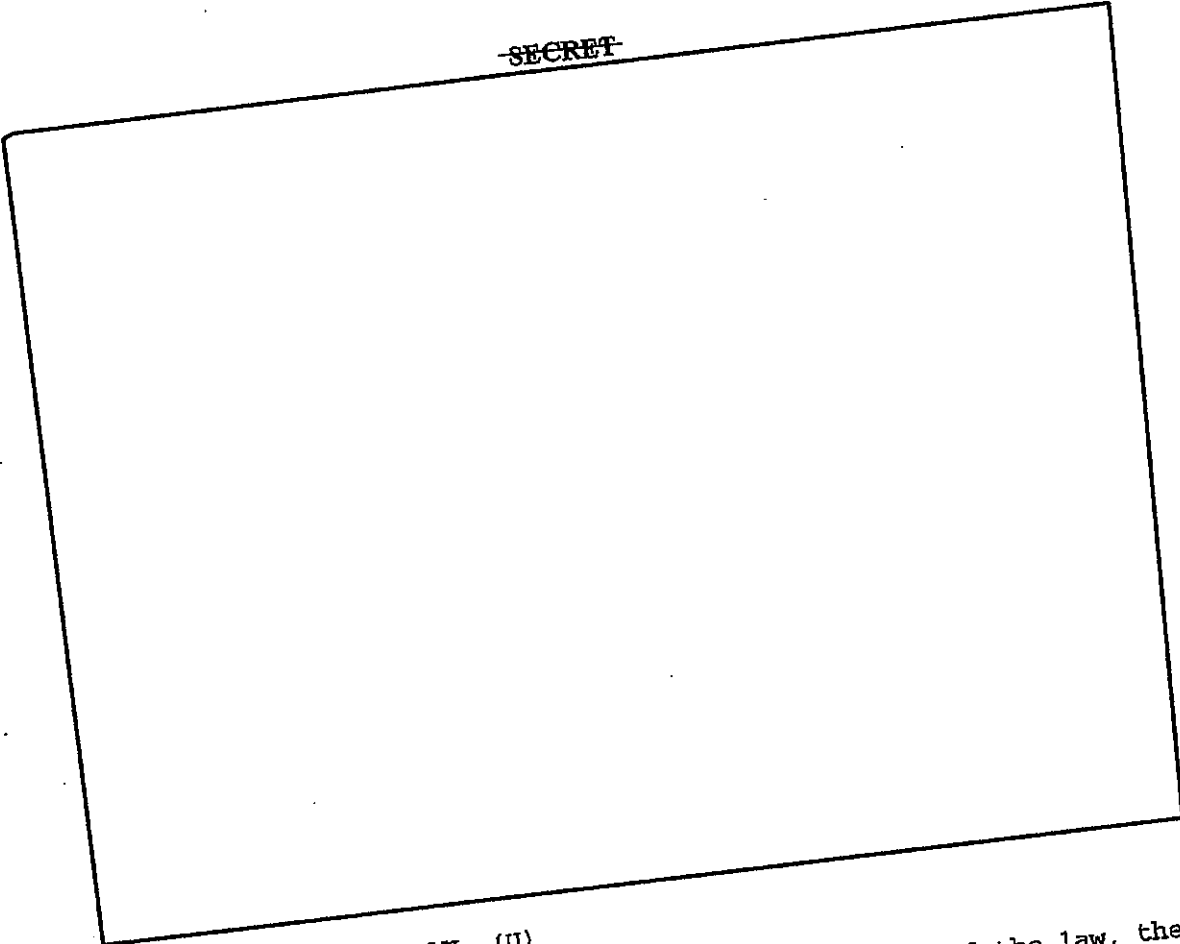


b3 Per FBI
b7E Per FBI

~~SECRET~~

~~SECRET~~

b3 Per FBI
b7E Per FBI



III. ANALYSIS OF LAW (U)

In light of the current state of technology and the law, the government respectfully submits that it is appropriate for this Court to continue to approve pen register applications including requests for authority to record and decode all post-cut-through digits. As set forth in detail below, 18 U.S.C. sections 3121(c) (the limitation provision of the pen register statute) and 3127(3) (the pen register definition) authorize the government to collect non-content post-cut-through digits, and incidental to

~~SECRET~~

~~SECRET~~

the collection of such non-content information, to record and/or decode (but not use except in a specified set of exigent circumstances) digits that constitute "content," if technology that would prevent such incidental collection is not reasonably available. This authority is augmented for pen register collections made pursuant to FISA, which includes enhanced authorities to collect post-cut-through digits. (U)

Furthermore, the government respectfully submits that the Court should not deny the recording or decoding of post-cut-through digits based on any of the opinions denying such collection cited in footnote 3 of the Court's June 18, 2009 Order.¹⁹ As noted above, none of those opinions is binding on

¹⁹. See June 18, 2009 Order at 2-3, n. 3 (citing In re Application of the United States, No. 08-MC-595 (JO), 2008 WL 5255815 (E.D.N.Y. Dec. 16, 2008) (Magistrate Judge Orenstein) (Orenstein Opinion) (attached hereto as Ex. C); In re Applications of the United States, 515 F. Supp. 2d 325 (E.D.N.Y. 2007) (Magistrate Judge Azrack) (Azrack Opinion), aff'd Nos. 06-mc-547, 06-mc-561, 07-mc-120, 07-mc-400 (E.D.N.Y. Dec. 17, 2007) (District Judge Gleeson) (summary affirmance); In re Application of the United States, Misc. No. H-07-613, 2007 WL 3036849 (S.D. Tex Oct. 17, 2007) (District Judge Rosenthal) (Rosenthal Opinion) (attached hereto as Ex. D); In re Application of the United States, 441 F. Supp. 2d 816 (S.D. Tex. 2006) (Magistrate Judge Smith) (Smith Opinion) (discussed above in the context of the September 2006 memorandum); In re Application of the United States, No. 6:06-mj-1130 (M.D. Fla. May 23, 2006) (Magistrate Judge Spaulding) (Spaulding Opinion) (attached hereto as Ex. E), aff'd No. 6:06-mj-1130 (M.D. Fla. June 20, 2006) (District Judge Conway) (Conway Opinion) (attached hereto as Ex. F)). In addition, footnote 3 quotes the D.C. Circuit's opinion in United States Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000). That case merely noted, however, that "no court has of yet considered the contention" of how to interpret 18 U.S.C. section 3121(c). Id. Finding that the F.C.C.

~~SECRET~~

~~SECRET~~

this Court. In addition, each opinion analyzes collection of post-cut-through digits in the context of a criminal pen register and Title 18, not in the context of FISA. Finally, the varying analyses in all the opinions are flawed. (U)

A. The Plain Text of the Pen Register Statute Authorizes the Government Incidentally to Record or Decode Content Post-Cut-Through Digits In Order to Collect Call Processing Information. (U)

1. As Originally Adopted, 18 U.S.C. Sections 3127(3) and 3121(c) Contemplated the Collection of All Post-Cut-Through Digits. (U)

Congress initially adopted the definition of "pen register" as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 302, 100 Stat. 1848 (ECPA). As originally enacted, 18 U.S.C. section 3127(3) defined "pen register" in terms of now out-dated telephone technology, referring to a "device" being attached to a "telephone line." Specifically, the earlier version of the pen register definition provided:

[T]he term "pen register" means a device which records or decodes electronic or other impulses which identify the number dialed or otherwise transmitted on the telephone line to which such device is attached

18 U.S.C. § 3127(3) (2000). (U)

was under an obligation to perform a reasoned analysis of the privacy impacts of its rule, the D.C. Circuit remanded to the agency. *Id.* at 462-63. As such, the court did not address the issue of how to interpret section 3121(c), and its observations, which were made in the context of Title III, not FISA, are dicta. (U)

~~SECRET~~

~~SECRET~~

The definition of "pen register" remained unaltered until 2001, but in the interim in 1994 Congress enacted CALEA (discussed above) and added the "limitation" provision of the criminal pen register statute, 18 U.S.C. § 3121(c). As originally enacted, this provision stated:

(c) Limitation - 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 (emphasis added). The limitation provision makes clear that although the purpose of a pen register is to collect "dialing and signaling information" utilized in call processing, Congress recognized that such devices have the ability to record or decode other information. (U)

Having recognized the potential for pen register devices to collect other information, including content, Congress drafted a legislative solution. That solution, embodied in the text of section 3121(c), mediates between the government's need for non-content post-cut-through digits and the possibility that content of this provision requires the government to use, in conjunction with pen register devices, "technology reasonably available to it" in order to "restrict[] the recording or decoding" to

SECRET

~~SECRET~~

"dialing and signaling information" (i.e. digits) "utilized" to connect calls. By modifying the word "technology" with the words "reasonably available to it," Congress recognized that it may not be possible to prevent the recording of some content digits at the collection point, and demonstrated its intent to allow the incidental recording of content when such technology is not "reasonably available." Indeed, as discussed more fully below, any other reading of this provision would render the words "reasonably available to it" superfluous in violation of the simple rule of statutory construction that all words of a statute be given meaning, if possible.²⁰ Congress deliberately chose to make the "reasonable availability" of filtering "technology" the cornerstone of the limitation provision, knowing that the existence of such technology was not assured. (U)

2. Amendments to 18 U.S.C. Sections 3127(3) and 3121(c) by the PATRIOT Act Further Support the Collection of All Post-Cut-Through Digits. (U)

In 2001, section 216 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, § 216, 115

²⁰ See TRW, Inc. v. Andrews, 534 U.S. 19, 31 (2001) (citation omitted) ("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."). (U)

~~SECRET~~

~~SECRET~~

Stat. 272, 288 (2001) (PATRIOT Act) amended both the definition of pen register in section 3127(3) and the limitation provision in section 3121(c). PATRIOT Act § 216, 115 Stat. at 288, 290. The PATRIOT Act amended the definition of pen register to clarify that the pen register provision applies to an array of modern communications technologies (e.g., 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 current definition of pen register now states, in pertinent part:

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

18 U.S.C. § 3127(3) (emphasis added). Thus, Congress amended the pen register definition in only two respects, both of which merely clarified the limits of existing law: (1) Congress broadened the language to include the recording or decoding of "dialing, routing, addressing or signaling information" in order to confirm the statute's proper application to communications in an advanced electronic environment; and (2) Congress confirmed the proper purpose and scope of a pen register device: to obtain

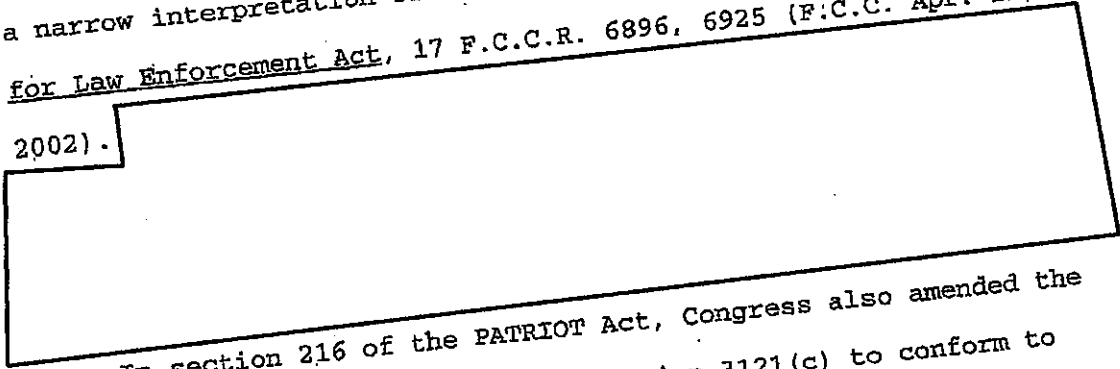
~~SECRET~~

~~SECRET~~

information used to process a wire or electronic communication, but not to obtain the "contents" of such communication. (U)

Importantly, in amending 18 U.S.C. section 3127(3), Congress clearly intended that through a pen register device, the government can lawfully obtain all non-content information -- "dialing, routing, addressing, or signaling information" -- transmitted by a targeted telephone. Accordingly, the plain language of the pen register definition specifically authorizes the government to record or decode those post-cut-through digits that "simply route the call to the intended party and are, therefore, unquestionably call-identifying information even under a narrow interpretation of that term." In re Commc'ns Assistance for Law Enforcement Act, 17 F.C.C.R. 6896, 6925 (F.C.C. Apr. 11,

2002).



In section 216 of the PATRIOT Act, Congress also amended the limitation provision in 18 U.S.C. section 3121(c) to conform to the revised language of the pen register definition. The amended 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

b3 Per FBI
b7E

~~SECRET~~

~~SECRET~~

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). Congress made essentially the same revisions to the limitation provision that it made to "the pen register definition: (1) it clarified that the term "pen register" applies not only to traditional telephone lines, but to all manner of modern electronic communications; and (2) it clarified that the purpose of a pen register is to collect call processing information, not to collect content. Congress left untouched the statement that the government "shall use technology reasonably available to it" to "restrict[]" recording or decoding to the digits "utilized" in call "processing." (U)

Accordingly, as reflected by the plain text, Congress left intact the scheme it had previously adopted in 1994. As long as filtering technology is not reasonably available, the government may record or decode all post-cut-through digits. As was true before the PATRIOT Act, if a pen register records or decodes information that includes the "contents of any wire or electronic communications," that information falls outside the definition of pen register and therefore outside the scope of output that the government may use. (U)

~~SECRET~~

~~SECRET~~

On their face, neither the original versions of the pen register definition and limitation provision nor the revised versions as amended by the PATRIOT Act dictate the means by which a pen register device should function technologically. By its own terms, 18 U.S.C. section 3127(3) is simply a definition. Notably, section 3127 is entitled "Definitions for Chapter." It is 18 U.S.C. section 3121, not section 3127, that sets forth the "general prohibition on pen register and trap and trace device use." Significantly, subparagraph (c) of this "prohibition" section, entitled "limitation," does not prohibit content collection outright, but only requires that the government use "technology reasonably available to it" to restrict the recording or decoding of digits to information used in call processing. 18 U.S.C. § 3121(c). (U)

3. The Opinions Denying Collection of Post-Cut-Through Digits Under the Criminal Pen Register Statute Interpret the Definition of Pen Register in Isolation, Resulting in a Strained "Plain Meaning" of the Text. (U)

Five of the six opinions denying collection of post-cut-through digits under a criminal pen register and cited in footnote 3 of the Court's June 18, 2009 Order, the Orenstein Opinion, the Spaulding Opinion, the Conway Opinion, the Rosenthal Opinion, and the Smith Opinion, base, at least primarily, their

~~SECRET~~

~~SECRET~~

holdings on the purported plain language of the criminal pen register statute but fail to give full weight to the language in the limitation provision at 18 U.S.C. section 3121(c). Two of the opinions rely on the purported plain text of the pen register definition, 18 U.S.C. section 3127(3), standing alone. See Orenstein Op., 2008 WL 5255815, at *3 (finding that "the [criminal pen register] statute . . . makes it unlawful for a pen register itself to record the contents of a communication"); Spaulding Op., No. 6:06-mj-1130 at 2 ("Congress was clear that the content of communications cannot be captured by use of pen register and trap and trace devices."). These two opinions fail to incorporate the language of section 3121(c). The Orenstein Opinion summarily declined to consider its relevance;²¹ the Spaulding Opinion failed to mention it, other than to note that no technology is reasonably available to filter content from non-content post-cut-through digits. See Orenstein Op. at *3; Spaulding Op. at 2. (U)

These opinions' reliance on the definition of pen register,

²¹ The Orenstein Opinion characterized the basis of its holding as a "narrow matter of statutory interpretation" of 18 U.S.C. section 3127(3), 2008 WL 5255815, at *3, and expressly declined to discuss the relevance of section 3121(c), finding that the government's interpretation of that provision "ha[d] been rejected" and that the government "ha[d] not sought to resuscitate it here." Id. at *3 n.7 (citing the Smith Op. at *7-*9; Azrack Op., 515 F. Supp. 2d at 334-35). (U)

~~SECRET~~

~~SECRET~~

divorced from the remainder of the statutory language, plainly contradicts the "cardinal rule that a statute is to be read as a whole, since the meaning of statutory language, plain or not, depends on context." King v. St. Vincent's Hosp., 502 U.S. 215, 221 (1991) (citing Massachusetts v. Morash, 490 U.S. 107, 115 (1988)). By disposing of the statutory language of section 3121(c) in a footnote, without any attempt to integrate the language into its interpretation, the Orenstein Opinion's reading of the criminal pen register statute is incomplete. This is especially true where, as here, the definition relied upon by Judge Orenstein was amended in precisely the same section of the PATRIOT Act, section 216, as the passage he insists requires no consideration. Likewise, the Spaulding Opinion's failure even to discuss the limitation provision undermines its plain reading of the text. As described above, Congress had every opportunity to remove the words "technology reasonably available" from the limitation provision, but elected instead to retain them. (U)

The Conway Opinion, affirming the Spaulding Opinion, references section 3121(c) but fails to give it its proper weight. Instead, Judge Conway concludes that Judge Spaulding correctly interpreted section 3127(3) as "flatly prohibiting the interception of communication content by pen registers" and that

~~SECRET~~

~~SECRET~~

"[t]he statute seems plain in that respect." Conway Op. at 5. Judge Conway dismisses section 3121(c) as an "additional privacy safeguard," failing to give any meaning to the words "technology reasonably available." Id. (U)

Similarly, the Rosenthal Opinion relies on an isolated interpretation of the pen register definition in section 3127(3) in concluding that "the prohibition on the collection of content is clear," Rosenthal Op., 2007 WL 3036849 at *7. The Rosenthal Opinion dismisses 3121(c) as "a supplement to the Government's obligation not to collect contents with a pen register." Id. at *8. Although Judge Rosenthal suggests that her interpretation reconciles the text of the limitation provision with the definition of "pen register," it does so only at the expense of the plain text of section 3121(c). It ignores the "technology reasonably available" language. Furthermore, Judge Rosenthal's conclusion that section 3121(c) is a "supplement" to the proscription on content in the pen register definition confuses the history of those provisions. As discussed above, the limitation provision of section 3121(c), including the "technology reasonably available" language, was enacted in CALFA in 1994; the definition of pen register was not revised to expressly refer to content until the PATRIOT Act in 2001, at which time corresponding amendments were made to section 3121(c),

~~SECRET~~

~~SECRET~~

but the technology reasonably available language was left intact. Rather than act as a "supplement," the limitation provision was intended to perform an independent statutory function apart from the pen register definition. (U)

Although it discusses canons of statutory construction and legislative history, the Smith Opinion also moors its holding in the plain language of the pen register statute without giving meaning to all of the language. Smith Op., 441 F. Supp. 2d at 823-26. Magistrate Judge Smith determined that the last sentence of the pen register definition is an "unqualified proscription" against content. *Id.* at 823-25. If anything, this "proscription" simply excludes "content" from what is defined as a pen register. Moreover, the Smith Opinion fails to consider the full text of section 3121(c). Magistrate Judge Smith concludes that section 3121(c) "imposes an affirmative obligation ('shall use technology') upon a law enforcement agency" authorized to install and use a pen register. *Id.* at 824. In so doing, he ignores the "reasonably available" caveat. (U)

Unlike the five opinions discussed above, the Azrack Opinion found the language of the statute ambiguous. *See* Azrack Op., 515 F. Supp. 2d at 332 (finding that while the pen register definition on its own is unambiguous, the language of section

~~SECRET~~

~~SECRET~~

3121(c) "clouds this lucidity"). While this conclusion at least acknowledges both the definition and limitation provisions, it fails to give each its proper weight. The government respectfully submits that the plain-language reading described in sections A.1 and A.2 above successfully gives meaning to each of the statutory provisions without ignoring any portion of the statutory text. (U)

B. The Legislative History of the Criminal Pen Register Statute Confirms that Congress Intended to Allow the Incidental Recording or Decoding of Content Post-Cut-Through Digits. (U)

1. Legislative History Regarding the Enactment of 18 U.S.C. Section 3121(c) Confirms that Congress Intentionally Created a Technology-Driven Minimization Scheme. (U)

Legislative history from the 1994 enactment of the pen register limitation provision confirms what the text of 18 U.S.C. section 3121(c) plainly implies. In 1994, Senator Leahy originally proposed 18 U.S.C. section 3121(c) as part of S.2375, the "Digital Telephone Act of 1994." See 140 Cong. Rec. S11,045-05 (1994). Most of the provisions of S.2375, including section 3121(c), were eventually adopted in CALRA. In his introductory remarks, Senator Leahy included a section-by-section summary in which he stated as follows regarding the limitation provision:

~~SECRET~~

~~SECRET~~

[This subsection] requires 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. S11,045-05 (emphasis added). Thus, Senator Leahy, the primary architect of section 3121(c), stated that the government was required to apply filtering technology only "when" such technology is reasonably available. When it is not, the government is permitted to "otherwise capture" content post-cut-through digits.²² (U)

In addition to Senator Leahy's statement, committee reports from both the House and Senate further confirm that Congress originally intended to permit the government incidentally to record or decode post-cut-through digits that may be content. Specifically, both reports state that 18 U.S.C. 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; H.R. Rep. No. 103-

²² Because he was the chairman of the committee that sponsored the bill, Senator Leahy's remarks are entitled to significant weight. See United States v. Int'l Union (UAW-CIO), 352 U.S. 567, 585 (1957). In this case, they are entitled to even greater weight, because both the Senate and House committee reports accompanying CALEA adopted Senator Leahy's above remark verbatim. See S. Rep. No. 103-402, at 31 (1994); H.R. Rep. No. 103-827(I), at 32 (1994). (U)

~~SECRET~~

~~SECRET~~

827(I), at 17 (emphasis added). Well in advance of the 1994 enactment of this provision, the term "minimize" had acquired a specific legal meaning under the electronic surveillance laws of both Title III, enacted in 1968, and FISA, enacted in 1978. (U)

For example, 18 U.S.C. section 2518(5) of Title III provides, in relevant part, that electronic surveillance "be conducted in such a way as to minimize the interception of communications not otherwise subject to interception" under Title III. Under well-established precedent, Title III "does not forbid the interception of all nonrelevant conversations, but rather instructs 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). (U)

Similarly, under FISA, each application for electronic surveillance submitted by the government must contain, among other things, a statement of the government's proposed minimization procedures. 50 U.S.C. § 1804(a)(5). FISA defines "minimization procedures," in part, as follows:

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

~~SECRET~~

~~SECRET~~

disseminate foreign intelligence information.

50 U.S.C. § 1801(h)(1). Both federal case law and FISA legislative history demonstrate that the definition of minimization procedures under FISA was intended to 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 an investigation develops over time. See, e.g., United States v. Rahman, 861 F. Supp. 247, 253 (S.D.N.Y. 1994), aff'd on other grounds, 189 F.3d 88 (2d Cir. 1999) (rejecting the notion that the "wheat" could be separated from the "chaff" while the "stalks were still growing"). In addition, the Senate Select Committee on Intelligence observed in its final report regarding FISA that in certain situations, "primarily for technological reasons, it may not be possible to avoid acquiring all conversations. In these situations, minimizing at the retention and dissemination stages becomes most important." S. Rep. No. 95-701, at 40 (1978) (Senate Intelligence Report). See In the Matter of Kevork, 634 F. Supp. 1002, 1017 (C.D. Cal. 1985) (stating that "minimization may occur at any of several stages"), aff'd on other grounds, 788 F.2d 566 (9th Cir. 1986). (U)

When drafting 18 U.S.C. section 3121(c) and its associated legislative history, Congress undoubtedly knew the legal meaning

~~SECRET~~

~~SECRET~~

that the term "minimize" had acquired under Title III and FISA, electronic surveillance laws that had, at the time, existed for many years and in the case of Title III nearly three decades. In any event, Congress is presumed, as a matter of law, to have known the legal meaning of that word. See United States v. Bonanno Organized Crime Family, 879 F.2d 20, 25 (2d Cir. 1989), relying on Goodyear Atomic Corp. v. Miller, 486 U.S. 174, 184-85 (1988) (As a matter of law, Congress is presumed to have been (a) knowledgeable about existing laws pertinent to later-enacted legislation, (b) aware of judicial interpretations given to sections of an old law incorporated into a new one, and (c) familiar with previous interpretations of specific statutory language.). (U)

Although Congress used the word "minimize" in the legislative history rather than in section 3121(c) itself, it is reasonable to infer, under the authorities cited above, that in describing the requirement of section 3121(c) as one of minimization, Congress made clear its intent that the government may acquire information falling outside the scope of a pen register (i.e., content) when such recording or decoding is a necessary incident of capturing all call processing information. Minimization of this non-pen register information can occur after acquisition. The government's and FBI's above-described policies

~~SECRET~~

~~SECRET~~

and procedures accomplish such post-acquisition minimization. (U)

2. The Legislative History of Section 216 of the PATRIOT Act Confirms that Congress Intended to Preserve the Post-Cut-Through Digits Minimization Scheme Created in 1994.. (U)

When it enacted the PATRIOT Act, as described below, Congress was aware that no post-cut-through digit filtering technology was reasonably available and yet left unchanged the minimization scheme under which the government may record or decode dialed digit content incidental to the recording or decoding of non-content, until such time as filtering technology is reasonably available. Indeed, the legislative history confirms what is suggested by the plain language of section 216 itself: that the amendments were meant to clarify that pen registers apply to a broad array of modern technologies and to reinforce that the existing content limitations continued to apply to these new technologies. (U)

Although the PATRIOT Act has no definitive congressional committee report, on October 11, 2001, the House Judiciary Committee reported on a predecessor bill, H.R. 2975, that proposed updating the language of sections 3127(3) and 3121(c) to confirm that pen registers apply to communications instruments other than traditional telephones:

[T]he section clarifies that orders for the installation of

~~SECRET~~

~~SECRET~~

pen register and trap and trace devices may obtain any non-content information - "dialing, routing, addressing, and signaling information" - utilized in the processing or transmitting of wire and electronic communications. Just as today, such an order could not be used to intercept the contents of communications protected by the wiretap statute. The amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in Smith v. Maryland, 442 U.S. 735, 741-43 (1979). Thus, for example, an order under the statute could not authorize the collection of email subject lines, which are clearly content. Further, an order could not be used to collect information other than "dialing, routing, addressing, and signaling" information, such as the portion of a URL (Uniform Resource Locator) specifying Web search terms or the name of a requested file or article.

H.R. Rep. No. 107-236(I), at 53 (emphasis added); see also Id. at 52 ("This section updates the language of the statute to clarify that the pen/register authority applies to modern communications technologies."). This report, which does not mention post-cut-through-digits, reveals that H.R. 2975 was focused on ensuring that the pen register statute applied to modern communications technologies, such as e-mail, while also ensuring that it was not being changed to allow the interception of content from such technologies. (U)

Similar statements were made regarding a predecessor bill in the Senate, the Uniting and Strengthening America Act, S. 1510, which included a section 216 identical in relevant part to the one soon thereafter enacted in the PATRIOT Act. See generally

~~SECRET~~

~~SECRET~~

147 Cong. Rec. S10,547-01, *S10,609 (Oct. 11, 2001).
 Contemporaneous comments about the legislation demonstrate that
 the amendments at issue were to ensure that pen registers apply
 to communications instruments other than traditional telephones.
 See 147 Cong. Rec. *S10,592 (Oct. 11, 2001) (Sen. Feinstein)
 ("[t]he problem with current law is that it has not kept up with
 technology"); 147 Cong. Rec. *S10,561, *S10,602 (Oct. 11,
 2001) (Sen. Hatch) ("[t]he legislation under consideration today
 would make clear what the federal courts have already ruled -
 that Federal judges may grant pen register authority to the FBI
 to cover, not just telephones, but other more modern modes of
 communication such as mail or instant messaging."). (U)

Contemporaneous statements about section 216 also make clear
 that its amendments were to ensure that pen registers apply to
 modern communications technologies aside from telephones. On
 October 25, 2001, Senator Leahy, the chairman of the Senate
 Judiciary Committee, appeared before the Senate and read final
 remarks about the Patriot Act, which were published in the
 Congressional Record. Senator Leahy observed: "[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.'" 147 Cong. Rec. S10,999 (daily ed. Oct. 25,
 2001). When considering the amendment to include "routing" and

~~SECRET~~

~~SECRET~~

"addressing" information among the data captured by a pen register, Senator Leahy expressed his concern that "the new terms might encompass matter considered content." 147 Cong. Rec. S11,000 (daily ed. Oct. 25, 2001) (emphasis added). To avoid this misinterpretation, he agreed to a provision in section 216 that "exclude[s] the use of pen/trap devices to intercept 'content'," although he stated that he would have preferred to see "these terms be defined" more clearly in the statute instead. Id. Thus, the restriction on acquisition of content codified in sections 3121(c) and 3127(3) was aimed at the expanded technologies subject to pen register authority - and ensuring that the "new" terms were not misinterpreted to change the nature of information a pen register order is used to collect. (U)

Senator Leahy's comments and analysis also clarify that section 216 does not alter the minimization scheme under which the government may record dialed digit content incidental to the recording of non-content, until such time as filtering technology is reasonably available. He acknowledged that he was aware that pen registers capture all electronic impulses transmitted by a targeted facility, that some impulses made after a call is connected could reflect content, and that there has been no change in technology that would better restrict pen register recording or decoding to call processing information only. 147

~~SECRET~~

~~SECRET~~

Cong. Rec. S11,000. Despite these facts, Senator Leahy also acknowledged that the "technology reasonably available" language in section 3121(c) remained in effect, noting that the statute "requires the government to use reasonably available technology that limits the interceptions under the pen-trap device laws 'so as not to include the contents of any wire or electronic communications.'" 147 Cong. Rec. S11,000. Similarly, his section-by-section analysis states that section 216 "further requires the government to use the latest available technology to insure [sic] that a pen register or trap and trace device does not intercept the content of any communications." 147 Cong. Rec. S11,007 (daily ed. Oct. 25, 2001). These repeated references to reasonably or latest available technology demonstrate that section 216 was not intended to be a departure from prior practice, including the minimization scheme created in 1994. (U)

3. The Opinions Denying Collection of Post-Cut-Through Digits Under the Criminal Pen Register Statute Misread the Legislative History. (U)

The two opinions cited in footnote 3 of the Court's June 18, 2009, Order that examine legislative history, the Smith and Azrack Opinions, misinterpret or take out of context a number of statements, particularly statements by Senator Leahy, and erroneously conclude that Congress intended to bar the use of pen register devices that could incidentally acquire content post-

~~SECRET~~

~~SECRET~~

cut-through digits. According to Magistrate Judge Smith, when Congress first codified the pen register statute under ECPA, it did not address the question of post cut-through digits, because "existing pen register technology in the 1980s did not allow over-collection of content" 441 F. Supp. 2d at 826. Magistrate Judge Smith asserted that Congress passed the CALEA "limitation" amendment to the pen register statute when it first became aware of the issue in 1994, and then, "acted again by inserting into the [PATRIOT] Act . . . three separate directives placing contents out of bounds for pen/trap devices." Id. In fact, the PATRIOT Act legislative history, though scant, proves just the opposite. As described above, Congress was aware that no post-cut-through digit filtering technology is reasonably available and yet left unchanged the minimization scheme under which the government may record dialed-digit content incidental to the recording of non-content, until such time as filtering technology is reasonably available. (U)

The Smith Opinion also takes and uses out of context portions of Senator Leahy's final remarks about the PATRIOT Act delivered on October 25, 2001 (described above). Magistrate Judge Smith quotes some of Senator Leahy's remarks and suggests that the Senator, "who had been instrumental in passing the CALEA 'reasonably available technology' limitation, declared on the

~~SECRET~~

~~SECRET~~

Senate floor that § 3121(c) had so far [at the time of the PATRIOT Act's enactment] not achieved its purpose of protecting dialed contents from collection by pen registers." Smith Op., 441 F. Supp. 2d at 821 (citing 147 Cong. Rec. S11,000). Magistrate Judge Smith further implied that Senator Leahy called for "judicial review" of the government's collection of post-cut-through digits, and that the addition of the phrase "so as not to include the contents of any wire or electronic communications" to 18 U.S.C. section 3121(c) was intended to stop the government from incidentally collecting content dialed digits. *Id.* (U)

To the contrary, Senator Leahy stated that his original proposal for the PATRIOT Act amendments to the pen register statute was threefold: (1) to give nationwide effect to pen register and trap and trace orders obtained by government attorneys and obviate the need to obtain identical orders in multiple federal jurisdictions; (2) to clarify that such devices can be used for computer transmissions to obtain electronic addresses, not just telephone lines; and (3) "as a guard against abuse," to provide for "meaningful judicial review" of government attorney applications for pen registers and trap and trace devices. 147 Cong. Rec. S10,999. Senator Leahy's third proposal was not adopted in the PATRIOT Act, and his comments regarding the FBI's failure to develop "filtering" technology to date were

~~SECRET~~

~~SECRET~~

directed at his disappointment that Congress had failed to include this third proposed amendment. (U)

In short, Senator Leahy had proposed that the criminal pen register application process should be subjected to heightened judicial review. Id. at S11,000. Currently, under the criminal pen register statute, the government must certify that the information likely to be obtained by the installation of a pen register device will be "relevant to an ongoing criminal investigation." Id. A court is required to issue an order upon seeing the certification and is not authorized to look behind the certification and evaluate the judgment of the prosecutor. Senator Leahy sought to amend this standard to require the government to include facts in its pen register certification. Id. Then, the court would grant the order only if it found that the facts supported the government's assertion of relevancy. Senator Leahy specifically stated that he sought this third amendment "due in significant part to the fact that pen/trap devices in use today collect 'content.'" Id. In other words, and as discussed above, Senator Leahy, like the rest of Congress, recognized that pen registers incidentally intercept some content and concluded that, because the government is incidentally collecting some content, heightened judicial review of the applications was necessary to ensure that the government was

~~SECRET~~

~~SECRET~~

properly using pen register orders. Id. A majority of Congress apparently did not agree with him, because this proposed amendment did not become law. Senator Leahy did not claim that under his proposed approach, or as amended by the PATRIOT Act, the criminal pen register statute would eliminate, or even curtail, the acknowledged status quo under which pen register devices capture all electronic impulses, non-content or otherwise, from the targeted facility. (U)

The Azrack Opinion also misinterprets or takes out of context numerous statements by Senator Leahy in its examination of the legislative history of the pen register statute, even though it ultimately concludes that "[l]egislative history fails to fully clarify the ambiguity created by the text of the [pen register statute]." Azrack Op., 515 F. Supp. 2d at 334. The Azrack Opinion acknowledges the presence of the term "minimize" in the legislative history of CALEA. Id. at 333 (citing S. Rep. No. 103-402, at 18; H.R. Rep. No. 103-827(I), at 17). Magistrate Judge Azrack agrees that "[v]iewed in isolation, particularly the word 'minimize,' these statements do appear to support the Government's theory." Azrack Op., 515 F. Supp. 2d at 333. Ultimately, however, she finds, based on Senator Leahy's 1994 statements on the Senate floor, that the legislative history of CALEA does not in the end support the government's

~~SECRET~~

~~SECRET~~

interpretation: "The bill [] protects privacy by requiring telecommunications systems to protect communications not authorized to be intercepted and by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information." Id. (quoting 140 Cong. Rec. 11,056 (Sen. Leahy)). Notably, this statement does not specifically refer to post-cut-through digits. Contrary to the Azrack Opinion, Senator Leahy's statements that the limitation provision is designed to restrict access to "transactional information" is consistent with the House and Senate Reports' expectation that the government would "minimize" such information. (U)

In turning to Leahy's comments regarding the PATRIOT Act amendments, the Azrack Opinion asserts that Leahy "worrie[d]" that there was "little or no guidance of what is covered by 'addressing' or 'routing,'" and notes his approval of the administration's willingness to "exclude the use of pen/trap devices to intercept 'content.'" Id. (citing 147 Cong. Rec. S11,000). The Azrack Opinion suggests that Leahy's "express concern that courts will erroneously grant the Government access to content with only pen register authorization" implies a total prohibition on even the incidental collection of post-cut-through digits. Id. (citing 147 Cong. Rec. S10,990, S11,000). The

~~SECRET~~

~~SECRET~~

Azrack Opinion fails to consider the full context of Senator Leahy's remarks. The language limiting "content" added in section 216 of the PATRIOT Act was intended to address any risk that terms describing new technology, such as "routing" and "addressing" information, would be misinterpreted to change the nature of information collected with pen register devices. Furthermore, the Azrack Opinion generally fails to consider the statements (discussed above) indicating that the limitation provision's minimization scheme had not changed. (U)

Finally, the Azrack Opinion mistakenly interprets Senator Leahy's statements that "[w]hen I added the direction on use of reasonably available technology . . . to the pen register statute as part of [CALEA] in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere relevance standard." Id. (citing 147 Cong. Rec. S11,000). Magistrate Judge Azrack considered this an important indication that Senator Leahy intended section 216 to address constitutional concerns regarding the use of pen register devices, presumably by restricting incidental collection of content post-cut-through digits. The Azrack Opinion takes out of context Senator Leahy's comments, which were directed towards his desire for heightened judicial review of criminal pen register applications, not the minimization scheme in place under the

~~SECRET~~

~~SECRET~~

limitation provision. Again, Senator Leahy's proposal for heightened judicial review was not adopted in the PATRIOT Act, and his comments regarding the FBI's failure to develop "filtering" technology to date were directed at his disappointment that Congress had failed to adopt his proposal.

(U)

C. Congress Has Provided Additional Authority to Allow the Government to Collect Post-Cut-Through Digits Under FISA. (U)

In addition to the plain text and legislative history, both of which, as described above, support an interpretation of the pen register statute authorizing the collection of post-cut-through digits, further support for this conclusion is found under FISA. In the USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (2006) (Reauthorization Act), enacted in March 2006, Congress augmented the government's authority under the FISA pen register provision to obtain all non-content post-cut-through digits related to the transmission and routing of a call. See § 128, 120 Stat. at 229. The section of the Reauthorization Act entitled "Authority for Disclosure of Additional Information in Connection with Orders for Pen Register and Trap and Trace Authority Under FISA," section 128, added a new subsection to the FISA pen register

~~SECRET~~

~~SECRET~~

provision, 50 U.S.C. § 1842, requiring that service providers disclose associated routing and transmission information as part of a FISA pen register. The amended section reads as follows:

An order issued under this section . . .

(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. . .

(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.

50 U.S.C. § 1842(d)(2)(C)(i)(III) (emphasis added). When requested by the government -- and if available from the recipient of the Court's order -- the amendment also requires disclosure of the same "routing or transmission information" for the customer or subscriber of incoming and outgoing communications alike. 50 U.S.C. § 1842(d)(2)(C)(ii)(III). (U)

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

~~SECRET~~

~~SECRET~~

(2005) (emphasis added). As referenced above and as explained more fully in the government's May 2006 Memorandum, post-cut-through digits dialed to transmit or route a telephone call to a destination party are non-content post-cut-through digits, which the government is unequivocally permitted to record through pen register surveillance. [REDACTED]

b3 Per FBI
b7E

D. The Canons of Statutory Construction Favor the Government's Authority to Record or Decode Post-Cut-Through Digits, Particularly in the FISA Context. (U)

Assuming, arguendo, that the criminal pen register provision may be read in two separate ways - one which would deny authorization to any device that may incidentally acquire content post-cut-through digits and another which would permit such acquisition when necessary subject to minimization - the Court must look to the relevant canons of statutory construction to resolve the ambiguity. The government respectfully submits that its interpretation most effectively harmonizes the whole statute, without rendering any word, phrase or section superfluous, and without repealing the minimization scheme that Congress enacted under the limitation provision - particularly when the additional FISA authorities described above are considered along with other unique aspects of national security law. (U)

~~SECRET~~

~~SECRET~~

1. No Clause or Word should be Rendered Superfluous.
(U)

As noted above, "[i]t is a cardinal principle of statutory construction that, . . . if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." TRW, 534 U.S. at 31 (citation omitted). Courts must strive to "give effect, if possible, to every clause and word of a statute." Id. (citation omitted). (U)

Both the Azrack and Smith Opinions address this issue. Indeed, the Azrack Opinion acknowledges that an interpretation of the definition of pen register denying authorization to any device that may incidentally acquire content post-cut-through digits renders section 3121(c) superfluous. See Azrack Op., 515 F. Supp. 2d at 334-35 ("The phrase counseling the Government to use 'technology reasonably available . . . so as not to include the contents of . . . communications' . . . is superfluous if the ban on content acquisition is absolute.") (quoting 18 U.S.C. § 3121(c)). Nevertheless, Magistrate Judge Azrack declined to find this issue "dispositive," largely because of what she saw as the more significant concerns raised by the canon of constitutional avoidance (discussed below). Id. at 336. (U)

Unlike Magistrate Judge Azrack, Magistrate Judge Smith rejected the government's argument that his reading of the

~~SECRET~~

~~SECRET~~

statute - that the concluding passages of 18 U.S.C. sections 3121(c) and 3127(3) amount to an "unqualified content proscription" - renders the words "technology reasonably available to it" superfluous. Smith Op., 441 F. Supp. 2d at 825. He determined that the government's conflicting interpretation "rests almost entirely on legislative silence," and that 18 U.S.C. section 3121(c) "does not say what the outcome would be if technology could not separate all content from non-content dialed digits." Id. at 824. Magistrate Judge Smith determined that "[t]he most natural reading of the provision is that Congress assumed that such technology would be available, and for that reason did not address or even contemplate the contrary scenario." Id. This determination contradicts indications that Congress was well aware that such technology does not exist and open registers are capable of incidentally collecting content. The Smith Opinion concluded that a reading that would permit interception of content post-cut-through digits "contradicts, or at least creates serious tension with, the explicit content prohibitions inserted into the statute." Id. at 825. The Smith Opinion concluded that the most harmonious reading of the statute would deny access to post-cut-through digits unless the government could demonstrate that no content post-cut-through dialed digits would be intercepted. Id. (U)

~~SECRET~~

~~SECRET~~

Under that interpretation, no device that is capable of acquiring content falls within the definition of pen register. However, if there were no such thing as a pen register that acquires communications content, then there also would have been no need for Congress to instruct the government to use technology "reasonably available to it" to restrict the recording or decoding of content when using pen register devices. Thus, under the interpretation advanced by Magistrate Judge Smith, section 3121(c) is left without a function in the statutory scheme. (U)

The doctrine against superfluties should apply with special force in this case. This is not an instance of a single word or tangentially related provision being rendered superfluous. Rather, the Smith and Azrack Opinions interpret one part of the criminal pen register provision, the definition, to render another part of the very same chapter, the limitation provision, superfluous to the statutory scheme.²³ Moreover, Congress amended both provisions in the very same section of the PATRIOT Act, section 216, and clearly was aware of and chose to retain both. One must therefore conclude that Congress saw a continuing

²³ The cases that deny access to post-cut-through digits based on the purported plain language of the statute, *see* Rosenthal Op., Spaulding Op., Conway Op., and Orenstein Op., likewise render section 3121(c) superfluous to the statutory scheme. (U)

~~SECRET~~

~~SECRET~~

purpose for the limitation provision separate from and in addition to the amended definition of pen register. The Smith Opinion's dismissal of the surplusage canon effectively rewrites section 216 of the PATRIOT Act to fit a preconceived - and inaccurate - notion of Congress's intent. (U)

2. The Doctrine Against Implied Repeals (U)

In addition to rendering subsection 3121(c) superfluous, an interpretation of the pen register statute denying requests to record or decode post-cut-through digits constitutes an implied repeal of the "technology reasonably available" provision in section 3121(c). "[A] repeal by implication will only be found when there is clear legislative intent to support it." United States v. Mitchell, 39 F.3d 465, 472 (4th Cir. 1994) (citation omitted). Evidence of the legislature's intent to repeal a statute by implication must be "clear and manifest," Radzanower v. Touche Ross & Co., 426 U.S. 148, 154 (1976) (quotation and citation omitted), and, "because an implied repeal is disfavored, there is a 'strong presumption' against finding such a repeal." Patten v. United States, 116 F.3d 1029, 1034 (4th Cir. 1997) (quoting Blevins v. United States, 769 F.2d 175, 181 (4th Cir. 1985)). In order to find an implied repeal, a court must find either that the two acts in question are "in irreconcilable conflict," or that "the later act covers the whole subject of

~~SECRET~~

~~SECRET~~

the earlier one and is clearly intended as a substitute[.]'" Radzanower, 426 U.S. at 154 (quoting Posadas v. Nat'l City Bank, 296 U.S. 497, 503 (1936)). (U)

As described above, in 1994, Congress added the limitation provision to restrict the recording or decoding of content with a pen register device. That limitation obligates the government to use technology that is reasonably available to it, and nothing more, to fulfill this objective. The government remains entitled to record or decode "dialing; routing, addressing, or signaling information" - and to incidentally record or decode content if no technology is reasonably available to restrict the incidental acquisition. Under an interpretation of the pen register statute prohibiting such incidental acquisition, the limitations on the government's obligation inherent in Congress's choice of the words "technology reasonably available" is eliminated. (U)

The circumstances of the passage of section 216 of the PATRIOT Act do not provide any indication, much less a "clear and manifest" indication, that Congress intended such a change. If Congress intended the definition of pen register, as amended under section 216 of the PATRIOT Act, to exclude a device that captures content, it would not have amended sections 3121(c) and 3127(3) at the same time and left intact the "technology reasonably available" language in 3121(c). (U)

~~SECRET~~

~~SECRET~~

Magistrate Judge Azrack dismissed the implied repeals claim, finding that because section 3121(c) is a "limitation," and the strict interpretation of the definition of "pen register" further limited the collection of content, there is no conflict in the provisions. Azrack Op., 515 F. Supp. 2d at 334. This conclusion is based on a reading of the limitation provision that ignores the phrase "technology reasonably available." As discussed above, Congress's choice to include qualifying language (i.e., "reasonably available") to describe the government's obligation to use "technology" to restrict recording or decoding of communications content can only have one purpose - to describe the outer limits of the government's obligation to avoid the collection of content at the point of acquisition. An expansive reading of the pen register definition effectively repeals the limits to the limitation provision. (U)

3. The Canon of Constitutional Avoidance (U)

The canon of constitutional avoidance is based on the assumption that Congress usually intends to avoid passing unconstitutional laws, and thus counsels that a court should favor statutory interpretations that do not raise "serious constitutional doubts." See Clark v. Martinez, 543 U.S. 371, 381 (2005). The Azrack and Smith Opinions rely on the canon of constitutional avoidance as a basis to deny government

~~SECRET~~

~~SECRET~~

applications for post-cut-through digits under pen register orders. See Azrack Op., 515 F. Supp. 2d at 335 (stating that "the most applicable canon of statutory construction is the doctrine of constitutional avoidance"); Smith Op., 441 F. Supp. 2d at 837. Judges Smith and Azrack both concluded that the interpretation of the statute allowing acquisition of post-cut-through digits, which may incidentally include content, would raise grave constitutional concerns under the Fourth Amendment, and therefore should be avoided. See Azrack Op., 515 F. Supp. 2d at 339 (finding that the government's request "would violate the Fourth Amendment"); Smith Op., 441 F. Supp. 2d at 837 ("The Government's reading of 18 U.S.C. § 3121(c) would impinge upon Fourth Amendment protections because it permits the collection of communications content without a warrant based on probable cause, in apparent violation of Katz v. United States, 389 U.S. 347, 353-54 [1] (1967)."). Although Judge Conway's opinion appears primarily to be based on her plain reading of the text, she also references Fourth Amendment concerns, describing recording and decoding of post-cut-through digits as an "interception" and a "statutory and constitutional violation." Conway Op. at 6 (referring to DAG Memo and stating it does not remedy the problem; "this Court cannot cede to the executive branch its responsibility to safeguard the Fourth Amendment."). (U)

~~SECRET~~

~~SECRET~~

The canon of constitutional avoidance does not allow the court to overlook the plain text of the statute and thereby disregard congressional intent and Congress's scheme, including the minimization scheme adopted in 1994, as a means to resolve any possible Fourth Amendment issues attendant to the incidental acquisition of possible content post-cut-through digits. "The canon is thus a means of giving effect to congressional intent, not of subverting it." Clark, 543 U.S. at 382. (U)

Moreover, the "serious constitutional doubt" claimed by Magistrate Judges Azrack and Smith and suggested by Judge Conway - that the government cannot collect the contents of a communication without a warrant issued upon probable cause - does not apply in the context of FISA pen register surveillance. In Katz, the Supreme Court explicitly declined to extend its holding that the Fourth Amendment requires a warrant to surveil content to national security cases. See Katz, 389 U.S. at 358 n.23 ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is not a question presented by this case."). In United States v. United States District Court (Keith), 407 U.S. 297, 321-22 (1972), the Supreme Court similarly declined to extend the Fourth Amendment warrant requirement to activities of foreign powers or their agents. No other federal

~~SECRET~~

~~SECRET~~

court has ever held that the Fourth Amendment warrant requirement applies to cases involving foreign powers or agents of foreign powers. See In Re Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002); H.R. Rep. No. 95-1283(I), at 17-21 (1978). Given the unique constitutional and statutory context of FISA pen register orders, the canon of constitutional avoidance does not counsel against the government's interpretation, and does not require the Court to conclude that the Congress intended to prevent the government from acquiring post-cut-through digits under FISA pen register orders. (U)

E. The Recording and Decoding of Post-Cut-Through Digits, With a Restriction on the Use of Content Digits Except in Rare, Emergency Circumstances, is Reasonable Under the Fourth Amendment. (U)

The government submits that the scheme adopted by Congress in 18 U.S.C. sections 3127(3) and 3121(c), which allows the incidental recording 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. 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 at 737, 742, 746 (emphasizing reasonableness as critical factor in reviewing constitutionality

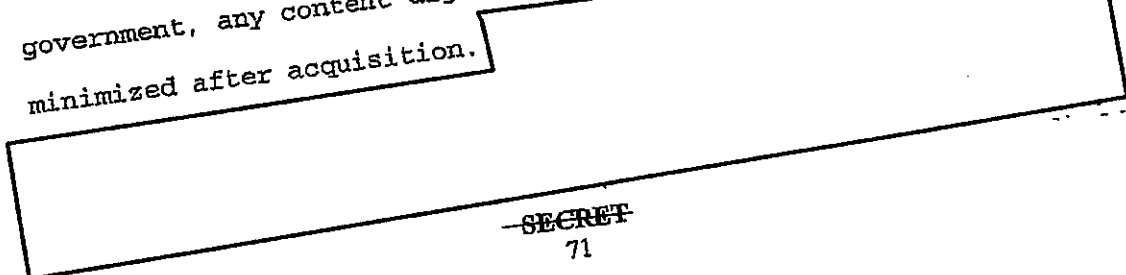
~~SECRET~~

~~SECRET~~

of FISA). (U)

Reasonableness, in this context, must be assessed under a general balancing approach, "by assessing, on the one hand, the degree to which it 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)). As recently observed by the Foreign Intelligence Surveillance Court of Review, "[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 Pursuant to Section 105B of the For. Intel. Surv. Act, 551 F.3d 1004, 1012 (FISA Ct. Rev. 2008). (U)

Here, the intrusion on privacy - recording or decoding the digits dialed by a targeted telephone after an initial call is set up - is slight - and in most circumstances the effect of the intrusion is nil. Under the procedures followed by the government, any content digits incidentally acquired will be minimized after acquisition.



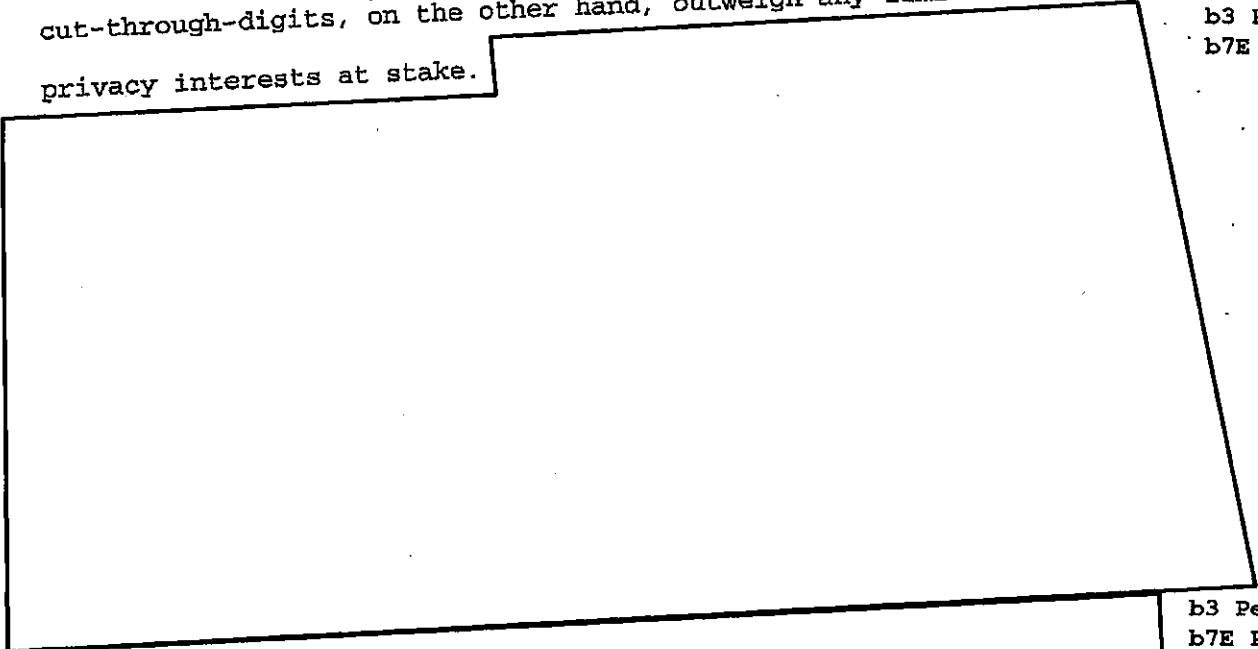
b3 Per FBI
b7E Per FBI

~~SECRET~~

FBI prohibits use of any such incidentally-acquired content digits for any investigative purposes other than in extremely rare, exigent circumstances, discussed below. (U)

The government's interests in recording or decoding post-cut-through-digits, on the other hand, outweigh any limited privacy interests at stake.

b3 Per FBI
b7E

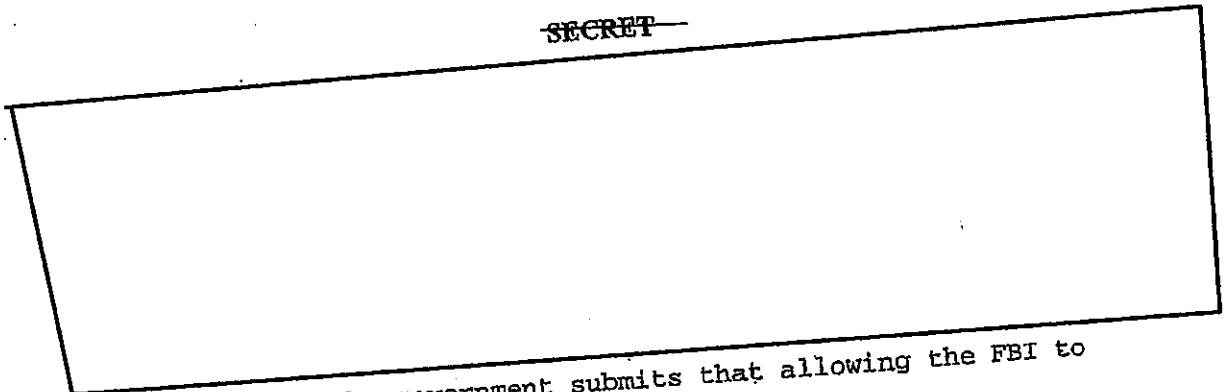


b3 Per FBI
b7E Per FBI

~~SECRET~~

~~SECRET~~

b3 Per FBI
b7E Per FBI



Finally, the government submits that allowing the FBI to use, for investigative purposes, incidentally acquired content digits in specified rare circumstances is also reasonable under the Fourth Amendment. As a practical matter, the government believes that the circumstances under which the government would need to and would be capable of identifying any meaningful content digits that it could use for investigative purposes to prevent immediate danger of death, serious physical injury or harm to the national security would be genuinely rare. (S)

Moreover, emergency exceptions to warrant requirements have long been recognized as a matter of statute (under both FISA and the criminal code) and as a matter of Fourth Amendment case law. See, e.g., 50 U.S.C. § 1805(e)(1) (allowing Attorney General to authorize emergency employment of electronic surveillance to obtain foreign intelligence information under certain circumstances); 18 U.S.C. § 2518(7) (allowing certain high-ranking Justice Department officials to authorize emergency surveillance in specified situations); Mincey v. Arizona, 437

~~SECRET~~

~~SECRET~~

U.S. 385, 393-94 (1978) ("Warrants are generally required to search a person's home or his person unless 'the exigencies of the situation' make the needs of law enforcement so compelling that the warrantless search is objectively reasonable under the Fourth Amendment.") (citation omitted). (U)

Furthermore, the government respectfully submits that the Court can safeguard incidentally acquired content post-cut-through digits by precluding the government from using them, if incidentally obtained, for any investigative purposes, except in rare cases, to prevent an immediate danger of death, serious physical injury or harm to the national security. Given the interests at stake when such emergency circumstances exist, the government submits that this exception is also objectively reasonable under the Fourth Amendment. ~~(S)~~

~~SECRET~~

~~SECRET~~

IV. CONCLUSION (U)

For all of the foregoing reasons, as well as the reasons set forth in the government's 2006 Memoranda and Report described above, the government respectfully submits that this Court should continue to approve the recording and decoding of post-cut-through digits under FISA pen register orders. ~~(S)~~

Respectfully submitted,

David S. Kris
Assistant Attorney General for National Security

Tashina Gauhar
Chief, Operations Section

By: b6, b7C
Chief, Counterintelligence Unit

b6, b7C

Attorneys

Office of Intelligence
National Security Division
United States Department of Justice


b6 Per FBI
b7C Per FBI

~~SECRET~~

~~SECRET~~VERIFICATION

The information set forth in Section II of this Memorandum, "Statement of Facts Concerning Post-Cur-Through Digits," is based upon my personal knowledge, my review and consideration of documents and information available to me in my official capacity, and my review and consideration of information provided to me by other law enforcement or civilian personnel whom I know or supervise. I make no representations as to the legal analysis included herein. I declare under penalty of perjury that the foregoing is true and correct to the best of my personal knowledge, information and belief. Executed pursuant to Title 28, United States Code, Section 1746 on this 17th day of

August, 2009. (U)

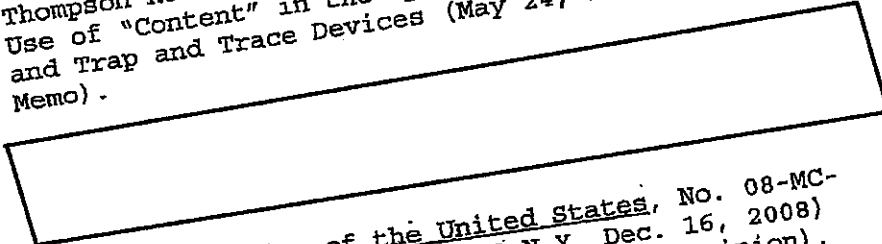

Anthony P. DiClemente
Section Chief
Operational Technology Division
Federal Bureau of Investigation

~~SECRET~~

~~SECRET~~

EXHIBIT LIST

A Memorandum by Deputy Attorney General Larry D. Thompson Re: Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices (May 24, 2002) (DAG Memo).



b3 Per FBI
b7E Per FBI

B

C

In re Application of the United States, No. 08-MC-595(JO), 2008 WL 5255815 (E.D.N.Y. Dec. 16, 2008) (Magistrate Judge Orenstein) (Orenstein Opinion).

D

In re Application of the United States, Misc. No. H-07-613, 2007 WL 3036849 (S.D. Tex Oct. 17, 2007) (District Judge Rosenthal) (Rosenthal Opinion).

E

In re Application of the United States, No. 6:06-mj-1130 (M.D. Fla. May 23, 2006) (Magistrate Judge Spaulding) (Spaulding Opinion).

F

In re Application of the United States, No. 6:06-mj-1130 (M.D. Fla. June 20, 2006) (District Judge Conway) (Conway Opinion).

~~SECRET~~

Ex. A

DAG

002/006



U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530


May 24, 2002

MEMORANDUM

TO:

THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
 THE ASSISTANT ATTORNEY GENERAL, ANTITRUST DIVISION
 THE ASSISTANT ATTORNEY GENERAL, TAX DIVISION
 ALL UNITED STATES ATTORNEYS
 THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
 THE ADMINISTRATOR OF THE DRUG ENFORCEMENT
 ADMINISTRATION
 THE COMMISSIONER OF THE IMMIGRATION AND
 NATURALIZATION SERVICE
 THE DIRECTOR OF THE UNITED STATES MARSHALS SERVICE

FROM:

Larry D. Thompson 

SUBJECT:

Avoiding Collection and Investigative Use of "Content" in the Operation of
Pen Registers and Trap and Trace Devices

This Memorandum sets forth the Department's policy regarding avoidance of "overcollection" in the use of pen registers and trap and trace devices that are deployed under the authority of chapter 206 of Title 18, United States Code, 18 U.S.C. § 3121, *et seq.*¹

The privacy that Americans enjoy in the content of their communications – whether by telephone, by facsimile, or by email – is a basic and cherished right. Both the Fourth Amendment and federal statutory law provide important protections that collectively help to ensure that the content of a person's private communications may be obtained by law enforcement only under certain circumstances and only with the proper legal authorization. In updating and revising the statutory law in this area, the recently enacted USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("the Act"), draws the appropriate balance between the right of individuals to maintain the privacy of their communications and the need for law enforcement to obtain the evidence necessary to prevent and prosecute serious crime.

¹ The authorities granted by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, *et seq.*, are outside the scope of this Memorandum.

003/006

06/03/02

16:56

202 514 6897

DAG

In particular, Section 216 of the Act revised and clarified existing law governing "pen registers" and "trap and trace" devices - which record limited information concerning the "processing and transmitting" of communications (such as the telephone numbers dialed on a phone) - so that these devices may clearly be used, not just on telephones, but in the context of any number of communications technologies.

At the same time, several provisions of the Act underscore the importance of avoiding unauthorized collection or use, by government agents, of the content of wire or electronic communications. In order to accomplish this important goal, this Memorandum briefly describes the relevant law and the changes made by the Act, and then sets forth Departmental policies in this area. Those policies include the following:

- Reasonably available technology must be used to avoid collection of any content.
- If, despite use of reasonably available technology, some collection of a portion of content occurs, no affirmative investigative use may be made of that content.
- Any questions about what constitutes "content" must be coordinated with Main Justice.

Prior Law Governing Pen Registers and Trap and Trace Devices. Since 1986, the use of "pen registers" and "trap and trace" devices has been governed by the provisions of chapter 206 of Title 18, United States Code. See 18 U.S.C. § 3121, et seq. Prior to the recent enactment of the USA Patriot Act, a "pen register" was defined in chapter 206 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. § 3127(3). Analogously, a "trap and trace" device was defined as "a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted." *Id.*, § 3127(4). Thus, a pen register could be used to record the numbers of all outgoing calls on a telephone, and a trap and trace device could be used to record the numbers of all incoming calls.

Because the Supreme Court has held that this sort of limited information concerning the source and destination of a communication is not protected by the Fourth Amendment's warrant requirement, see *Smith v. Maryland*, 442 U.S. 735 (1979), chapter 206 permitted an order authorizing a pen register or trap and trace device to be issued without showing probable cause. Instead, an order shall be issued if the Government "certifie[s] that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a) (2000). By contrast, the contents of a telephone conversation are generally protected by the Fourth Amendment, see *Katz v. United States*, 389 U.S. 347 (1967), as well as by the more extensive procedural protections of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968), codified as amended at 18 U.S.C. § 2510, et seq. ("Title III").

004/006

06/03/02 16:56 202 514 6897

DAG

In enacting the provisions of Chapter 206 governing pen registers and trap and trace devices, Congress also amended Title III to exempt pen registers and trap and trace devices from the requirements of the latter statute. See Pub. L. 99-508, § 101(b), 100 Stat. 1848 (1986) (adding 18 U.S.C. § 2511(h)(i)). However, in order to address the possibility that a pen register might, due to technological limitations, obtain some limited measure of "content," Congress later specifically provided in chapter 206 that an agency authorized to use a pen register must "use technology reasonably available to it" that restricts the information obtained to that used in "call processing." Pub. L. No. 103-414, § 207(b), 108 Stat. 4279 (1994) (amending 18 U.S.C. § 3121(c)).

Relevant Amendments made by the USA Patriot Act. The Act made several changes to chapter 206 that are of relevance here. In particular, section 3121(c) was amended to make explicit what was already implicit in the prior provision, namely, that an agency deploying a pen register must use "technology reasonably available to it" that restricts the information obtained "so as not to include the contents of any wire or electronic communications." The amended section 3121(c) now reads, in full, as follows:

A governmental 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), as amended by Pub. L. No. 107-56, § 216(a), 15 Stat. at 288 (emphasis added).

Similarly, in amending the definitions of "pen register" and "trap and trace device" to make them more technologically neutral, the Act again expressly reiterates what was already implicit in the prior statute, namely, that a pen register or a trap and trace device is not to be viewed as an affirmative authorization for the interception of the content of communications. Thus, the amended definition of a "pen register" now provides, in pertinent part:

[T]he 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

18 U.S.C. § 3127(3), as amended by Pub. L. No. 107-56, § 216(c)(2), 115 Stat. at 290 (emphasis added). Likewise, the Act amends the definition of "trap and trace device" so that it now provides:

005/006

06/03/02

15:57

202 514 8897

DAG

[T]he 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

18 U.S.C. § 3127(4), as amended by Pub. L. No. 107-56, § 216(c)(3), 115 Stat. at 290 (emphasis added).

Department Policy Regarding Avoidance of "Overcollection" in the Use of Pen Registers and Trap and Trace Devices. Although, as noted, the Act's specific addition of references to "content" in chapter 206 probably does not alter pre-existing law on this point, it is appropriate, in light of Congress' action, to clearly delineate Department policy regarding the avoidance of "overcollection," i.e., the collection of "content" in the use of pen registers or trap and trace devices under chapter 206. This policy includes the following basic principles.

1. Use of reasonably available technology to avoid overcollection. As mandated by section 3121(o), an agency seeking to deploy a pen register or trap and trace device must ensure that it uses "technology reasonably available to it" that restricts the information obtained "so as not to include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c) (West Supp. 2002). This provision imposes an affirmative obligation to operate a pen register or trap and trace device in a manner that, to the extent feasible with reasonably available technology, will minimize any possible overcollection while still allowing the device to collect all of the limited information authorized.

Moreover, as a general matter, those responsible for the design, development, or acquisition of pen registers and trap and trace devices should ensure that the devices developed or acquired for use by the Department reflect reasonably available technology that restricts the information obtained "so as not to include the contents of any wire or electronic communications."

2. No affirmative investigative use of any overcollection that occurs despite use of reasonably available technology. To the extent that, despite the use of "technology reasonably available to it," an agency's deployment of a pen register does result in the incidental collection of some portion of "content," it is the policy of this Department that such "content" may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security. For example, if, despite the use of reasonably available technology, a telephone pen register incidentally recorded a bank account number and personal identification number (PIN) entered on an automated bank-by-phone system, those numbers should not be affirmatively used for any investigative purpose.

Accordingly, each agency must take steps to ensure that any incidental collection of a portion

06/03/02 16:57 202 514 6897

DAG

006/006

of "content" is not used for any affirmative investigative purpose.² Investigating agencies should take appropriate measures to ensure compliance with this directive, and United States Attorneys should likewise ensure that federal prosecutors do not make any investigative use of such content, whether in court applications or otherwise.

3. Coordination of issues concerning what constitutes "content". In applying the above principles, agencies should be guided by the definition of "content" that is contained in Title III: the term "content" is there defined to include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8) (West Supp. 2002). Similarly, in describing the sort of information that pen registers and trap and trace devices are designed to capture, the provisions of Chapter 206 make clear that "dialing, routing, addressing or signaling information" that is used in "the processing and transmitting of wire or electronic communications" does not, without more, constitute "content." 18 U.S.C. § 3127(3) (West Supp. 2002); *id.*, § 3121(e).

The Assistant Attorney General for the Criminal Division (AAG) should ensure that the Criminal Division provides appropriate guidance, through amendments to the United States Attorneys' Manual or otherwise, with respect to any significant general issues concerning what constitutes the "content" of a communication.

To the extent that, in applying the above principles, specific issues arise over whether particular types of information constitute "content," such questions should be addressed, as appropriate, to the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

Construction of this Memorandum. This Memorandum is limited to improving the internal management of the Department and is not intended to, nor does it, create any right, benefit, or privilege, substantive or procedural, enforceable at law or equity, by any party against the United States, the Department of Justice, their officers or employees, or any other person or entity. Nor should this Memorandum be construed to create any right to judicial review involving the compliance or noncompliance of the United States, the Department, their officers or employees, or any other person or entity, with this Memorandum.

² This is not to say that an agency should not retain a file copy of all of the information it received from a pen register or trap and trace device. An agency may be statutorily required to keep a record of all of the information it obtains with a particular pen register or trap and trace device, see, e.g., 18 U.S.C. § 3123(a)(3), as amended by Pub. L. No. 107-56, § 216(b)(1), 115 Stat. at 289 (requiring that, in certain limited circumstances, an agency must maintain and file with the issuing court a record of "any information which has been collected by the device"), and, in the event of a subsequent prosecution, the agency may be required to produce to defense counsel a complete record of what was recorded or captured by a pen register or trap and trace device deployed by the agency in a particular case. This Memorandum prohibits affirmative investigative uses. Accordingly, nothing in this Memorandum should be construed to preclude an agency from maintaining a record of the full information obtained by the agency from a pen register or trap and trace device.

APPROVED FOR PUBLIC RELEASE

ALL INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 01-19-2022 BY



b6 Per FBI

b7C Per FBI

Ex. B

Ex. C

Westlaw.

Not Reported in F.Supp.2d
 Not Reported in F.Supp.2d, 2008 WL 5255815 (E.D.N.Y.)
 (Cite as: 2008 WL 5255815 (E.D.N.Y.))

Page 1

Only the Westlaw citation is currently available.

United States District Court,
 E.D. New York.

In the Matter of an APPLICATION OF THE
 UNITED STATES of America FOR AN ORDER
 AUTHORIZING THE USE OF A PEN REGISTER
 AND A TRAP AND TRACE DEVICE ON WIRE-
 LESS TELEPHONE Bearing Telephone Number
 [Redacted], Subscribed To [Redacted], Serviced by
 [Redacted].

No. 08 MC 0595(JO).

Dec. 16, 2008.

West KeySummary
 Telecommunications 372 \Rightarrow 1475

372 Telecommunications

372X Interception or Disclosure of Electronic
 Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public
 Officers

372k1475 k. Carrier's Cooperation; Pen
 Registers and Tracing. Most Cited Cases

A district court denied the government authoriza-
 tion to have its agents install and use, or cause to be
 installed and used, a device or process that would
 record all dialing, routing, addressing, and signal-
 ing information, but that would only exclude the
 decoding of any post-cut-through dialed digits,
 since such a device would not be a "pen register"
 within the meaning of the governing statute. It was
 unlawful for a pen register to record the contents of
 communication, and by recording all the informa-
 tion that the government desired the contents of
 communication could also be intercepted. 18
 U.S.C.A. §§ 3127(3), 2510(8).

Amy Busa, United States Attorneys Office, Eastern
 District of New York, Brooklyn, NY, for Applica-
 tion of the United States of America for an Order

Authorizing the Use of a Pen Register and a Trap
 and Trace Device on Wireless Telephone.

REDACTED MEMORANDUM AND ORDER

JAMES ORENSTEIN, United States Magistrate
 Judge.

*1 The government seeks authorization to install
 and use a pen register device. This routine applica-
 tion is the first that has been presented to me since
 the decision by a district judge of this court in *In*
the Matter of an Application of the United States of
America for an Order Authorizing the Use of Two
Pen Register and Trap and Trace Devices, 2008
 WL 5082506 (E.D.N.Y. Nov.26, 2008) ("*In re*
United States"). Because such applications are
 time sensitive, I write as briefly as possible to ex-
 plain the manner in which I resolve it. In short, I
 grant the government's application, but only if the
 relevant provider of telecommunications service
 would record the requested information, including
 pre-cut-through dialed digits, for its own business
 purposes without the requested order and only if, in
 addition, the provider can and will delete and post-
 cutthrough dialed digits ("PCTDD") before provid-
 ing such information to any government agent. If
 these conditions are not met, and if instead the gov-
 ernment seeks to have the provider transmit some
 post-cut-through dialed digits to the government in
 the expectation that a government agency will de-
 lete such information without ever decoding it be-
 fore passing the filtered information to the specific
 agents conducting the instant investigation, I deny
 the application.

A. Precedent

Where, as here, an Article III judge of this court has
 ruled unambiguously on a matter of law on indistin-

Not Reported in F.Supp.2d
 Not Reported in F.Supp.2d, 2008 WL 5255815 (E.D.N.Y.)
 (Cite as: 2008 WL 5255815 (E.D.N.Y.))

guishable facts, I am hesitant to do anything other than follow that ruling. In the absence of any controlling decision by the United States Supreme Court or the United States Court of Appeals for the Second Circuit, I of course look for guidance to a decision by a district judge of this court. However, a single district judge's ruling does not establish binding precedent within a district. *See, e.g., ATSI Communs., Inc. v. Shaar Fund, Ltd.*, 547 F.3d 109, 112 & n. 4 (2d Cir.2008) (citing cases). As a result, I am obliged to give the matter presented to me for decision my best independent reading of applicable law, regardless of whether that reading accords with that of my superior.^{FN1}

FN1. In a recent decision, a district judge wrote that a magistrate judge "was not required to consider" a decision written by a district judge in another district "as 'district court decisions are not treated as binding precedents in other cases.'" *In re Bulk Oil (USA) Inc.*, 2007 WL 1121739, at * 10 n. 9 (S.D.N.Y. Apr.11, 2007) (quoting *IBM Credit Corp. v. United Home for Aged Hebrews*, 848 F.Supp. 495, 497 (S.D.N.Y.1994)). That observation is dicta, and in any event plainly does not address the precise procedural issue here. However, I have not found any more apposite case law on the question of whether a magistrate judge is bound to adhere to the view of a single district judge within the same district with which a different district judge would be free to disagree.

The decision on the instant application falls to me because the application was submitted earlier today while I was the magistrate judge on criminal duty. As an adjunct to an Article III court, a magistrate judge may exercise delegated powers of the court as such, subject to review by a district judge pursuant to Federal Rule of Criminal Procedure 59. The review of a magistrate judge's ruling on a pen register application will normally be assigned to the

district judge of this court on "miscellaneous" duty pursuant to Local Rule 50.5. If the author of *In re United States* were the district judge currently assigned to such miscellaneous duty, I would simply defer to his interpretation as a matter of judicial economy rather than force the government to seek review that would inevitably lead to the same result.^{FN2} But where, as here, an appeal of my decision would be directed to a district judge who has not yet considered the issue and would not be bound by the analysis or result in *In re United States*, I conclude that my obligation is to conduct my own analysis. Otherwise, as a practical matter—because a pen register application is ordinarily directed to magistrate judges as a matter of course, and no party has both the incentive to appeal the grant of such an application and the ability or standing to do so—a single district judge's decision in favor of the government on the instant legal question would freeze the development of the law in a district, and possibly in a circuit, in a way that would not be possible with respect to motions normally made in the first instance to a district judge.

FN2. Even more obviously binding upon me is the directive in *In re United States* that I "issue, if still necessary, an Order authorizing the installation of the pen registers on the SUBJECT TELEPHONES that is consistent with the representations" that the government made in that case and that are largely similar to the government's proposal here. 2008 WL 5082506, at *8. Although the government has not yet advised me that any such order is necessary (and I assume it would have done so in the intervening weeks if the matter were still a live one), I am unquestionably bound to issue the relevant order in that case upon request.

B. Analysis

Not Reported in F.Supp.2d
 Not Reported in F.Supp.2d, 2008 WL 5255815 (E.D.N.Y.)
 (Cite as: 2008 WL 5255815 (E.D.N.Y.))

*2 Since 2001, Congress has defined 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). As thoroughly discussed by some of my colleagues, that formulation has led to a vexing problem of statutory interpretation. The process normally used to install a pen register ordinarily allows the installing party to record and decode not simply the numbers a telephone user has dialed in order to be connected to another party, but also a great deal of other information that can be transmitted in the form of dialed digits but that nevertheless constitutes the "contents" of a communication; for example, a person calling an automated banking service must dial the telephone number of the service, and then enter additional digits that identify the caller's account number and the code needed to authorize access to the caller's account. The telephone number may properly be intercepted by a pen register; the additional numbers, known as "post-cut-through dialed digits" or "PCTDD," are "content" within the meaning of 18 U.S.C. § 2510(8), and accordingly may not be recorded or decoded. See *In the Matter of Applications of the United States of America for Orders (1) Authorizing the Use of Pen Registers and Trap and Trace Devices and (2) Authorizing Release of Subscriber Information*, 515 F.Supp.2d 325 (E.D.N.Y.2007) ("EDNY PCTDD") (magistrate judge decision); FN3 *In the Matter of the Application of the United States of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information*, 2007 WL 3036849 (S.D.Tex. Oct.17, 2007) ("SDTX PCTDD") (district judge decision).

FN3. It is my understanding that the cited

decision by a magistrate judge was appealed to the district judge on miscellaneous duty and upheld over the government's objection. I was unable to find a citation for that decision in the time available to consider the instant application.

In the instant application, following an approach approved in *In re United States*, the government proposes to avoid the difficulty described above by insulating the agents and prosecutors conducting the instant investigation in one of two ways:

[I]f possible, the [relevant service] provider will forward only pre-cut-through dialed digits to the investigative agency. If the provider's technical capabilities require it to forward all dialed digits, including PCTDD, however, the investigative agency will only decode and forward to the special agents the numbers that are dialed before the call is cut through. Thus no PCTDD will be decoded or accessed by anyone.

Sealed Application at 3 n. 1 (citing *In re United States*, 2008 WL 5082506, at * 1 n. 3 ("It is irrelevant that the provider will forward PCTDD to the Government and that the Government will therefore be able, if it violates the court order, to record and decode it... Congress, in Title III [18 U.S.C. § 2510 et seq.], has clearly expressed its belief that the Government can without supervision limit its investigatory activities so as to protect the constitutional rights of suspects.")).

*3 I find that proposal insufficient for the following reason. The pen register statute does not merely forbid the government as such from decoding content such as PCTDD; if it did, I would agree that the government's proposal is workable. Rather, the statute also makes it unlawful for a pen register itself to record the contents of a communication. FN4. The government explicitly seeks authorization to have its agents install and use, or cause to be installed and used, a device or

Not Reported in F.Supp.2d
 Not Reported in F.Supp.2d, 2008 WL 5255815 (E.D.N.Y.)
 (Cite as: 2008 WL 5255815 (E.D.N.Y.))

process that will record all dialing, routing, addressing, and signaling information but that will only exclude the decoding of any PCTDD within such information. See Sealed Application at 3. Thus, as a result of the orders the government would have me issue, agents of the government (or employees of a service provider, acting at their behest) would install and use a device or process to record the contents of communications. ^{FN5} In doing so, they would be using a device or process that cannot be considered a "pen register," and would thereby violate the law. That the same agents, or others acting on their behalf, would somehow later delete the portion of the recording that constituted the contents of the communication would not serve to undo the already completed unlawful act, nor would it retroactively transform something that was not a pen register into something that was.

^{FN4} More precisely, Title III generally makes it illegal for a person, including a service provider, to intercept and disclose the contents of an wire communication. 18 U.S.C. § 2511(1). That prohibition, however, does not apply to the use of a "pen register" as that term is defined in the pen register statute. *Id.* § 2511(2)(h). Accordingly, because a device or process that records content such as PCTDD cannot be considered a "pen register," the use of such a device or process is unlawful. There are other exceptions to the general prohibition in Title III, including an important one discussed below and several other that are inapposite to the instant application.

^{FN5} Indeed, without such recording of contents, there would be nothing for the service provider or the investigative agency to delete later.

^{FN6} I do not read *In re United States* to take the position that PCTDD would not in fact be recorded at some point before dele-

tion. To the contrary, in a later part of the same opinion, the court explicitly writes that so-called "cell-site information" (a different subset of dialing, routing, addressing, and signaling information the collection of which the government does not explicitly request in the instant application) "becomes a 'historical record' " and therefore amenable to disclosure under the hybrid authority of the pen register statute and 18 U.S.C. § 2703(d) "as soon as it is recorded by the provider." 2008 WL 5082506, at *4 n. 8 (emphasis added).

I recognize the possibility that the service provider may have a legitimate reason to record all of the dialing, routing, addressing, and signaling information at issue here for its own purposes, and that in some such circumstances that recording would not run afoul of the general prohibition against intercepting the contents of communications. See 18 U.S.C. § 2511(2)(a)(i). If the provider at issue here does in fact do that, and can then strip away PCTDD before employing the process or device that the government characterizes as a pen register and therefore without providing any PCTDD to any instrumentality of the government, then the pen register the government proposes would meet the statutory definition and I would approve it.

But if that is not the case, I must deny the application. ^{FN7} That is so even if it is the service provider that deletes all PCTDD before providing it to any government agency. If the service provider's recording of content would be accomplished only by virtue of a court-ordered installation and use of some device or process, then that device or process could not properly be considered a pen register within the meaning of 18 U.S.C. § 3127. As a result, even if the deletion of the recorded PCTDD were to be accomplished entirely by the service provider before any information was forwarded to the government investigating agency, the violation would already have occurred. ^{FN8}

Not Reported in F.Supp.2d
Not Reported in F.Supp.2d, 2008 WL 5255815 (E.D.N.Y.)
(Cite as: 2008 WL 5255815 (E.D.N.Y.))

Page 5

FN7. I find unpersuasive the government's reliance on the reference in *In re United States* to the fact that "Congress, in Title III, has clearly expressed its belief that the Government can without supervision limit its investigatory activities so as to protect the constitutional rights of suspects." The government omits the next part of the decision, which explicitly states the portion of Title III to which the court was referring: 18 U.S.C. § 2518(5) (every order "shall contain a provision that the authorization to intercept shall be ... conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter."). See 2008 WL 5082506, at *1 n. 3. The cited provision of Title III recognizes that an agent who has been authorized to eavesdrop on certain portions of an otherwise private communication cannot, as a practical matter, restrict the interception precisely to the authorized topics; as a result, the statute commands no more than that the agent seek to minimize the interception of contents that are not the subject of the authorizing order. Congress could seek to enact a similar practical solution to the problem of intercepting contents via a device or process that would otherwise be defined as a pen register, and in fact did something quite like that in 1994. See 18 U.S.C. § 3121(c) (requiring a government agency using a pen register to use "technology reasonably available to it ... so as not to include the contents of any wire or electronic communication"). That provision was enacted prior to the 2001 amendment to the definition of the term "pen register" that categorically excluded any device or process that records the content of a communication. Although the government has in the past argued that the failure

to repeal the 1994 provision means that the 2001 amendment cannot be interpreted to preclude the use of a pen register to record or decode PCTDD, that argument has been rejected, and the government has not sought to resuscitate it here. See *EDNY PCTDD*, 515 F.Supp.2d at 334-35; *SDTX PCTDD*, 2007 WL 3036849, at *7-*9.

FN8. Because I conclude that the provider's action in deleting PCTDD it recorded as a result of a court order would not cure the statutory violation, I need not consider whether, if my analysis thus far is incorrect, it would still be impermissible for the provider to transmit some PCTDD to the investigating agency and have the latter do further deletions before providing only non-content to the specific agents conducting the investigation. To the extent that this ruling may be appealed however, I provide the following alternative basis for denying so much of the government's request as would rely on such a procedure. No provision of the relevant statutory scheme draws any meaningful distinction between one agent and another within the same investigating agency, or indeed between one member of the executive branch of government and another. Even if the government does not wish to characterize its executive branch as unitary for purposes of this issue, it does not cite any authority that would countenance the kind of line-drawing it contemplates. If it is unlawful under 18 U.S.C. § 2511(1) for a service provider to disclose PCTDD to the particular agent conducting the investigation, notwithstanding any exception in 18 U.S.C. § 2511(2), then there appears to be nothing in either Title III or the pen register statute that would allow the provider to disclose the same PCTDD to any other government

Not Reported in F.Supp.2d
 Not Reported in F.Supp.2d, 2008 WL 5255815 (E.D.N.Y.)
 (Cite as: 2008 WL 5255815 (E.D.N.Y.))

Page 6

agent. If there is some other statutory basis for distinguishing among the government's agents in this context, the government has not brought it to my attention.

Conclusion

I emphasize that my basis for denying the requested relief in part is a narrow matter of statutory interpretation. I see no constitutional difficulty with allowing the government to obtain the information it seeks to use for investigative purposes by means of a device or process that would qualify as a pen register but for the fact that, during the collection process, PCTDD information is initially recorded and then quickly deleted. Nor do I mean to convey a belief that Congress would or should, if presented with the issue, do anything other than endorse the methodology the government proposes. However, Congress has taken great care to establish a finely calibrated statutory regime to regulate various forms of electronic surveillance; to the extent that I cannot reconcile an otherwise seemingly appropriate surveillance technique with the relevant statutory provisions, I conclude that I must leave it to Congress to change the law rather than accept the government's implicit invitation to do so.

*4 For the reasons set forth above, I grant the government's application only to the extent that the relevant service provider would in any event record the relevant post-cut-through dialed digits for its own purposes and only to the extent that the provider is able to delete such information before disclosing any other dialing, routing, addressing, or signaling information to the government. To the extent that the provider would not in any event record post-cut-through dialed digits without the requested orders, or is unable to delete all such information from the dialing, routing, addressing, and signaling information it would disclose to the government, I deny the government's application. I therefore direct the government, if it continues to seek a pen re-

gister in this case and if such relief is available consistent with the foregoing analysis, to submit to me a proposed order in conformity with this decision.
 FN9

FN9. In light of the importance of this issue and the likelihood that other magistrate judges will confront it, I will prepare a redacted version of decision that can be filed on the public docket without compromising any continuing criminal investigation.

SO ORDERED.

E.D.N.Y., 2008.

In re Application of the U.S. for an Order Authorizing the Use of a Pen Register and a Trap and Trace Device on Wireless Telephone
 Not Reported in F.Supp.2d, 2008 WL 5255815
 (E.D.N.Y.)

END OF DOCUMENT



Ex. D

Westlaw.

622 F.Supp.2d 411

622 F.Supp.2d 411

(Cite as: 622 F.Supp.2d 411)

Page 1

C

Only the Westlaw citation is currently available.

United States District Court,
S.D. Texas,
Houston Division.

In the Matter of the Application of the UNITED STATES of America for an Order: (1) Authorizing the Installation and Use of a Pen Register and Trap and Trace Device, and (2) Authorizing Release of Subscriber and Other Information.

Misc. Case No. H-07-613.

Oct. 17, 2007.

Background: Government filed application for a court order authorizing installation and use of a pen register and trap/trace device, access to cell-site information and access to post-cut-through dialed digits.

Holdings: The District Court, Lee H. Rosenthal, J., held that:

(1) government was entitled to order authorizing use of a pen register and trap-and-trace device and release of subscriber and other information, and (2) government could not obtain "post-cut-through dialed digits" containing communication contents.

Order granted in part and denied in part.

West Headnotes

[1] Telecommunications 372 ↪1475

372 Telecommunications

372X Interception or Disclosure of Electronic Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public Officers

372k1475 k. Carrier's Cooperation; Pen Registers and Tracing. Most Cited Cases
Government was entitled to order authorizing use

of a pen register and trap-and-trace device and release of subscriber and other information, including cell-site information, where authorization sought was limited to provision of cell-site information at the origin and termination of calls and during the progress of calls not initiated by the government itself, and did not extend to information that could be used to track the location of the phone. 18 U.S.C.A. §§ 2703, 3121.

[2] Telecommunications 372 ↪1475

372 Telecommunications

372X Interception or Disclosure of Electronic Communications; Electronic Surveillance

372X(B) Authorization by Courts or Public Officers

372k1475 k. Carrier's Cooperation; Pen Registers and Tracing. Most Cited Cases
Government could not obtain "post-cut-through dialed digits" containing communication contents under the authority of the Pen/Trap Statute. 18 U.S.C.A. §§ 2703, 3121.

MEMORANDUM AND OPINION

LEE H. ROSENTHAL, District Judge.

The United States of America has filed two *ex parte* applications for orders authorizing the installation and use of a pen register and trap-and-trace device. The magistrate judge granted the Government's requests in part and denied them in part. Specifically, Magistrate Judge Smith granted the request for a pen register and trap-and trace device but denied access to cell-site information and post-cut-through dialed digits.^{FN1} Magistrate judges and district judges have divided over the Government's ability to obtain such data by way of a pen-register application and order.^{FN2} The courts and the Government would all benefit from additional case-law development. As one judge has noted, the best way to test

622 F.Supp.2d 411
 622 F.Supp.2d 411
 (Cite as: 622 F.Supp.2d 411)

the limit of the Government's authority may be through developed records, trial court opinions on suppression motions, and appellate review. See *In re Applications of the United States of Am. for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F.Supp.2d 76, 81-82 (D.Mass.2007).

Some of the issues discussed in these cases and raised by the Government's applications are addressed below.

I. The Applications

The Government filed two *ex parte* applications for orders authorizing the installation and use of a pen register and trap-and-trace device with respect to two separate phone numbers (the "Target Devices"). The applications requested orders directing the Target Devices' service providers to disclose to or to provide on demand by Drug Enforcement Administration (the "Investigative Agency") agents both historical information and prospective information. The applications seek: (1) "[f]or the Target Device[s], records or other information pertaining to subscriber(s) or customer(s), including historical cell site information and call detail records (including in two-way radio feature mode) for sixty days before the date of the order; and (2) "[f]or the Target Device[s], after receipt and storage, records or other information pertaining to subscriber(s) or customer(s), including the means and source of payment for the service and cell site information, provided to the United States on a continuous basis for (a) the origination of a call from the Target Device[s] or the answer of a call to the Target Device[s], (b) the termination of the call and (c) if reasonably available, during the progress of the call" (Docket Entry No. 1 at 2-3; Docket Entry No. 2 at 2-3). The applications appear to request real-time or prospective cell-site information at the beginning and end of calls made or received on the Target Devices, as well as cell-site informa-

tion for the duration of the calls if reasonably available.

The applications request a variety of other subscriber records and other information relating to certain information captured by the pen registers and trap-and-trace devices on the Target Devices, as well as disclosure of changes in service regarding the Target Devices. The applications also ask the court to authorize the Investigative Agency to install, or cause the provider to install, and to use a pen-register device that would record dialing, routing, addressing, or signaling information (including post-cut-through dialed digits) transmitted from the Target Devices, to record the date and time of the dialings and to record the length of time the phone receiver is "off the hook," for a period of sixty days.

Additionally, the Government requests that the Investigative Agency be permitted to install, or cause the provider to install, and use, a trap-and-trace device on the Target Devices anywhere in the United States. The trap-and-trace device is to capture and record the incoming electronic and other impulses that identify the originating numbers or other dialing, routing, addressing, or signaling information reasonably likely to identify the source of a wire or electronic communication and to record the date, time, and duration of calls created by such incoming impulses, for sixty days. The Government asserts that to the extent that additional digits received are the content of a call as opposed to the number called, this information will not be used for any investigative purpose.

The Government bases these requests on 18 U.S.C. §§ 2703(c), 2703(d), 3122, and 3123 and 47 U.S.C. § 1002. According to the Government, Magistrate Judge Smith signed an order authorizing a pen register and trap-and-trace device, but not for cell-site information or post-cut-through dialed digits. The Government has in effect asked this court for a more expansive order based on the same applica-