UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF TEXAS
HOUSTON DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING (1) INSTALLATION AND USE OF A PEN REGISTER AND TRAP AND TRACE DEVICE OR PROCESS, (2) ACCESS TO CUSTOMER RECORDS, AND (3) CELL PHONE TRACKING	§ § § § § § § § § §	MAGISTRATE NO. H-06-356M

BRIEF *AMICUS CURIAE* OF ELECTRONIC FRONTIER FOUNDATION AND CENTER FOR DEMOCRACY AND TECHNOLOGY IN REGARD TO COURT'S MAY 24, 2006 ORDER ON POST-CUT-THROUGH DIALED DIGITS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Law Review Articles and Treatises

The Electronic Frontier Foundation ("EFF") and the Center for Democracy and Technology ("CDT") file this brief *amicus curiae* in support of the Court's denial of applications by the United States ("the Government") for orders authorizing collection of "post-cut-through dialed digits under the Pen/Trap Statute," Order of May 24, 2006 ("Order"), and in opposition to the Government's June 16, 2006 brief ("Government Brief") arguing against that denial.[1]

Although correctly denying the Government "access to any post-cut-through dialed digits which could possibly reveal call contents," Order at 1, Gov't Br. at 1, the Court has permitted the Government to reargue the proposition that it may obtain post-cut-through dialed digits under the Pen/Trap Statute, 18 U.S.C. §§ 3121-3127. *Amici* respectfully submit that the Government's applications cannot be granted without violating federal statutes and the Fourth Amendment, and that the Government must obtain a probable cause warrant under the procedures of the Wiretap Act, 18 U.S.C. §§ 2510-2522, in order to collect any post-cut-through dialed digits ("PCTDDs").

Part I of this brief addresses the relevant statutes' origins in the Supreme Court's Fourth Amendment precedents, concluding that, as a constitutional matter, PCTDDs may only be acquired with a search warrant. Part II explains why, as a statutory matter, PCTDDs may not be acquired under the Pen/Trap Statute and counters the Government's argument that 18 U.S.C. § 3121(c) supports a contrary result. Finally, Part III briefly addresses the Court's question regarding the availability of technology distinguishing between PCTDDs that do and do not contain content, and explains how the Government's investigative needs may be served without violence to the Constitution or the statute's plain language.

---

[1] EFF's interests as *amicus* are set forth in its June 14, 2006 motion, which sought leave for EFF and other parties who may join EFF to file this brief and was granted in the Court's order of June 15, 2006. EFF is joined by CDT, a non-profit public interest and Internet policy organization that seeks to represent the public's interest in an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty. CDT and its senior staff have been directly involved in legislative, judicial, and administrative proceedings concerning wiretapping since before the passage of ECPA in 1986, and CDT was a lead petitioner challenging the FCC on "post-cut-through dialed digits" in the *U.S. Telecom Ass'n v. FCC* case discussed below. *Amici* have not seen the Government's applications or the Court's specific orders denying them, and are unaware of the facts of any case before this Court.

I. Telephone Communications Content is Protected by the Fourth Amendment

The contents of telephone communications are fully protected by the Fourth Amendment. *Katz v. United States*, 389 U.S. 347, 353-354 (1967). The Government must satisfy stringent procedural requirements before it can acquire the contents of communications. *Berger v. New York*, 388 U.S. 41, 63-64 (1967) ("[I]t is not asking too much that officers be required to comply with the basic command of the Fourth Amendment before the innermost secrets of one's home or office are invaded. Few threats to liberty exist which are greater than that posed by the use of eavesdropping devices."). Congress implemented these requirements in the Wiretap Act. 18 U.S.C. §§ 2510-2522. *See, e.g.*, 18 U.S.C. § 2518(1) (detailed affidavit requirements for application); *id*., § 2518(3) (probable cause and necessity determination by judge); *id*., § 2518(4) (detailed warrant requirements); *id*., § 2518(5) (duration and minimization requirements).

By contrast, the Supreme Court has found no reasonable expectation of privacy in telephone numbers dialed or transmitted to initiate telephone calls. *Smith v. Maryland*, 442 U.S. 735, 745 (1979); *id*. at 742-744 (pen register does not "acquire the contents of communication," but only "numerical information" that is "voluntarily conveyed…to the telephone company" so that calls may be completed).[2] Accordingly, the Pen/Trap Statute provides comparatively limited judicial oversight of pen/trap devices. *See, e.g.,* 18 U.S.C. § 3122(b) (application to court need only "certify" that information likely to be obtained is "relevant to a criminal investigation"); *id*., § 3123(a) (court may grant application based only on certification).

---

[2] For purposes of this brief, *amici* adopt the content/non-content distinction. However, *amici* do not endorse the reasoning of *Smith v. Maryland*, which has been repeatedly criticized by legal scholars. *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1137-1138 (2002); Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 524-528 (2005); Anita Ramasastry, *Lost In Translation? Data Mining, National Security and the "Adverse Inference" Problem*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 757, 764-766 (2006). Moreover, *amici* do not believe that *Smith* validates modern practice with respect to pen registers and trap and trace devices. *See generally* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act,* 69 S. CAL. L. REV. 949. 982-989 (1996) (discussing the limited capacity of the pen/trap devices analyzed in *Smith* and explaining how modern pen/trap devices collect far more information).

As described below, PCTDDs contain communications content that is not used to connect calls, and their acquisition is therefore governed by the Supreme Court's requirements in *Berger* (and therefore the Wiretap Act) as opposed to *Smith* (and therefore the Pen/Trap Statute). The government ignores this constitutional issue, but it is unavoidable if this Court construes the Pen/Trap Statute to authorize collection of communications content, contrary to its plain language.

II. The Pen/Trap Statute by its Plain Meaning Prohibits the Acquisition of Post-Cut-Through Dialed Digits

A. The Pen/Trap Statute Does Not Authorize the Acquisition of Communications Content

The Pen/Trap Statute empowers the Court to issue an order "authorizing the installation and use of a pen register or trap and trace device" upon application and proper certification by the government.[3] 18 U.S.C. §§ 3122, 3123. In pertinent part, "pen register" is defined as:

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

18 U.S.C. § 3127(3) (emphasis added). Similarly, "trap and trace device" is defined in pertinent part as:

> A device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, or 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) (emphasis added). As the emphasized language plainly states, pen/trap devices *cannot* record, decode or capture information that includes the contents of *any* communication, *by definition*. The legislative history of the Pen/Trap Statute, enacted as part of the Electronic Communications Privacy Act of 1986 ("ECPA"), is equally clear that pen/trap devices cannot obtain content, but only non-content information used to connect calls:

---

[3] *Amici* will refer to pen registers and trap and trace devices as "pen/trap devices" except where drawing a distinction between the two is necessary to the discussion.

> The term "pen register" means a device which records or decodes electronic or other impulses which identify the *numbers dialed or otherwise transmitted for the purpose of routing telephone calls*, with respect to wire communications, on the phone line to which such device is attached. The term does not include the contents of a communications, rather it records the numbers dialed.

H.R. Rep. No. 99-647, at 78 (1986) (emphasis added). The government's acquisition of communications content, by contrast, is governed by the strict procedures of the Wiretap Act, which requires the government to apply for and be issued a special warrant. 18 U.S.C. § 2518.

B. Post-Cut-Through Dialed Digits are Communications Content

Post-cut-through dialed digits are those dialed by an individual after a call has been connected, *i.e.*, has been "cut through." *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 456 (D.C. Cir. 2000). As the Government concedes, and as this Court has recognized, PCTDDs can include communications content. Order 1 (PCTDDs "can represent call content, such as bank account numbers, Social Security numbers etc."); Gov't Br. at 4, citing *U.S. Telecom Ass'n*, 227 F.3d at 456 (D.C. Cir. 2000) (PCTDDs "can represent call content, such as when subjects call automated banking services and enter account numbers, or call voicemail systems and enter passwords, or call pagers and enter call-back telephone numbers (which are considered numeric messages)"); *see Brown v. Waddell*, 50 F.3d 285, 293-294, 294 n. 11 (4th Cir. 1995) ("pager clone" used by law enforcement to monitor numbers received by a suspect's digital display pager was not a "pen register," as it was "undisputed" that a caller can "convey coded messages of unlimited substantive content" to a pager subscriber).

As the D.C. Circuit further described, PCTDDs "include not only the telephone numbers dialed after connecting to a dial-up long-distance carrier (*e.g.*, 1-800-CALL-ATT) but also... credit card or bank account numbers dialed in order to check balances or transact business using automated telephone services," *U.S. Telecom Ass'n*, 227 F.3d at 456, and therefore can "represent call content." *Id.* at 462 ("subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers."). For this reason "it may be that a Title III [Wiretap Act] warrant is

required to receive all post-cut-through digits." *Id.*; *see also In re Application of the United States of America for an Order Authorizing the Use of a Pen Register and Trap on [xxx] Internet Service Account/User Name [xxxx@xx.com]*, 396 F. Supp. 2d 45, 48 (S.D. Mass. 2005) (the acquisition of PCTDDs that reveal content is not authorized under the Pen/Trap Statute).

Amici contend that the D.C. Circuit's tentative conclusion in 2000 that a warrant under the Wiretap Act is required to receive all PCTDDs was correct. Moreover, as detailed more fully below, any uncertainty on this point was eliminated in 2001 when Congress amended the Pen/Trap Statute to flatly and without exception forbid the collection of content. Indeed, any device that has the capability of collecting PCTDDs that contain content cannot be a pen/trap device. *See Brown*, 50 F.3d at 293-294, 294 n. 11 (controlling distinction between pen/trap and interception devices is "the capability of the former to record only outgoing or incoming telephone numbers, [and] of the latter, to record messages with substantive content"; key issue is "*capability*" of device to receive content, "whether or not it happens to do so during a particular period of interception") (emphasis in original); *see also People v. Bialostok*, 610 N.E.2d 374, 378 (N.Y. Ct. App. 1993) (devices that can acquire communications contents cannot be authorized under Pen/Trap Statute).

Therefore, even if *some* PCTDDs are non-content "dialing, routing, signaling or addressing" ("DRAS") information, the Pen/Trap Statute cannot authorize their capture, because other PCTDDs are likely to contain content. [4] Indeed, it is likely that the vast majority of PCTDDs contain content. Over the past twenty years, there has been a dramatic rise in the use of dialed digits to conduct substantive transactions over the telephone; a wide range of services now use PCTDDs for interactive prompting and responses. Therefore, the proportion of PCTDDs

---

[4] *Amici* further contend that *all* PCTDDs contain content, i.e., all PCTDDs are, from the perspective of the originating local carrier, indistinguishable from any other content transmitted post-cut-through, and absent a warrant under the Wiretap Act, telephone numbers transmitted to a second carrier may only be acquired via a pen-trap device installed with the second carrier. However, the Court need not agree with this position in order to conclude that the Pen/Trap Statute cannot authorize capture of PCTDDs.

used to connect to a second communi cations carrier is likely to be relatively small, and the risk that PCTDDs will include content is not incidental. As detailed in the f ollowing subsectio n, Congress responded to this rise in the use of di aled digits as content by am ending the Pen/Trap Statute to make clear that it cannot be used to obtain any content.

C. The Privacy-Protective Provision at 18 U.S.C. § 3121(c) is Not an Implicit Authorization for the Acquisition of Content

The Government's *only* argument in the face of the Pen /Trap Statute's plain limitation to non-content is a construction of 18 U.S.C. § 3121(c) that either ignores or m isconstrues the legislative history of the statute, which indica tes a clear Congressional intent to preclude the collection of any content via pen/trap device.

The original definitions of pen/trap devices did not *explicitly* prohibit the collection of content. Fo r exam ple, a "pen reg ister" was de fined as "a device which records or decodes electronic o r oth er im pulses which iden tify nu mbers dia led or o therwise tran smitted on the telephone line to which such device is attached." 18 U.S.C. § 3127(3) (1986); *see also id*. at § 3127(4) (definition of "trap and trace device"). However, Congress intended that the term "pen register" "does not include the contents of a comm unication, rather it records the num bers dialed." H.R. Rep. No. 99-647, at 78 (1986). In 1986, when the Pen/Trap Statute was adopted, most phones were still rotary and the possibility of using PCTDDs as content in banking or other transactions was not a significan t issue. Because Congress assum ed that dialed num bers did no t include content, an explicit prohib ition on content collect ion was unnecessary. *See Bialostok*, 610 N.E.2d at 378 ("The traditional pen register considered in *Smith v. Maryland* was, to la rge extent, self-regulating. Neither through police m isconduct nor th rough inadvertence could it reveal to an yone any in formation in which the telephone us er had a leg itimate expectation of privacy.").

However, by 1994, when Congress was consider ing the Communications Assistance for Law Enforcement Act, it had become clear that dialed digits were b eing used to communicate a wide variety of content, as reflected in the following exchange between Senator Leahy and FB I

Director Freeh:

> SEN. LEAHY: You say this would not expand law enforcement's authority to collect data on people, and yet if you're going to the new technologies, where you can dial up everything from a video movie to do your banking on it, you are going to have access to a lot more data, just because that's what's being used for doing it.
>
> MR. FREEH: I don't want that access, and I'm willing to concede that. What I want with respect to pen registers is the dialing information, telephone numbers which are being called, which I have now under pen register authority. As to the banking accounts and what movie somebody is ordering in Blockbuster, I don't want it, don't need it, and I'm willing to have technological blocks with respect to that information, which I can get with subpoenas or other process. I don't want that in terms of my access, and that's not the transactional data that I need.

Joint Hearing on Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technology and Services: Hearings Before the Subcomm. on Technology and Law of the Senate Judiciary Comm. and the Subcomm. on Civil and Constitutional Rights of the House Judiciary Comm., 103d Cong., 2d Sess. 50 (1994).[5]

As a result of this new concern over the collection of content via pen/trap devices, and in response to Director Freeh's willingness to accept "technological blocks" with respect to such information, Congress included in CALEA a provision to "further *protect[] privacy* …by *restricting* the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information." S. Rep. No. 103-402, at 31 (1994) (emphasis added); *see also* H.R. Rep. No. 103-827, at 32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3512 (provision "*requires* government agencies…to use, when reasonably available, technology that restricts the information captured by [a pen register] to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured." (emphasis added). When first enacted in 1994, this new privacy-protective provision--18 U.S.C. § 3121(c)--stated:

> *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

---

[5] *Available at* http://www.eff.org/Privacy/Surveillance/CALEA/freeh_031894_hearing.testimony.

dialing and signaling information utilized in call processing.

Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, § 207, 108 Stat. 4279, 4292 (1994). [6] Congress recognized that PCTDDs might inappropriately deliver content to law enforcement with a pen/trap device, but it thought that the problem could be solved by the application of technology at the government's end that would distinguish between content PCTDDs and signaling PCCTDs.

However, by 2001, when Congress was considering the USA PATRIOT Act, it became clear that 18 U.S.C. § 3121(c) had not solved the problem, as the "technological blocks" necessary to effectively protect dialed digit content still did not exist. Instead, the government admitted that there was no technology available to it that allowed it to distinguish content from non-content PCTDDs. As a high-ranking Congressional staffer explained:

> The FBI had advised Senator Leahy in June 2000 that pen register devices "do capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party." As Senator Leahy noted, the impulses made after the call is connected could reflect the electronic banking transactions a caller makes, or the electronic ordering from a catalogue that a customer makes over the telephone, or the electronic ordering of a prescription drug. Confronted with this fact, the administration agreed that the pen register and trap and trace laws should expressly exclude the use of such devices to intercept "content," which is broadly defined in 18 U.S.C. 2510(8), and this addition was made to section 216 of the USA PATRIOT Act.

Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145, 1198 (2004) (citing 147 Cong. Rec. S11,000 (daily ed. Oct. 25, 2001) (indicating that the FBI had informed Senator Leahy that there had been no change in technology to better restrict the recording or decoding of dialing and signaling information to exclude content)). Therefore, to address the concern that had not been fully addressed by CALEA's addition of 18 U.S.C. § 3121(c), Congress explicitly prohibited even the incidental delivery of PCTDDs, amending the definitions of "pen register" and "trap and trace device" to explicitly prohibit the collection of

---

[6] Congress later amended § 3121(c) to include trap and trace devices and to extend the Pen/Trap Statute to reach electronic networks. Gov't Brief at 6. This amendment is not relevant to *amici's* analysis.

any communications content. *See* 18 U.S.C. §§ 3127(3), 3127(4) (information recorded, decoded or captured by pen registers or trap and trace devices, respectively, "shall not include the contents of any communication").

Placed in this context, it is plain that 18 U.S.C. § 3121(c) is exactly what it purports to be: a "limitation" on the Government's ability to collect content via pen/trap devices. Yet the Government argues, perversely and without support, that this "limitation" expands the Government's authority under the Pen/Trap Statute. Gov't Br. at 6 ("Section 3121(c) conclusively declares that…the Government is not barred from receiving…information simply because it may contain content."). The Government essentially argues that even though the explicit language of the Pen/Trap Statute precludes the use of pen/trap devices to collect content, pen/trap devices may nevertheless do so if no reasonably available technology can restrict collection to non-content. This argument is not only absurd in light of the legislative history, but also fails purely as a matter of statutory construction.

First, as a threshold matter, the Government ignores the fact that § 3121(c) was amended in 1994, seven years before Congress flatly barred the use of pen/trap devices to obtain *any* content in § 3127. This Court should not entertain the Government's strained reading of § 3121 – enacted in 1994 – as an exception to a completely unqualified prohibition enacted in 2001.

Second, the text of § 3121(c) presumes that the "Government agency" be "authorized to install and use" a pen/trap device "under this chapter" in the first place. Therefore, § 3121(c) does not govern this Court's decision as to what devices may be authorized, and no pen/trap device lawfully authorized "under this chapter" may collect communications content. 18 U.S.C. §§ 3127(3), (4); *cf. Brown v. Waddell, supra*.

Third, both the Supreme Court and Congress have clearly distinguished communications content from non-content, and the Pen/Trap Statute expressly prohibits pen/trap devices from collecting communications content. This specific, patent restriction necessarily precludes any contrary reading of a "limitation" provision. *Busic v. United States*, 446 U.S. 398, 407 (1980) ("a more specific statute will be given precedence over a more general one").

Finally, the Government's reading of § 3121(c) should be rejected under the canon of constitutional avoidance because permitting the collection of communications content without a warrant based on probable cause creates significant Fourth Amendment issues. *Harris v. United States*, 536 U.S. 545, 555 (2002) ("when ' a statute is susceptible of two constructions, by one of which grave and doubtful constitutional questions arise and by the other of which such questions are avoided, our duty is to adopt the latter'") (citation omitted).

Were the Court to accept the Government's highly strained reading of § 3121(c), not only would it ignore the express will of Congress and settled canons of statutory construction, it would also create a *de facto* exception to the Wiretap Act that permits the Government to violate the Fourth Amendment. The Court should not expand the law in such an unjustifiable manner.[7]

III. Reasonable Alternatives are Available to the Government

The Court also asked whether there exists reasonably available technology that allows the Government to separate call-identifying PCTDDs from those that are content.[8] Amici are unaware of any such technology, nor was the FCC in 2002. In the Matter of Communications Assistance for Law Enforcement Act, *Order on Remand*, CC Docket No. 97-213, ¶ 82 (2002) ("Order on Remand"). Nevertheless, the Government has other, lawful means of acquiring PCTDD. A pen/trap order that excludes PCTDD will reveal whether the surveillance target is

---

[7] The Government attempts to salvage its position by insisting that where content is collected, "no affirmative investigative use shall be made of that information except to prevent immediate danger of death, serious bodily injury, or harm to the national security." Gov't Brief at 9, quoting Deputy Attorney General Larry Thompson, *Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices* (May 24, 2002). Yet the need for such a voluntary pledge only underscores the fact that the Pen/Trap Statute lacks any "minimization" requirement because it does not contemplate the "overcollection" of content – unlike the Wiretap Act, which specifically provides for post-collection minimization. 18 U.S.C. § 2518(5). Had Congress anticipated that content could be swept up by a pen/trap device, it would certainly have required minimization. The absence of such a requirement makes clear that Congress did not expect content to be collected.

[8] Because *amici* do not have access to Exhibit A of the Government Brief, which explains the Government's position as to the reasonable availability of technology for separating content from non-content in post-cut-through dialed digits, the discussion here is minimal.

dialing a secondary carrier as opposed to a bank or pharmacy; the Government may then use procedures under 18 U.S.C. § 2703 of the Stored Communications Act to obtain PCTDD from the secondary carrier. Alternatively, the Government can obtain a wiretap order as to the primary carrier.

Finally, *amici* note that even after the PATRIOT Act's amendment of § 3121(c), the FCC specifically declined to allow law enforcement agencies to "extract dialed digits on content channels using their own decoders" because such power would conflict with CALEA's requirement that carriers take measures to ensure the privacy and security of communication data not authorized to be intercepted. Order on Remand, ¶ 88. Instead, the FCC believed the Government should seek appropriate court orders to authorize electronic surveillance, and then obtain the desired information from carriers, which have the technical capability to provide the information. *Id*. ¶ 89.

IV. Conclusion

For the foregoing reasons, the Governm ent's applications for orders authorizing collection of post-cut-through dialed digits under the Pen/Trap Statute should be denied.

DATED: June 30, 2006

Respectfully submitted,

By _____

Kevin S. Bankston
Lee Tien
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Telephone: (415) 436-9333 x 126
Facsimile: (415) 436-9993

James X. Dempsey
John B. Morris
CENTER FOR DEMOCRACY AND TECHNOLOGY
1634 Eye Street NW #1100
Washington DC, 20006
Telephone: (202) 637-9800
Facsimile: (202) 637-0968