UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE GOVERNMENT APPLICATIONS SEEKING AUTHORIZATION TO INTERCEPT ALL PCTDD VIA A PEN REGISTER ORDER	:	**06 Misc. 547 (JMA)** **06 Misc. 561 (JMA)**

MEMORANDUM OF LAW BY AMICUS CURIAE
FEDERAL DEFENDERS OF NEW YORK

FEDERAL DEFENDERS OF NEW YORK, INC.
APPEALS BUREAU
52 Duane Street, 10th Floor
New York, New York 10007
Tel.: (212) 417-8742

Attorney for Amicus Curiae

YUANCHUNG LEE,
Of Counsel.

TO: **ROSLYNN R. MAUSKOPF, ESQ.**
United States Attorney
Eastern District of New York
147 Pierrepont Street, 16th Floor
Brooklyn, New York 11201
Attn.: **JED DAVIS, ESQ.**
Assistant United States Attorney

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND OTHER AUTHORITIES

MISCELLANEOUS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN RE GOVERNMENT APPLICATIONS SEEKING AUTHORIZATION TO INTERCEPT ALL PCTDD VIA A PEN REGISTER ORDER	:	**06 Misc. 547 (JMA)** **06 Misc. 561 (JMA)**

MEMORANDUM OF LAW BY AMICUS CURIAE
FEDERAL DEFENDERS OF NEW YORK

INTRODUCTION

The Federal Defenders of New York ("FDNY") submits this Memorandum of Law, at the Court's invitation, as amicus curiae in connection with the Government's pending applications seeking to intercept and capture, via solely a Pen Register Order issued pursuant to 18 U.S.C. § 3123, all "post-cut-through dialed digits" ("PCTDD") generated by the target telephones. The Government has submitted a Memorandum of Law in support of its applications. See "Government's Memorandum of Law in Support of Its Request for Authorization to Acquire Post-Cut-Through Dialed Digits via Pen Registers," by Assistant United States Attorneys Jed Davis and Scott Klugman, dated January 19, 2007 ("Gov. Br.").[1]

Three courts have considered the precise issue before this Court, and all have rejected the Government's request to acquire

[1] The Government subsequently filed a supplemental letter-brief discussing two Florida decisions, see infra, which were unmentioned in its original brief. See Letter of AUSA Jed Davis, dated January 31, 2007.

PCTDD via a Pen Register Order based upon the plain and clear language of the relevant statute. See In the Matter of the Application of the United States for an Order Authorizing [] Installation and Use of a Pen Register and Trap and Trace Device or Process, 441 F. Supp.2d 816 (S.D. Tx. 2006) ("Tx. Op.") (attached as Exhibit A); In the Matter of the Application of the United States of America, Case No. 6:06-mj-1130 (Magistrate Judge Spaulding) (M.D. Fl. May 23, 2006) ("Fl. Mag. Op.") (attached as Exhibit B); In the Matter of the Application of the United States, Case No. 6:06-mj-1130 (District Judge Conway) (M.D. Fl. June 20, 2006) ("Fl. Dist. Op.") (attached as Exhibit C). This Court should do the same.

First, the plain language of 18 U.S.C. §§ 3127(3) & (4), as well as § 3121(c), requires rejection of the Government's applications. Congress has specifically and explicitly barred the use of either a pen register or "trap and trace device"[2] to "record" or "capture" communications content, and the Government concedes that PCTDD include content. The Court therefore need not go beyond the statutory text to reject the Government's request to intercept PCTDD content via a Pen Register Order. See infra Point

[2] A trap-trace device is simply a pen register in reverse -- its core function is to capture the phone numbers of incoming calls to the target telephone rather than the phone numbers of outgoing calls dialed from the target telephone. E.g., Orin S. Kerr, Internet Surveillance Law after the USA PATRIOT Act, 2003 Nw. U. L. Rev. 607, 632-33 (2003). There is no difference, either as a constitutional or statutory matter, between the two devices.

I.

Second, well-established law requires the Government to obtain at least a warrant issued upon a showing of probable cause of criminality -- and not merely a Pen Register Order issued upon a mere "certification of relevance" -- before conducting surveillance that captures "hybrid" communications, i.e., communications containing both Fourth Amendment-protected content and unprotected non-content. Cases arising from Government efforts to intercept or search the contents of digital pagers -- devices capable only of receiving and storing numbers, some of which qualify as non-content (e.g., telephone numbers) and some of which qualify as content (e.g., coded communications) -- demonstrate that persons have Fourth Amendment-protected privacy interests in hybrid information and that therefore the Government cannot acquire such information through a mere Pen Register Order. PCTDD, like pager communications, constitute hybrid communications. See infra Point II.

Third, this Court should reject the Government's "ju-jitsu" reading of § 3121(c) -- a reading that perversely transforms an explicit "limitation" on Government power into an implicit conferral of additional, unmentioned power. The Government's unnatural reading contradicts the plain language of § 3127(3) & (4), does not jibe with the statutory text of § 3121(c) itself, and converts § 3121(c) into an unconstitutional statute authorizing

Government surveillance of communications contents on a standard far lower than probable cause. See infra Point III.

Finally, while the Government spends much time trawling legislative history from 1994 and 2001 for stray comments purportedly supporting its reading of § 3121(c), see Gov. Br. 22-32 & all attached exhibits, this Court need not -- and should not -- consult extraneous sources because the plain language of §§ 3127 & 3121 bars the Government from acquiring content through a Pen Register Order. E.g., Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997) ("Our inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent."). But even if this Court were to consider legislative history, the result would be the same: Congress understood that the Government could not, as a constitutional matter, acquire content on less than probable cause, and therefore specifically barred the use of pen registers and trap-trace devices, installed upon a showing of mere relevance, to capture content. See infra Point IV.[3]

[3] Amicus has benefitted from the amicus brief filed by the Electronic Frontier Foundation ("EFF") in the Texas case, as well as from discussions with EFF attorney Kevin Bankston. A copy of the EFF's amicus brief in the Texas case is attached as Exhibit D.

BACKGROUND

1. The Fundamental Distinction Between Content and Non-Content

Regardless of the medium (e.g., the mail, the telephone, or the Internet), surveillance law is guided by the fundamental distinction between "content" and "non-content," i.e., between the substance of a communication and the "envelope" or "addressing" information concerning that communication. E.g., Orin S. Kerr, Internet Surveillance Law after the USA PATRIOT Act, 2003 Nw. U. L. Rev. 607, 611-16 & 641 (2003). Essentially, while communications content is protected by the Fourth Amendment (and thus requires at least a warrant issued upon probable cause before it can be captured), non-content is not and therefore may be acquired upon a lesser showing. The constitutional distinction is mirrored in the statutory scheme, which accords far greater protection to content than to non-content.

Content is defined broadly as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8). In the context of postal mail, "the content information is the letter itself, stored safely inside its envelope." Kerr, supra, at 611. For telephone calls, the content is simply the substance of the call, usually an actual conversation between the participants. Id. For e-mail communications, content is the body or text of the e-mail. Id. at 612.

Non-content (or "envelope") information is addressing or routing information concerning a particular communication. In the context of postal mail, it refers to "information derived from the outside of the envelope," for instance the addresses of the sender and recipient. Kerr, supra, at 611. For telephone calls, "envelope information includes the number the caller dials, the number from which the caller dials, the time of the call, and its duration." Id. For e-mail communications, envelope information is that contained in the "mail header," which describes the origin, route, and destination of a particular e-mail. Id. at 612.

The distinction between content and non-content is of constitutional significance. Content, on the one hand, has been accorded full protection under the Fourth Amendment since Katz v. United States, 389 U.S. 347, 353-54 (1967), in which the Court held that persons have legitimate privacy interests in the substance of their telephone conversations and thus that the Government's warrantless eavesdropping was unconstitutional. See also 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."). Envelope information, on the other hand, has not been accorded Fourth Amendment protection. In Smith v. Maryland, 442 U.S. 735, 745

(1979), the Court held that a probable-cause warrant was not required before the police used a pen register to capture the telephone numbers dialed from the defendant's telephone. This was because no legitimate privacy interest exists in non-content envelope information, such as dialed telephone numbers. 442 U.S. at 742.

Smith specifically distinguished Katz on the ground that pen registers capture only non-content envelope information, explaining that "a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications." 442 U.S. at 741 (emphasis in original). Pen registers, the Court ruled, "do not hear sound. They disclose only the telephone numbers that have been dialed -- a means of establishing communication." Id. (emphasis added), quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977); see id. at 167 ("Pen registers . . . do not acquire the 'contents' of communications, as that term is defined by 18 U.S.C. § 2510(8).").

The constitutional distinction is reflected in the statutory scheme established by Congress to regulate the Government's surveillance of various media. Katz's basic holding is embodied in the Wiretap Act, 18 U.S.C. §§ 2510-2522,[4] which requires the

[4] The Wiretap Act, commonly referred to as "Title III," has (continued...)

Government to demonstrate (at a minimum) probable cause of criminality before a eavesdropping warrant, authorizing the interception of the content of communications, can be issued. See 18 U.S.C. § 2518.[5] In turn, the Pen Register and Trap-Trace Device Statute, 18 U.S.C. §§ 3121-3127 (hereinafter "Pen/Trap Statute"), reflects Smith by requiring only a "certification" from a Government attorney that the "information likely to be obtained is relevant to an ongoing criminal investigation" before an Order authorizing the installation and use of a pen/trap device must be issued. 18 U.S.C. § 3122(b)(2).

It bears emphasizing that a court has no discretion in this matter: Upon presentation by a Government attorney of a

---

[4] (...continued)
existed since 1968. However, the Electronic Communications Privacy Act of 1986 ("ECPA") brought Title III within its fold by amending Title III to extend its prohibition on content interception -- originally reaching only "wire" and "oral" communications -- to e-mails and other "electronic" communications. Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 2004 Geo. Wash. L. Rev. 1557, 1564 (2004).

The ECPA "created the statutory framework of privacy protections and related standards for law enforcement access covering electronic communications and remotely stored electronic records." Id. at 1558. That basic structure, with some minor modifications, remains in place today. Id.

[5] The warrant required by the Wiretap Act has been called a "super-warrant" because the Act requires the Government to demonstrate to the issuing court's satisfaction not only probable cause of criminality but also, for instance, that other, less-invasive investigative techniques have failed (or are likely to fail). E.g., 18 U.S.C. § 2518(3).

"certification of relevance," a court must issue the desired Pen/Trap Order. A court must accept the certification on its face and may not conduct an "independent judicial inquiry into the veracity of the attested facts." In re Application of the United States, 846 F. Supp. 1555, 1558-59 (M.D. Fla. 1994). The judicial role "is ministerial in nature." United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995).

Because of the extremely low showing required for issuance of a Pen/Trap Order, Congress specifically defined pen/trap devices to preclude their use to capture Fourth Amendment-protected content. These devices, by definition, cannot be employed to "record" or "capture" content:

> **§ 3127. Definitions for chapter**
>
> As used in this chapter --
>
> . . .
>
> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . .
>
> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . .

18 U.S.C. § 3127 (2007) (emphases added).

To make the prohibition on "record[ing]" or "captur[ing]" communications content with pen/trap devices even clearer, Congress in another section of the Pen/Trap Statute specifically exhorted all Government agencies authorized to obtain a Pen/Trap Order to use whatever technology "reasonably available" to ensure that these devices are not misused to intercept content. This "limitation" is an additional congressional command, directed specifically to Executive Branch agencies, that pen/trap devices not be used to acquire content:

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

18 U.S.C. § 3121(c) (2007) (emphases added). By employing the terms "pen register" and "trap and trace device," defined elsewhere in the Pen/Trap Statute, this additional "limitation," addressed to the Government, thus assumes the definitional prohibition set forth in § 3127(3) & (4). Content may not be "record[ed]" or "capture[d]" by pen/trap devices, both as a matter of statutory definition and as congressional command.

2. PCTDD Contain Content

Post-cut-through dialed digits, or PCTDD, are "digits dialed after calls are connected or 'cut through.'" United States Telecom Assoc. v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000); accord Texas Op., 441 F. Supp.2d at 818 (PCTDD "are any numbers dialed from a telephone after the call is initially set up or 'cut through.'"). Occasionally, when a "party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party," PCTDD are simply telephone numbers. 441 F. Supp.2d at 818. Outside of the narrow context of credit-card calls, calls made using prepaid phone cards, collect calls, or other similar arrangements, however, PCTDD are digits that "transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like." Id. As the D.C. Circuit explained, PCTDD constitute "call content" in these familiar, everyday situations:

> For example, 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.

U.S. Telecom Assoc., 227 F.3d at 462. The Government concedes that such PCTDD constitute content. Gov. Br. 2.

Although amicus is not aware of statistics on this precise matter, it is likely that in this day and age, the large majority

of PCTDD is content. Though calling cards and the like are still sometimes used, most digits punched after a call has been completed represent content information such as passwords and account numbers. Uses of the telephone for these everyday purposes, where the PCTDD generated are indisputably content, surely outnumber instances in which calling cards and such are employed.

3. Current State of Technology

Amicus is informed that the Court has conducted a sealed ex parte proceeding in which the Government claimed that no technology currently available is capable of sorting, with 100% accuracy, PCTDD that constitute content from PCTDD that do not. Gov. Br. 5. This is the same assertion made by the Government in the Texas litigation. See Tx. Op., 441 F. Supp.2d at 824.

The Government is apparently uninterested in developing or using technology capable of sorting PCTDD content from PCTDD non-content with anything less than 100% accuracy. 441 F. Supp.2d at 824 & n.17; see also infra Point III (discussing Government's reading of § 3121(c)). For instance, available technology is likely capable of capturing only PCTDD that number precisely 10 digits dialed in an uninterrupted sequence -- the number of digits in a phone number dialed after an initial credit-card or calling-card call has been cut-through (i.e., the 3-digit area code plus the 7-digit local phone number). Excluding PCTDD with fewer or more than 10 digits would likely eliminate the capturing of the

vast majority of content-PCTDD. Yet because such technology would not capture all possible non-content PCTDD with 100% accuracy (for instance, a call to a phone in a foreign country), the Government currently "employs no filtering technology" whatsoever. Tx. Op., 441 F. Supp.2d at 823.

It is undisputed, in any event, that technology has long been available to sort pre-cut-through dialed digits -- i.e., digits dialed before a call has connected -- from post-cut-through digits.[6] Pre-cut-through digits are necessarily non-content -- they are simply the phone numbers dialed by the target telephone. Restricting a pen register to capturing only pre-cut-through digits, therefore, guarantees that no content is captured. A Department of Justice manual mentions a similar method of preventing the capture of content:

> **Caveat.** Technology is available to limit the pen register device so that it only records a specified number of dialed digits, for example, the first 10 digits. . . . [Doing so would] eliminate the inadvertent collection of the "content" of a communication . . . .

R. Stabe, Electronic Surveillance – Non-Wiretap, at § 3.4, in Federal Narcotics Prosecutions, quoted in Tx. Op., 441 F. Supp.2d at 825.

[6] Amicus believes that this capability is part of the "J-Standard".

4. Prior Decisions Concerning PCTDD

As noted, three courts have considered the same question presented here -- whether the Government may capture and record PCTDD that include content with a mere Pen Register Order. All rejected the Government's application on the plain language of the Pen/Trap Statute, specifically the definitions of pen/trap devices set forth in § 3127(3) & (4) and the additional "limitation" on content acquisition set forth in § 3121(c). See Tx. Op., 441 F. Supp.2d at 826 ("Courts should not be in the business of crafting exceptions to unqualified proscriptions handed down by Congress. 'Shall not include contents' is not a precatory suggestion, it is a plain commandment."); Fl. Mag. Op. at 2 ("Congress was clear that content of communications cannot be captured by use of pen register and trap and trace devices."); Fl. Dist. Op. at 5 (describing § 3127(3) & (4) as "flatly prohibiting the interception of communication content by pen registers and trap-and-trace devices").[7]

[7] Two earlier courts expressed skepticism in dicta about the Government's claim that it was authorized to acquire content PCTDD through a mere Pen/Trap Order. See United States Telecom Assoc., 227 F.3d at 462 (suggesting that "it may be that a Title III warrant is required to receive all post-cut-through digits"); In re Application of the United States, 396 F. Supp.2d 45, 47-48 (D. Mass. 2005) ("Would anyone doubt that although this action of dialing the second number [to punch in account numbers or passwords after the initial call has been completed] creates '. . . dialing, routing, addressing or signaling information . . . ,' the government would be prohibited from obtaining this information on a pen register because it contains the 'content' of a (continued...)

DISCUSSION

Point I

The Plain Language of the Pen/Trap Statute Requires Rejection of the Government's Applications.

1. Introduction

The plain text of the statute is of course the starting point in statutory interpretation. Barnhart v. Sigmon Coal Co., 534 U.S. 438, 450 (2002). If the text is clear and unambiguous, it is also the end point. Id. Consideration of sources beyond the text is both unnecessary and inappropriate when its language is plain. Robinson, 519 U.S. at 340 ("Our inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent."); accord Virgilio v. City of New York, 407 F.3d 105, 112 & 115 n.10 (2d Cir. 2005).

The plain language of the Pen/Trap Statute bars the Government from capturing content through a pen/trap device. The Government's effort to manufacture ambiguity out of clear statutory language fails badly, see infra Point III, and this Court need not consult extraneous sources to reject the Government's applications.

2. Pen/Trap Devices, by Definition, Do Not Acquire Content

Section 2511(a)(1) of Title 18 of the United States Code

---

[7] (...continued)
communication?").

generally bars anyone from "intentionally intercept[ing] . . . any wire, oral, or electronic communication." Congress then carved out specific exceptions to this general prohibition. These include when one of the parties to the intercepted communication has given consent, see 18 U.S.C. § 2511(2)(c)-(d); when the Government has obtained a wiretapping warrant, see id. § 2516; and when the interception is done pursuant to a valid Pen/Trap Order, see id. § 2511(2)(h).

The contours of the pen/trap exception to § 2511(a)(1)'s general bar on interception of wire and electronic communications are laid out in the Pen/Trap Statute, 18 U.S.C. §§ 3121-3127. To start, § 3121(a) states that "no person may install or use a pen register or trap and trace device without first obtaining a court order under section 3123 . . . ." Section 3123, in turn, provides that upon receiving an application from a Government attorney certifying that the information likely to be obtained through the use of the desired pen/trap device will be relevant to a criminal investigation, a court "shall enter an ex parte order authorizing the use of a pen register or trap and trace device anywhere within the United States." 18 U.S.C. § 3123(a)(1).

To understand the scope of an "order authorizing the use of a [pen/trap] device," we go to § 3127, which defines all terms used in the Pen/Trap Statute. See 18 U.S.C. § 3127 (entitled "Definitions for chapter"). Specifically, the two devices whose

use is authorized by a § 3123(a) order are defined as follows:

> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication . . .
>
> (4) the term "trap and trace device" means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided, however, that such information shall not include the contents of any communication . . .

18 U.S.C. § 3127 (2007). It bears emphasizing that § 3127 states the legal definition of pen/trap devices -- and a fortiori the lawful scope of a § 3123 Order authorizing their use. Section 3127 does not purport to describe, as a factual or technological matter, the actual workings or reach of devices that may otherwise be called "pen registers" or "trap-trace devices." Section 3127 simply provides that for purposes of the Pen/Trap Statute, pen/trap devices are solely (and simply) what its definitions prescribe.

Sections 3127(3) & (4) define pen/trap devices as mechanisms or processes that "record" or "capture" a particular category of "information." Membership of the class is defined both positively and negatively. Positively, § 3127 states that pen/trap devices capture "dialing, routing, addressing, or signaling information." Negatively, § 3127 excludes "the contents of any communication"

from the category of information capable of capture by pen/trap devices. Combining the positive with the negative, pen/trap devices are devices that, as a matter of law, "capture" "dialing, routing, addressing, or signaling information," but excluding "the contents of any communication." And to repeat: the ban concerns the "captur[ing]" or "record[ing]" (or, more simply, interception) of content through pen/trap devices, not simply the subsequent use of such information against the target.

Section 3127's ban on acquisition of content through pen/trap devices jibes with well-settled understanding concerning the reach of such mechanisms. As the Supreme Court long ago explained, "[p]en registers . . . do not acquire the 'contents' of communications, as that term is defined by 18 U.S.C. § 2510(8)." New York Telephone, 434 U.S. at 167; accord Smith, 442 U.S. at 741 ("[P]en registers do not acquire the contents of communication.") (emphasis in original); United States v. Rodriguez, 968 F.2d 130, 135 (2d Cir. 1992) (pen register "does not capture the contents of the communications"). Whatever a device that "capture[s]" or "record[s]" content may be, it is by definition not a pen/trap device.

3. Section 3121(c) Additionally Exhorts the Government Not to Misuse Pen/Trap Devices to Acquire Content

Section 3127's ban on content acquisition through pen/trap devices is reinforced and repeated in § 3121(c), in a slightly

different context. Section 3121(c) is explicitly addressed to "government agenc[ies] authorized to install and use" pen/trap devices, and exhorts them to employ "technology reasonably available" to ensure that only "dialing, routing, addressing, and signaling information" -- and not content -- is "record[ed]" or captured by their use of these devices. Section 3121(c) employs the terms "pen register" and "trap and trace device" (thus assuming and adopting their definitions as set forth in § 3127(3) & (4)), and is described specifically as a "limitation" on Government power:

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

18 U.S.C. § 3121(c) (2007). To repeat: By employing the terms "pen register" and "trap and trace device," terms of art defined elsewhere in the Pen/Trap Statute, Section 3121(c) necessarily adopts those definitions and the limits set forth therein. Whatever the precise scope of § 3121(c)'s "limitation," therefore, it cannot as a logical matter exceed the bounds established by § 3127's definitions.

The principal difference between § 3121(c) and § 3127 is the audience addressed. Section 3121(c), on the one hand, is directed

specifically to "government agenc[ies] authorized to install and use a pen register or trap and trace device under this chapter." It exhorts them to use reasonably available technology to ensure that pen/trap devices are not misused to acquire content. It "operates as an additional privacy safeguard," Fl. Dist. Op. at 5, an additional reminder to the Government that pen/trap devices shall not be used to intercept content. Section 3127, on the other hand, is more fundamental: It states that, by definition, pen/trap devices cannot be used to capture or record content (regardless of who is using the devices). It is the ultimate command, not merely an exhortation to a particular audience. The limits set forth in § 3127 are foundational; § 3121(c)'s "limitation" assumes those limits and cannot trump them.

4. Conclusion

The Pen/Trap Statute thus plainly and unambiguously bars the use of pen/trap devices to capture or record anything qualifying as "content." 18 U.S.C. §§ 3127(3), 3127(4) & 3121(c). PCTDD indisputably include content. The Government therefore cannot acquire PCTDD through a Pen/Trap Order. All three courts that have considered this question have reached this conclusion, see supra, and this Court should do so as well.

Point II

The Government Cannot Intercept Hybrid Communications (i.e., Communications Containing Both Content and Non-Content) on a Mere Showing of Relevance Because Such Interception Constitutes a Fourth Amendment "Search" and thus Cannot Be Justified by a Pen/Trap Order.

Although the precise question of whether PCTDD may be acquired through a Pen/Trap Order is a new one, the more fundamental and directly related question of whether the Government can lawfully intercept hybrid communications -- i.e., communications containing both Fourth Amendment-protected content and unprotected non-content -- based only on a showing of "relevance" (the standard for issuance of a Pen/Trap Order) is not. Courts have held that a pen/trap device cannot be used to intercept hybrid communications, both because doing so exceeds the essential nature of such devices and because persons have cognizable Fourth Amendment privacy interests in hybrid communications.

Numerous cases have analyzed Government efforts to intercept communications to or search the memory banks of digital-display pagers -- devices capable solely of receiving or storing a series of numbers, which can include non-content telephone numbers as well as numeric code messages qualifying as content. Courts have consistently ruled that such efforts constitute Fourth Amendment "searches," that they cannot be performed solely pursuant to a Pen/Trap Order, and that a wiretap warrant must instead be

obtained.

The Government's application here, seeking to use a pen register to intercept hybrid PCTDD, is directly analogous to earlier law-enforcement efforts to intercept the hybrid communications transmitted to digital pagers. Because a probable-cause warrant (or its equivalent) is required for the latter, it is also required for the former. This body of law further reinforces and confirms the plain reading of the Pen/Trap Statute set forth in Point I, supra: The Government cannot use a Pen Register Order to intercept PCTDD.

1. The Pager Clone Cases: Interception of Hybrid Pager Communications Cannot Be Conducted through a Pen/Trap Order

Before the proliferation of wireless cellphones in the mid-1990s, pagers were the device of choice for persons who wished to remain reachable even when not tethered to a land-line telephone. There were several kinds of pagers,[8] but the one relevant to the instant discussion is the "digital display pager." This device could only receive transmissions, and only numeric transmissions at that. See, e.g., Brown v. Waddell, 50 F.3d 285, 287 (4th Cir. 1995). A person who desires to reach the owner of the pager would

[8] Some pagers ("tone and voice pagers") are capable of receiving a brief voice transmission. Others ("tone only pagers") are capable only of signaling that someone had called and left a message, which the owner of the pager could retrieve by making a separate phone call. See generally Brown, 50 F.3d at 291. Neither is implicated here.

call the telephone number associated with the pager, and when connected, would punch in a series of numbers -- usually the phone number of the caller -- which would then be transmitted to the pager itself. The pager would indicate to its owner (by beeping or vibrating) that someone had called, and the owner could then access the numbers punched in by the caller by pressing a button on the pager.

While the "basic intended function of these pagers was to receive telephone numbers . . . , they could actually receive and display combinations of up to 24 (or 25) numbers and dashes in a single transmission." Id. at 287. Some of these numbers represent coded communications between the sender and the recipient, rather than telephone numbers. Id. at 292 (noting that while pagers "usually [] display telephone numbers . . . , [they also] receive and display an unlimited range of number-coded substantive messages"). As one court explained, "the pager device is capable of conveying substantive information by combining digits in various sequences. Both telephone numbers and coded messages may be conveyed." People v. Pons, 509 N.Y.S.2d 450, 453 (Sup. Ct. 1986).

Telephone numbers, of course, constitute non-content "envelope" information in which no Fourth Amendment privacy interest exists. See Smith, 442 U.S. at 742. Coded numeric messages, in contrast, constitute Fourth Amendment-protected content, since they plainly "concern[] the substance, purport, or

meaning of [a] communication." 18 U.S.C. § 2510(8). Communications transmitted to pagers are therefore of the hybrid variety, containing both content and non-content.

In Brown, a local police officer suspected that Brown was engaged in drug trafficking. 50 F.3d at 287. Knowing that Brown owned two digital pagers, the officer sought a Pen Register Order under § 3123 to conduct surveillance of her pager communications. Id. at 287 & 290. After receiving the § 3123 order, the officer obtained two "pager clones" from the pager company. Id. at 287. The clones "allowed [the officer] to receive any numeric messages sent to Brown's pagers at the same time that they were received and displayed on her pagers." Id.

The officer monitored Brown's pager communications for nearly a month. In so doing, "it is undisputed that [in addition to telephone numbers, the officer] intercepted a number of numeric messages containing more extensive sets of numbers than those in telephone numbers, including at least one that was conceded to be a code indicating that a caller which it identified was 'en route.'" Id. at 287-88. No incriminating information was discovered, however, and the police officer terminated his surveillance.

After Brown learned that the police had intercepted her pager transmissions, she sued the officer (and the city) for unlawful interception of her pager communications. Id. at 287-88. Brown

contended that the officer violated § 2511's general ban on interception of electronic communications by employing the pager clones. Id. at 288. In his defense, the officer claimed that the § 3123 Pen Register Order authorized his interception of Brown's pager communications. Id. The district court agreed with the officer, but the Fourth Circuit reversed on Brown's appeal, flatly rejecting the officer's contention that the § 3123 order authorized the interception of Brown's pagers.

"The dispositive issue," the Circuit explained, "is whether the use by [the officer] of pager clones to receive and record numeric messages [] simultaneously received by Brown's [] pagers was, for purposes of relevant law, effectively the use of a 'pen register.'" 50 F.3d at 289. After canvassing the language of the Pen/Trap Statute, case law (including Smith), and relevant legislative history, the court concluded that a pager clone is not the functional equivalent of a pen register. Id. at 291-93. Especially important is the court's conclusion that for pager clones "to retain pen register status," the "numbers capable of being [] transmitted by [Brown's pagers, and thus captured by the pager clones,] would have to be limited to raw telephone numbers." Id. at 293 (emphasis added).

And because it was undisputed that Brown's pager communications included both raw telephone numbers and "coded messages of unlimited substantive content," the "investigative

technique of using a [pager] clone . . . cannot be considered the use of a 'pen register' within the meaning of the ECPA." Id. at 294. Rather, the officer should have obtained a wiretap warrant before intercepting Brown's pager communications. As the Fourth Circuit explained, "That a digital display pager programmed to receive numeric transmissions has the capacity to receive by that means coded substantive messages . . . is what makes the interception subject to the authorization requirements of §§ 2516 & 2518." Id. at 294 n.11.

Other courts agree with Brown's conclusion that a device that intercepts hybrid communications, such as a pager clone, is simply not a "pen register." The Florida Supreme Court so held in State v. Jackson, 650 So.2d 24 (Fla. 1995), suppressing evidence in a criminal case obtained through surveillance conducted by a pager clone authorized under a pen register order. The court explained that "because the interception of a pager may disclose telephone numbers and coded messages . . . , monitoring a pager with a duplicate digital display pager is more intrusive than using a pen register or trap-and-trace device." Id. at 28. Instead of a pen register order, the Florida Supreme Court held, the police should have obtained a wiretap warrant. Id. at 29.

A New York court reached the same conclusion in People v. Pons, 509 N.Y.S.2d 450, 453 (Sup. Ct. 1986), finding that "[t]he monitoring of [a] telephone pager device is more intrusive than the

use of a pen register" because a pager "is capable of conveying substantive information by combining digits in various sequences. Both telephone numbers and coded messages may be conveyed." Because persons have Fourth Amendment-protected interests in those messages, "[t]he monitoring of a digital display [] pager poses a threat to the privacy of citizens" and thus requires a probable-cause warrant. Id. at 454.

Finally, in several other cases, including at least one from this District, the Government itself assumed and acknowledged that a wiretap warrant was required to intercept the hybrid communications transmitted to digital pagers. See United States v. David, 940 F.2d 722, 727 (1st Cir. 1991) (Government agents applied for wiretap warrant before using pager clone); United States v. Benjamin, 72 F. Supp.2d 161, 185-86 (W.D.N.Y. 1999) (same, and specifically explaining that "[t]he same standard for assessing probable cause governs an application to intercept electronic communications over a digital display pager as for a wiretap or eavesdropping warrant issued pursuant to 18 U.S.C. § 2518"); United States v. Persico, 1994 WL 36367 at *13, No. CR-92-00351 (CPS) (E.D.N.Y. Jan. 28, 1994) (Government sought wiretap warrant before "intercept[ing] transmissions to Fusco's beeper").

The lesson of all these cases, directly applicable to the PCTDD issue, is simple: Surveillance capturing hybrid communications (consisting of both non-content telephone numbers

and content numeric codes) cannot be conducted under a mere Pen Register Order but instead requires a wiretap warrant.

2. The Pager Memory Cases: Hybrid Information Is Protected by the Fourth Amendment

A closely related body of law concerns Government efforts to search the memory or storage of digital pagers in order to recover their contents. In these cases, courts consistently held that such efforts (often following the defendant's arrest) constitute Fourth Amendment "searches" because users of pagers possess recognized privacy interests in their contents, which include both telephone numbers and coded numeric messages.

Of course, if pager memories stored only non-content telephone numbers, the Fourth Amendment would not be implicated. As Smith held, persons have no cognizable privacy interests in telephone numbers dialed or received. 442 U.S. at 742 & 745. By holding that searches of pager memories are barred absent a search warrant or its equivalent, therefore, courts have accorded Fourth Amendment protection to hybrid information.

As former Chief Judge Mukasey of the Southern District of New York summarized, "courts have consistently held that the owner of an electronic pager has a legitimate privacy interest in numerical codes transmitted to the device . . . ." United States v. La Paz, 43 F. Supp.2d 370, 373 (S.D.N.Y. 1999). These cases include United States v. Ortiz, 84 F.3d 977, 983-84 (7th Cir. 1996) (upholding

search of pager memory under "search incident to arrest" exception to warrant requirement); United States v. Reyes, 922 F. Supp. 818, 832-33 (S.D.N.Y. 1996) ("This Court accepts Reyes' assertion, unopposed by the Government, that he had a reasonable expectation of privacy in the contents of his pagers' memories.") (emphasis added); and United States v. Chan, 830 F. Supp. 531, 534-35 (N.D. Cal. 1993) ("[Defendant] had a reasonable expectation of privacy in the contents of the pager's memory.").

3. Conclusion

The Government's applications seek to intercept hybrid communications, i.e., PCTDD, solely though a Pen Register Order issued upon a showing of mere relevance. The applications must be rejected because, as the above cases demonstrate, surveillance of hybrid communications (1) is outside the lawful reach of pen/trap devices, see supra Point II.1; and (2) constitutes a "search" intruding upon privacy interests protected by the Fourth Amendment, see supra Point II.2. A wiretap warrant issued under § 2516 is required before the Government can intercept hybrid communications.

Point III

The Government's Effort to Transform § 3121(c)'s Explicit "Limitation" into an Implicit Empowerment Fails Because It Contradicts the Unambiguous Definitions in § 3127 and Misreads the Plain Language of § 3121(c) Itself.

Undaunted by the plain language of the Pen/Trap Statute and abundant case law barring the use of pen/trap devices to capture communications containing content, the Government argues that § 3121(c) empowers it to obtain all PCTDD, including that qualifying as content, because no "technology reasonably available" ("TRA") can sort, with 100% accuracy, non-content PCTDD from content PCTDD. The unavailability of such technology, the Government asserts, frees it from the Pen/Trap Statute's ban on content acquisition and empowers it to acquire all PCTDD -- even if this involves the capturing of content on a mere showing of relevance.

This Court should reject the Government's argument because there is no ambiguity in § 3121(c)'s "limitation" on acquiring content through pen/trap devices. Section 3121(c) uses -- and thus assumes -- the definitions set forth in § 3127(3) & (4). Whatever else § 3121(c) may authorize, it cannot override the fundamental command embedded in those definitions: Pen/trap devices may not be used to acquire content.

The Government's effort also fails on its own terms -- it is a poor reading of § 3121(c). None of the concepts critical to its

construction of § 3121(c) -- for instance, the overriding command that the Government be permitted to capture all possible non-content; the need for 100% sorting accuracy in the TRA; the allowance of "incidental" capture of content; or a "minimization" requirement when capturing content -- appears in the statutory text. And the Government's newfound attempt to cure a fatal flaw in its reading, which permits the Government to obtain Fourth Amendment-protected content on a showing far lower than probable cause, by invoking the suppression remedy in § 2515 of the Wiretap Act fails badly. The plain language of § 2515, requiring suppression only of unlawfully intercepted "wire" and "oral" communications, proves that it does not apply at all to "electronic" communications, which is what PCTDD are.

A reading requiring so much imaginative projection must be rejected, especially when a far more natural reading, resting solely on the language of the text, is available: The Government may not use a pen/trap device to acquire communications content.

1. The Government's Reading of § 3121(c)

For convenience, we quote again the relevant provision:

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

the contents of any wire or electronic communications.

18 U.S.C. § 3121(c) (2007). As discussed above, the plain and natural reading of § 3121(c) is that it is an additional exhortation, directed specifically to the Executive Branch, to comply with the ban on content acquisition found in the definition of pen/trap devices in § 3127(3) & (4). See supra Point I.3. The ultimate command, embodied either in § 3127's definitions or in § 3121(c)'s direction to the Government, is identical: Thou shalt not acquire content with a pen/trap order.[9]

The Government, in contrast, reads § 3121(c) as follows:

> If there is TRA that enables a pen register to distinguish the processing information that is its target from contemporaneously-transmitted content, § 3121(c) requires the government to use that technology and as result [sic] acquire only the non-content. If there is no TRA that can make that distinction with complete accuracy, however, § 3121(c) only requires the government to operate the pen register using the TRA that exists -- even though the pen register may also obtain some content as it pursues processing information.
>
> Thus, provided the government uses what technology is reasonably available to avoid incidental access to content, 18 U.S.C. § 3121(c) permits a pen register incidentally to access the remainder that TRA cannot avoid. . . . [And because current] TRA has no [] capability to avoid the risk that a pen register collecting PCTDD non-content may also access PCTDD

[9] And as mentioned, technology is readily available to prevent the capture of content through a Pen Register Order. By configuring the pen register so that it captures only pre-cut-through dialed digits, for instance, the Government will have abided by the joint command of § 3121(c) and § 3127 that no content be captured by a pen/trap device.

> content[,] . . . [the Government] has satisfied 18 U.S.C. § 3121(c)'s precondition to incidental access to the remaining content, [and thus may capture] PCTDD content [through a Pen Register Order].

Gov. Br. 13-14 (emphasis in original). Here is more of the same, in a condensed form:

> 18 U.S.C. § 3121(c) obligates the government to use technology reasonably available to restrict a "pen register" to collecting processing information. Accordingly, to the extent that TRA permits, § 3121(c) serves to minimize the frequency with which a device that collects non-content . . . also acquires content. To the extent that the technology is not reasonably available to keep a "pen register" from accessing content in the course of collecting non-content, § 3121(c) creates a safe harbor that permits the incidental access to occur.

Gov. Br. 17-18. And to dampen concerns that the Government would use content acquired through pen/trap devices against the target, the Government assures the Court that such use would be barred by a section of the Wiretap Act, § 2515. There is no need to worry about possible abuses of the Pen/Trap Statute, the Government asserts, because § 2515 prohibits the Government "from using both the content in issue, as well as its fruits, unless that content was acquired in accordance with" the Wiretap Act. Gov. Br. 3; see id. 4, 12 & 18.

Unpacking these passages yields the following four core concepts. That none finds root in the text of § 3121(c) should be apparent.

First, the Government assumes that the overriding command of

§ 3121(c) is to ensure that the Government acquires all possible non-content through a pen/trap order. All other considerations are subsidiary; this goal must always be satisfied.

Second, the measure of whether the Government has complied with the Pen/Trap Statute boils down to whether it has employed "technology reasonably available" to minimize the acquisition of content, while capturing all non-content. If the Government uses TRA to reduce the amount of content captured in the course of capturing all possible non-content, it falls within a "safe harbor" permitting it to acquire this content, despite § 3127's content ban. Gov. Br. 18.

Third, the Government reads "technology reasonably available" to mean technology that "can make th[e] distinction [between content and non-content] with complete accuracy." Gov. Br. 13. Only technology capable of perfectly sorting content from non-content (so that the Government acquires all possible non-content) can qualify as the "reasonably available" technology mentioned in § 3121(c).

The three elements are intertwined: If TRA cannot perfectly distinguish content from non-content, then the Government is freed from the Pen/Trap Statutes's seemingly absolute ban on content acquisition. Instead, its sole obligation becomes the duty to "minimize" the "incidental" acquisition of content, while acquiring all possible non-content. Gov. Br. 18. Lack of perfect sorting

technology, in short, frees the Government to acquire content.

Fourth and finally, although the Government can capture content through a pen/trap device, it cannot use this information (or its fruits) against the target. Gov. Br. 3. Section 2515, allegedly, bars the affirmative use of communications content incidentally acquired through a Pen/Trap Order.

2. The Government's Readings Founders from the Start Because § 3121(c) Cannot Empower the Government to Do What § 3127's Definitions Bar It from Doing

The Government's effort to wrest an implicit empowerment out of the explicit "limitation" of § 3121(c) does not even get off the ground. Section 3121(c) uses the terms "pen register" and "trap and trace device," defined elsewhere in the Pen/Trap Statute. See 18 U.S.C. § 3127(3) & (4). Section 3121(c) thus assumes the definitions set forth in § 3127(3) & (4) and cannot extend the reach of these devices beyond the limits set forth in their very definitions.

Section 3127's definitions are logically prior to § 3121(c). Section 3121(c)'s "limitation" operates within the bounds set by the statutory definitions; it cannot exceed them. If any inconsistency exists, the definitions trump.

And as discussed extensively already, pen/trap devices by definition do not capture communications content. Point I.2, supra. A "pen register" is defined as a device or process that

"records" routing and signaling information, "provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127(3). Similarly, a "trap and trace device" is defined as a device or process that "captures" incoming routing and signaling information, "provided, however, that such information shall not include the contents of any communication." Id. § 3127(4).

It is hard to imagine how Congress could have stated the point more clearly. Pen/trap devices cannot be used to "capture" or "record" content.[10]

The Government attempts to deflect this fatal blow by claiming that the definitions in § 3127 are themselves ambiguous. Gov. Br. 15-16. It claims that the plain reading offered above is only one "possible interpretation." Gov. Br. 15. Another reading would permit the Government to use a Pen/Trap Order to capture content because a device qualifies as a pen/trap device so long as it is capable of capturing non-content routing or processing information, even if it sometimes also captures content. Id. at 15-16. As the

[10] There is in any event no inconsistency between § 3127 and § 3121(c). As noted, § 3121(c) has a different function than § 3127's definitions but nonetheless reinforces them: Instead of providing a generally applicable definition, as § 3127 does, § 3121(c) is specifically addressed to "government agenc[ies] authorized to install and use" pen/trap devices under the Pen/Trap Statute. Section 3121(c) "operates as an additional privacy safeguard," Fl. Dist. Op. at 5, an additional exhortation to the Government to abide by the ban on content acquisition embedded in § 3127(3) & (4). See generally supra Point I.3.

Government claims, "a device or process that records non-content 'dialing' information . . . meets the statutory definition [of pen/trap devices] at the time such non-content is recorded, regardless of whether at other times, the same device or process . . . obtains content . . . ." Id. at 16.

Amicus submits that this reading needs no rebuttal beyond the language of § 3127 itself.[11] Section 3127 plainly defines pen/trap devices as mechanisms or processes that capture routing or processing information, but which information "shall not include [] content." By definition, therefore, a pen/trap device is one that does not "record" or "capture" content. See 18 U.S.C. § 3127(3) & (4). The dual-function, content-acquiring device postulated by the Government's reading is simply not a pen/trap device within the meaning of the Pen/Trap Statute.

3. The Government's Reading Goes Far Beyond the Text of § 3121(c).

Even apart from its inconsistency with the definitions in § 3127, the Government's reading of § 3121(c) falters when considered on its own terms. It not only perversely transforms an explicit "limitation" on Government power into an enlargement of Government authority, but does so upon projections having no basis in the

[11] No one but the Government sees any ambiguity in § 3127, e.g., Tx. Op., Fl. Mag. Op., and Fl. Dist. Op., itself compelling evidence that the ambiguity is solely of the Government's imagination.

statutory text.

None of the four core components of the Government's reading finds root in the text. First and foremost, the Government assumes that § 3121(c)'s overriding command is to permit the Government to capture all possible non-content via a Pen/Trap Order and that all other considerations are secondary. But nothing in the Pen/Trap Statute supports this premise. While the Statute authorizes the use of a Pen/Trap Order to intercept non-content routing information, it says nothing about whether all non-content must always be captured, even if the cost of such acquisition is the "incidental" acquisition of content. Given the explicit ban on content acquisition via pen/trap devices found in both § 3127's definitions and § 3121(c)'s "limitation," the far more natural reading is that the Government's access to non-content is circumscribed by the content prohibition: The Government may acquire non-content with a Pen/Trap Order, but not at the cost of capturing content.

As the Texas court put it, the Government's "minimize content but allow all non-content" reading of § 3121(c) fits the statutory text far more poorly than the alternative reading -- "maximize non-content [when possible], but disallow all content." Tx. Op., 441 F. Supp.2d at 824-25. The only absolute in § 3121(c) and § 3127, after all, is the ban on content acquisition. The Pen/Trap Statute's overriding command is simply "Thou shalt not acquire

content."[12]

Nor are the second and third elements of the Government's reading based on the statutory text, which (1) does not limit the "technology reasonably available" solely to technology capable of sorting content from non-content with 100% accuracy, and (2) says nothing about permitting the "incidental" capture of content so long as the Government uses TRA to "minimize" such capture. Perfecting sorting, incidental content access, and minimization appear nowhere in § 3121(c).[13]

---

[12] Therefore, if there is "technology reasonably available" capable of limiting the information "capture[d]" or "record[ed]" by a pen/trap device to only non-content "processing" information, a Government agency must ("shall") use that technology even if it means that not all possible non-content will be acquired. And as noted, technology is readily available to ensure that no PCTDD are captured, thus abiding by the Pen/Trap Statute's command that no content be captured through the use of Pen/Trap Orders.

[13] Consider for instance the Government's strenuous effort to inject a content-minimization requirement into the Pen/Trap Statute, one akin to the minimization requirement found in § 2518(8) of the Wiretap Act. 18 U.S.C. § 2518(5) (2007) (surveillance authorized by wiretap warrant must be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception" under Wiretap Act); see Gov. Br. 24-26. Undaunted by the absence of any mention of minimization in the Pen/Trap Statute, the Government seizes upon a single line in the legislative history of 1994's CALEA, in which minimization is mentioned, Gov. Br. 24, and concludes from this single reference that "Accordingly, 18 U.S.C. § 3121(c) was intended to permit access to dialed-digit content incidental to the recording of dialed-digit non-content, provided that the government keeps the recording of such content to a practical minimum by means of 'technology reasonably available' to it." Gov. Br. 26.

Suffice it to say that the plain language of the statute trumps an isolated passage mined from volumes of legislative (continued...)

Finally, the Pen/Trap Statute says nothing about barring the use of content "incidentally" acquired through a pen/trap device against the target of the investigation. This is potentially a fatal flaw in the Government's reading because communications content is protected by the Fourth Amendment, see supra, and thus surely cannot be used in a criminal case against someone if it were obtained upon mere a showing of relevance.[14] If Congress had intended to allow the "incidental" capturing of content through pen/trap devices, therefore, it would have enacted a suppression remedy. That it did not is a gaping hole in the Government's reading. The Government's attempt to plug the hole by injecting the suppression remedy found in § 2515 of the Wiretap Act into the Pen/Trap Statute, however, fails badly.

A brief history is required to comprehend the fullness of the Government's present folly, for this is not the first solution the Government has proposed to cure this flaw. In the other three cases in which the Government sought to acquire PCTDD via a Pen

---

[13] (...continued)
history. This is especially so when Congress specifically placed a minimization requirement in the closely related Wiretap Act, but not in the Pen/Trap Statute, and when the plain text of the Pen/Trap Statute bars the acquisition of all content through the use of pen/trap devices, period, regardless of attempts to minimize.

[14] Of course, the problem arises only because the Government reads the Pen/Trap Statute as authorizing it to acquire communications content with only a Pen/Trap Order. If the Statute does not authorize the acquisition of content with pen/trap devices, no problem exists.

Register Order, the Government did not argue that § 2515 barred it from using communications content acquired via a Pen/Trap Order. Rather, it offered those courts only a voluntary pledge, based on an unenforceable internal Department of Justice memorandum, that it would not use such content "for any affirmative investigative purposes, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security." Deputy Attorney General Larry D. Thompson, "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices," May 24, 2002, quoted in Texas Op., 441 F. Supp.2d at 822 n.14; see also Fl. Mag. Op. at 2; Fl. Dist. Op. at 2. Section 2515 played no role in the Government's argument to those courts.

That only self-policing prevented the Government's use of contents acquired through a Pen Register Order obviously weakened its reading of the Pen/Trap Statute. If Congress had anticipated that content could be inadvertently swept up by a mere pen/trap order, as the Government asserts, surely it would have explicitly barred the affirmative use of such content against the target. The absence of such a prohibition was a gaping hole in the Government's construction.

The Government makes no mention of the DOJ Memo in its submissions to this Court. Rather, it offers a new solution that adopts the suppression remedy of the Wiretap Act, or Title III. As

the Government now states, the Court can construe the Pen/Trap Statute to permit the incidental capturing of content with a Pen Register Order because "th[at] content is subject to 18 U.S.C. § 2515's ban on use, absent separate authorization under Title III." Gov. Br. 12. As the Government further explains, quoting § 2515 in its entirety: "Since Title III's inception, 18 U.S.C. § 2515 has contained the following comprehensive prohibition on use by the government of the contents of wire communications in the event they are acquired without Title III's requisites for interception having been satisfied:

> Whenever any wire or oral communication has been intercepted, no part of the contents of such communication and no evidence derived therefrom may be received in evidence in any trial, hearing or other proceeding in or before any court, grand jury, department, officer, agency, regulatory body, legislative committee or any other authority of the United States, a State, or a political subdivision thereof if the disclosure of that information would be in violation of this chapter.

18 U.S.C. § 2515 (West 2006). Accordingly, 18 U.S.C. § 2515 precludes the government from making direct or derivative use of the contents of intercepted wire communications except as authorized by Title III . . . ." Gov. Br. 6. There is no need to worry about the Government using the content it "incidentally" acquires through a Pen/Trap Order, the Government assures this Court, because such content "would be subject to suppression" under § 2515. Id. 18; see id. 11-12 (Section 2515 "preclude[s] the government from using [] content" acquired through a pen/trap

device) (emphasis in original).

The problem with this argument is that § 2515 plainly does not apply to electronic communications, which is what PCTDD are. Section 2515 provides for suppression solely of "wire" and "oral" communications captured without a wiretap warrant. "Wire communication" means as "any aural transfer[14] made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection . . .," 18 U.S.C. § 2510(1) (emphasis added), and "oral communication" means "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception . . . ." Id. § 2510(2) (emphases added).

PCTDD, by definition "dialed digits," are neither wire nor oral communications. Rather, they fall within the broad category of "electronic communication," defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system . . . ." Id. § 2510(12). The catch-all category of "electronic communication" is "very broad," United States v. Herring, 993 F.2d 784, 787 (11th Cir. 1983), and encompasses essentially all electric

[14] An "aural transfer" is defined to mean "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18) (emphasis added).

or electronic signals that do not involve sound waves or the human voice. PCTDD are clearly electronic communications.[15]

The exclusion of improperly captured electronic communications from the suppression remedy provided in § 2515 is no accident. In fact, it is an exclusion made at the Government's prompting. When the Wiretap Act's ban on interception of oral and wire communications was extended to electronic communications in 1986, Congress accepted DOJ's proposal to reject simultaneously extending the Act's statutory suppression remedy to computer and other electronic communications. See Orin S. Kerr, Lifting the Fog of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law, 54 Hastings L.J. 805, 817 (2003). The plain language of § 2515 thus does not authorize suppression of improperly acquired electronic communications. E.g., Wayne R. LaFave et al., 2 Crim. Proc. § 4.3(a) (2d ed. 2006) (When the "category of 'electronic communication' was added to the statute in the 1986 amendment, . . . it was not placed on the same plane as the 'wire communication' and 'oral communication' categories. Although unauthorized interception of protected electronic communications is prohibited . . . violation of the prohibition is

---

[15] The Government's own discussion makes this even clearer. It defines PCTDD as "digits that a user dials after the initial call setup is completed, or 'cut-through' from an originating telephone switch to the next switch in the sequence needed to connect a call." Gov. Br. 1. A "switch," in turn, is a "sophisticated computer capable of connecting numerous calls at any given time." Id. 1 n.1.

not grounds for suppression of the evidence obtained.").

As a result, the Government has consistently argued to courts around the country -- in direct contrast to its position before this Court -- that § 2515 does not authorize the suppression of improperly obtained electronic communications. Courts have uniformly adopted the Government's view given the plain language of § 2515. See, e.g., United States v. Forest, 355 F.3d 942, 949 (6th Cir. 2004) ("Suppression is [] not a permissible remedy under Title III for the illegal interception of an electronic communication."); United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003) ("By its terms, 18 U.S.C. § 2515 applies only to 'wire or oral communications,' and not 'electronic communications'.") (emphasis in original); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 461 n.6 (5th Cir. 1994) (Wiretap Act's exclusionary remedy does not apply to electronic communications); United States v. Meriweather, 917 F.2d 955, 960 (6th Cir. 1990) ("[Title III] does not provide an independent statutory remedy of suppression for interceptions of electronic communications."). Commentators agree that § 2515 does not apply to electronic communications, e.g., Deirdre K. Mulligan, Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act, 2004 Geo. Wash. L. Rev. 1557, 1566 ("[T]he ECPA contains no statutory exclusionary rule for wrongfully acquired electronic communications."); 4 No. 2 Criminal

Practice Guide 8, "Searching and Seizing Computers," Part IV ("Electronic Surveillance in Communications Networks"), Section E.1 ("Title III provides for suppression of wrongfully intercepted oral and wire communications, but not electronic communications."), although this omission has garnered a fair amount of criticism in the academy. See generally Kerr, Lifting the Fog, supra; Michael S. Leib, E-Mail and the Wiretap Laws: Why Congress Should Add Electronic Communications to Title III's Statutory Exclusionary Rule and Expressly Reject a "Good Faith" Exception, 34 Harv. J. Legisl. 393 (1997).

The Government's attempt to use § 2515 to plug the Fourth Amendment hole in its argument thus fails. Nothing but a voluntary, unenforceable promise offers this Court assurance that PCTDD content acquired through the desired Pen Register Order will not be affirmatively used against the target.

4. Conclusion

This Court should reject the Government's attempt to transform § 3121(c)'s explicit limitation into an implicit expansion of Government powers. The Government's reading contradicts the plain language of § 3127. Point III.2, supra. It is also a poor reading of § 3121(c) itself. Point III.3, supra. Moreover, it perversely converts § 3121(c) into a provision authorizing Government surveillance of communications contents on a mere showing of relevance. This reading turns upside down the canon of

constitutional avoidance -- courts are supposed to construe statutes to avoid constitutional infirmities, not to create constitutional problems where none exists. E.g., Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Construction Trades Council, 485 U.S. 568, 575 (1988) ("[W]here an otherwise acceptable construction of a statute would raise serious constitutional problems, [a court should] construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress."). Even if there were any ambiguity in the Pen/Trap Statute, therefore, this Court must reject the Government's effort to transform it into an unconstitutional authorization to intercept Fourth Amendment-protected communications content on a showing far lower than probable cause. See generally supra Point II.

Point IV

This Court Should Not Consider Legislative History Because the Plain Language of the Pen/Trap Statute Bars the Use of Pen/Trap Devices to Acquire Content. But the Result Is the Same Even if Those Sources Are Considered.

The plain language of § 3127's definitions and § 3121(c)'s "limitation" bars the use of a Pen Register Order to intercept communications content. The Government's applications must therefore be denied. And because the plain language of the Pen/Trap Statute requires this result, this Court should not consider extraneous sources such as legislative history: "It is axiomatic that the plain meaning of a statute controls its

interpretation[] and that judicial review must end at the statute's unambiguous terms." Lee v. Bankers Trust Co., 166 F.3d 540, 544 (2d Cir. 1999) (internal citation omitted). Accord Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997) ("Our inquiry must cease if the statutory language is unambiguous and the statutory scheme is coherent and consistent."); Rubin v. United States, 449 U.S. 424, 430 (1981) ("When we find the terms of a statute unambiguous, judicial inquiry is complete . . . ."); Greenery Rehab. Group v. Hammon, 150 F.3d 226, 231 (2d Cir. 1998) ("If the statutory terms are unambiguous, our review generally ends and the statute is construed according to the plain meaning of its words."); Milman v. Box Hill Systems Corp., 192 F.R.D. 105, 108 (S.D.N.Y. 2000) (where plain language is unambiguous, "it is unnecessary and improper to use the statute's legislative history as an interpretive tool"); City of New York v. Beretta U.S.A. Corp, 228 F.R.D. 134, 144 (E.D.N.Y. 2005) (JBW) ("[Judicial] inquiry begins with the statutory text, and ends there as well if the text is unambiguous.") (quoting BedRoc Ltd. v. United States, 541 U.S. 176, 183 (2004)).

But even if this Court considers legislative history, the result is the same. Congress has long understood that communications content is protected by the Fourth Amendment and thus that content cannot be acquired with an easily obtained pen/trap order, issued upon the very low showing of relevance. A

sampling of the relevant legislative history proves the point.

When Congress enacted the Pen/Trap Statute in 1986 as part of the ECPA, it adopted the traditional understanding of these devices' essential nature -- they are mechanisms that capture only non-content envelope information, in particular the phone numbers of incoming or outgoing calls for the subject telephone. As the Supreme Court explained in United States v. New York Tel. Co., 434 U.S. 159, 166-67 (1977), pen registers "do not hear sound. They disclose only the telephone numbers that have been dialed -- a means of establishing communication." Pen registers "do not acquire the 'contents' of communications, as that term is defined by 18 U.S.C. § 2510(8)." Id. at 167. Smith v. Maryland echoed these sentiments in 1979, quoting New York Telephone's definition of pen registers and explaining that "a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications." 442 U.S. at 741 (emphasis in original).

Congress thus defined pen/trap devices in 1986 as follows:

> (3) the term "pen register" means 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 . . . ;
>
> (4) the term "trap and trace device" means a device which captures the incoming electronic or other impulse which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted;

18 U.S.C. § 3127 (1986).[16]

That the original definitions did not explicitly preclude the acquisition of content through pen/trap devices is of no moment. First, given the long-held understanding that pen/trap devices captured solely telephone numbers and not content of any kind, see, e.g., New York Telephone and Smith, an explicit restriction on content would have been superfluous. Second, given that most telephones in 1986 were still rotary and the possibility of acquiring numbers that constitute content (such as PCTDD) was for the most part only theoretical, a content restriction would have seemed unnecessary. E.g., People v. Bialostok, 610 N.E.2d 374, 378 (N.Y. 1993) ("The traditional pen register considered in Smith v. Maryland was, to large extent , self-regulating. Neither through police misconduct nor through inadvertence could it reveal to anyone any information in which the telephone user had a legitimate expectation of privacy."); see Tx. Op., 441 F. Supp.2d at 826 ("Because the existing technology in the 1980s did not allow over-collection of content, there was no need for Congress to address the contents problem in that portion of the ECPA.").

Legislative history from 1986 confirms that Congress understood that pen/trap devices could not be used to acquire content:

---

[16] These definitions remained unaltered until the 2001 PATRIOT Act. See infra.

> 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 communication, rather it records the numbers dialed.

H.R. Rep. No. 99-647, at 78 (1986) (emphasis added). As a result, the 1986 definitions of pen/trap devices "had never been [] construed" as permitting the capture of "the contents of communication that happen to include numbers . . . ." Kerr, supra, 2003 Nw. U. L. Rev. at 642.

And Congress was well aware that persons possess Fourth Amendment-protected privacy interests in communications content by 1994, when the first version of § 3121(c) was enacted as part of that year's Communications Assistance for Law Enforcement Act (CALEA). By this time, Congress also recognized that dialed digits were no longer exclusively used to convey non-content routing information, as they had been in the past, but instead were sometimes used to communicate a wide variety of content such as bank account numbers or passwords. The concern thus arose in Congress that pen registers capable of acquiring dialed digits would improperly capture communications content. When pressed on this point, the Executive Branch's principal representative -- FBI Director Louis Freeh -- expressly conceded that he did not wish to intercept any content through a Pen/Trap Order:

> SENATOR 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.
>
> DIRECTOR 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 processes. I don't want that in terms of my access, and that's not the transactional data I need.

Wiretapping: Joint Hearing of the Technology and Law Subcomm. of the Senate Judiciary Comm. and the Civil and Constitutional Rights Subcomm. Of the House Judiciary Comm., 103d Cong., 2d Sess. 50 (March 18, 1994).[17] To reinforce Director Freeh's concession (that the Government should not be permitted to intercept content with a pen/trap order), Senator Leahy "drafted the original version of 18 U.S.C. § 3121(c) in 1994 out of concern that pen register 'devices collected content and such collection was unconstitutional on the mere relevance standard.'" Gov. Br. 29 (quoting Senator Leahy, 147 Cong. Rec. S11000 (October 25, 2001)).

Accordingly, § 3121(c) was enacted to ensure that the

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

Government would not unconstitutionally capture communications content through a pen/trap order.[18] The accompanying House Report described this provision as one that "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." H.R. Rep. No. 103-827 at 32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3512.

Congress returned to this issue in the 2001 USA PATRIOT Act. By that time, Congress recognized that § 3121(c)'s explicit limitation on content acquisition had not achieved its purpose of protecting dialed contents from unconstitutional acquisition through pen/trap orders. As Senator Leahy lamented,

> When I added the direction on use of reasonably available technology (codified as 18 U.S.C. § 3121(c)) 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. Nevertheless, the FBI advised me in June 2000, that pen register devices for telephone services

---

[18] The initial version of § 3121(c) provided:

> 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.

18 U.S.C. § 3121(c) (1994 edition).

> "continue to operate as they have for decades" and that "there has been no change . . . that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."

147 Cong. Rec. S10990, S10999 (October 25, 2001). That is, despite § 3121(c)'s exhortation against content acquisition and the uncontroverted recognition that using pen/trap orders to acquire content was barred by the Fourth Amendment, e.g., Statement of Senator Leahy, 147 Cong. Rec. S10990, S10999 ("[C]ontent . . . may be captured only upon a showing of probable cause, not the mere relevancy of the pen/trap statute."), the FBI continued to operate pen/trap devices in a manner that allowed the Government to acquire even dialed content. "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,' . . . 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).

Congress thus explicitly prohibited all acquisition of content through pen/trap devices, amending their definitions to flatly bar the collection of communications content through these mechanisms. See 18 U.S.C. § 3127(3) & (4) (2007). As Senator Leahy explained, "the Administration agreed that the definition[s] should expressly exclude the use of pen/trap devices to intercept 'content' . . . ." 147 Cong. Rec. S10990, S10999 (emphasis added). The "clarification

that 'such information shall not include the contents of any communication," in sum, "was added at Senator Leahy's recommendation to ensure that [the Pen/Trap Statute] did not trump the Wiretap Act." Kerr, supra, 2003 Nw. U. L. Rev. at 637-38.

At the same time, Congress amended § 3121(c) to make even more explicit the absolute ban on content-acquisition through pen/trap devices. See 18 U.S.C. § 3121(c) (2007). Taken together, the changes wrought by the PATRIOT Act to the Pen/Trap Statute "makes it explicit that content can not be collected through such pen register orders." Statement of Senator Hatch, 147 Cong. Rec. S10547, S10561. Senator Feinstein agreed: "[T]his legislation makes it clear that [pen/trap] orders do not allow law enforcement to eavesdrop on or read the content of communication. Only the origin and destination of the messages will be intercepted." Id. at S10691; see generally Texas Op., 441 F. Supp.2d at 826 ("Advised in 2001 that pen registers continued to collect content despite CALEA's technology limitation, Congress acted again by inserting into the PATRIOT Act not one but three separate directives placing contents out of bounds for pen/trap devices.").

The Pen/Trap Statute, in sum, was amended to ensure that the statutory scheme mirrored the constitutional line between content and non-content. As a House Report accompanying a closely related predecessor to the PATRIOT Act explained:

[T]he 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, 741-743 (1979).

107 H. Rep. 236, Part 1, at 51 (October 11, 2001), quoted in Gov. Br. at 26-27 n.14. The legislative history thus reinforces the plain language of the Pen/Trap Statute: Communications content can not be acquired through Pen/Trap Orders.

CONCLUSION

For the foregoing reasons, amicus respectfully submits that this Court should deny the Government's applications seeking to intercept all PCTDD generated by the target telephones, including PCTDD content, through a Pen Register Order.

Dated: New York, New York
February 9, 2007

Respectfully submitted,

FEDERAL DEFENDERS OF NEW YORK, INC.
APPEALS BUREAU

By: _____
YUANCHUNG LEE
Attorney for Amicus Curiae
52 Duane Street, 10th Floor
New York, New York 10007
Tel.: (212) 417-8742

CERTIFICATE OF SERVICE

I certify that a copy of this Memorandum of Law has been served by e-mail and first class mail to the United States Attorney/E.D.N.Y.; Attn.: **JED DAVIS, ESQ.**, Assistant United States Attorney, 147 Pierrepont Street, 16th Floor, Brooklyn, New York 11201.

Dated: New York, New York
February 9, 2007

_____
YUANCHUNG LEE