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)**<br>**06 Misc. 561 (JMA)** |

**SUPPLEMENTAL MEMORANDUM OF LAW BY AMICI CURIAE**


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

ELECTRONIC FRONTIER FOUNDATION
Kevin Bankston, Esq.
454 Shotwell Street
San Francisco, CA 94110
Tel.: (415) 436-9333 x 126

**YUANCHUNG LEE,**
Federal Defenders of New York
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)**<br>**06 Misc. 561 (JMA)** |

**SUPPLEMENTAL MEMORANDUM OF LAW BY AMICI CURIAE**

**INTRODUCTION**

The Federal Defenders of New York ("FDNY"), joined by the Electronic Frontier Foundation ("EFF")[1], submit this Supplemental Brief in response to the Government's May 18th letter-brief ("May 18th Br.") and June 1st supplemental memorandum of law ("June 1st Br."). This Supplemental Brief principally addresses the

[1] Statement of Interest of *Amicus* EFF: EFF is a member-supported, non-profit legal foundation that litigates to protect free speech and privacy rights in the digital age. As part of that mission, EFF has served as counsel or amicus in key cases addressing the electronic surveillance statutes at issue here, including the first published decision addressing (and denying) a Government request to capture PCTDD content via a Pen/Trap Order. 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) ("Texas Op."). EFF also served as amicus to a Magistrate of this Court when it denied a Government application to track a cell phone's location without probable cause, see In the Matter of the Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. &/or Cell Site Info., 396 F. Supp. 2d 294 (E.D.N.Y. 2005), and the Sixth Circuit recently relied heavily on the reasoning of an amicus brief from EFF when finding a Fourth Amendment reasonable expectation of privacy in stored email, see Warshak v. United States, ___ F.3d ___, 2007 WL 1730094 at *10 (6th Cir. June 18, 2007).

Government's argument, set forth in the June 1st memorandum, that communications content in the form of "post-cut-through dialed digits" ("PCTDD") are exempt from the probable cause and warrant requirements of the Fourth Amendment. Amici respectfully submit that PCTDD-content is fully protected by the Fourth Amendment: A person who uses her telephone to check her account balances, pay bills, and transfer funds by transmitting PCTDD-content (e.g., coded passwords, account-identifying information, and personal identification numbers (PINs)) over the phone lines -- the modern-day substitute for what formerly would have been a live conversation between the user and the recipient of her call -- has "a subjective expectation of privacy [in that content] that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001). Therefore, the Government can intercept this information only upon a showing of (at least) probable cause of criminality, and this Court should not allow the Government to end-run the Fourth Amendment by using a Pen/Trap Order -- issued upon a mere assertion of relevance -- to capture PCTDD-content.

This Brief also responds to some of the missteps in the Government's May 18th letter-brief, which largely repeats its earlier, flawed statutory analysis. Principally, this Brief demonstrates that (1) 18 U.S.C. § 3121(c), upon which the Government's claim of authority to acquire PCTDD content rests entirely, contains no "condition precedent" whatsoever, and that

even if it did, the Government's assumption that the absence of the condition yields its desired result (authorization to "incidentally" intercept PCTDD content through a pen/trap device) is based neither on the language of the statute nor on logic; and (2) the absence of a statutory suppression remedy for improperly acquired PCTDD content fatally undermines the Government's reading of the Pen/Trap Statute.

## DISCUSSION

### Point I

### Persons Have Constitutionally Protected Privacy Interests in PCTDD-Content Transmitted over the Telephone Lines.

In its May 18th Brief, the Government conceded that users of pagers (12 million of them at last count, see June 1st Br. 7) have a constitutionally protected privacy interest in the "content" transmitted to and stored in their beepers, even if they exist in the form of digits or numerals. May 18th Br. 5. As the Government acknowledged after citing United States v. La Paz, 43 F. Supp.2d 370, 373 (S.D.N.Y. 1999) ("[C]ourts have consistently held that the owner of an electronic pager has a legitimate privacy interest in numeric codes transmitted to the device . . . . "):

> There is no dispute . . . that a person has a reasonable expectation of privacy in the content of telephonic communications that he stores, or that he transmits or that are transmitted through a service provider. Nor is there any dispute that if the government acquires such content on a showing of less than probable cause (e.g., a pen register order), that evidence is subject to suppression.

May 18th Br. 5.

The Government apparently changed its mind two weeks later. In its June 1st Brief, the Government turns 180 degree, now claiming that persons have no cognizable privacy interests in PCTDD content whatsoever, even though such content is functionally and otherwise identical to the content at issue in the pager cases.

The Government is wrong. As we argued in our original submission, PCTDD content -- like other communications content transmitted from one party to another via the telephone wires -- is fully protected by the Fourth Amendment. Amicus Br. 21-29; see also Texas Op., supra, 441 F. Supp.2d at 837 (Government's attempt to capture PCTDD content without a probable cause warrant is "in apparent violation of Katz"). Simply put, PCTDD content and voice content are constitutionally indistinguishable. Using the telephone to check one's account balance, transfer funds, inspect recent credit card transactions or reorder prescriptions by transmitting closely guarded personal-identification information via dialed digits is simply the modern-day substitute for what would have been, in days when only rotary telephones existed, a person-to-person phone conversation. The Supreme Court has long accorded Fourth Amendment protection to such calls, Katz v. United States, 389 U.S. 347 (1967), and this Court must do the same for their contemporary analog.

A. A Brief Factual Overview: PCTDD-Content, like Its Voice Equivalent, Travels on the Content Channel and Is Rarely Accessed by the Service Provider.

Every telephone call uses two channels, a "control" (or "call data") channel and a "content" channel. June 1st Br. 9-10; accord Note, Is "Big Brother" Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies to Use Dialed Digit Extraction, 84 Minn. L. Rev. 1051, 1054 (2000). The control channel "handles routing, addressing and other signaling information" transmitted in the form of pre-cut-through digits, June 1st Br. 9, and is used by the service provider to route calls to their destination. Once a call is connected or "cut through," the control channel is reassigned to handle / route another call, see Note, supra, at 1054 (control channel "remains operational only until the phone call has been properly routed, which occurs when it rings on the other end of the line"), and all further information in the original call -- including both voice content and dialed-digit content -- is conveyed along the content channel. June 1st Br. 9.

Pre-cut-through dialed digits, traveling on the control channel, are used by phone companies to route calls and are regularly recorded for billing purposes by the provider "in the ordinary course of business." Smith v. Maryland, 442 U.S. 735, 744 (1979); accord June 1st Br. 10 ("A provider often records pre-cut-through digits for billing and network planning purposes.").

In contrast to the "often record[ed]" pre-cut-through digits,

phone companies rarely access information traveling on the content channel, be it voice content or content in the form of post-cut-through digits. June 1st Br. 10; see Note, supra, at 1078 ("[P]ost-cut-through numbers . . . do not appear on the monthly bill, nor are they documented on a permanent record."). As most phone users already know, phone companies do not ordinarily monitor what is transmitted over the phone line after a call has reached its destination. Instead, a provider "monitor[s] and collect[s] information traveling over the content channel" only rarely, when it "suspects that a user is fraudulently obtaining service or misusing the service to harass another person." June 1st Br. 10. As the Government concedes, equipment used by the phone company to record information traveling over the content channel "is reserved for detection of calling fraud, harassment and similar misuse." Id. 24. Thus, provider monitoring of post-cut-through information traveling over the content channel, whether in the form of human voices or dialed digits, occurs infrequently.[2]

B. Because Transmitting PCTDD Content Is the Modern-Day Substitute for a Person-to-Person Phone Call, *Katz* Controls.

In the days before touch-tone telephones and advanced computers, a person who wanted to check her account balance, pay

[2] This limited exception originated long ago in the common law, which held that telephone subscribers have impliedly consented to eavesdropping by the phone company that is reasonably necessary to effectively maintain the service or prevent its fraudulent use. See, e.g., Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967); see also infra Point I.C.2.

her bills or transfer funds between accounts over the telephone had to call her bank and speak to an actual person to complete these transactions. After her call was cut-through to her bank, she would speak with an employee, give the employee her identifying information (such as her account number, password, PIN or Social Security number), and then ask the employee to perform the requested tasks. Similarly, a person who wished to check recent transactions on her credit card, reorder her prescriptions, receive information about the current performance of her 401(k) account or check the status of her flight over the telephone would have to call her credit card company / pharmacy / mutual fund adviser / airline and speak with someone in person.

The development of touch-tone telephones and advanced computers have changed how these ordinary, everyday communications occur. Instead of speaking with a live person employed by her bank, credit card company, pharmacy or airline, a person can call the company's automated system and, after the call has been cut-through, request the same information and complete the same tasks that formerly could be achieved only through a live phone conversation.

Apart from this technological advance, however, no difference exists between the live conversation of days past and today's use of PCTDD content. PCTDD are simply a modern-day way of communicating via the telephone touch pad more quickly and easily

what used to be done by person to person conversation. The core transaction remains the same: A user transmits communications content over the telephone wires to her intended recipient. See Note, supra, at 1077 ("There is no functional difference, in terms of expectations, between an individual who calls a bank and speaks to an actual banker to get his balance or an individual who calls a bank and uses an automated system to get his balance. Either way, the individuals are transmitting information over the telephone wire that they do not wish to expose to the public.").

The Fourth Amendment has long protected telephone conversations. The Supreme Court ruled 40 years ago that the Government violated the Fourth Amendment by eavesdropping on a telephone call made from a public phone booth without first obtaining a probable-cause warrant. Katz, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967). As the Court explained, "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment." Katz, 389 U.S. at 353.

Because using the telephone to communicate via PCTDD content is simply the modern-day equivalent of a live telephone conversation, the Fourth Amendment protects the former as it protects the latter. As the Supreme Court explained, "We are not

inclined to hold that a different constitutional result is required because the telephone company has decided to automate." Smith, 442 U.S. at 744-45.[3] Technological updating does not change the constitutional rule. Therefore, because communicating with another party via PCTDD content is simply the "modern day counterpart" of a telephone conversation, id. at 744, Katz requires courts to accord PCTDD content the same level of constitutional protection as voice content.

C. Persons Have a Reasonable Expectation of Privacy in Communications Content They Transmit over the Phone Lines.

The same result obtains when applying Katz's two-prong test for determining whether the Fourth Amendment is implicated, because persons who use their telephones to check their account balances or reorder prescriptions by transmitting PCTDD have "a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33 (2001), citing Katz, 389 U.S. at 361 (Harlan, J., concurring) ("[T]here is a twofold

[3] In Smith, the Court used this rule -- that technological updates do not change the constitutional result -- to find that the defendant had no reasonable expectation of privacy in the pre-cut-through digits -- i.e., telephone numbers -- he dialed to complete his calls. This was so because the automated "switching equipment that processed those numbers is merely the modern day counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." 442 U.S. at 744. And because "[p]etitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy" if the operator later disclosed the numbers to the police, id., the same result obtained even though "the telephone company has decided to automate." Id. at 744-45.

requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

First, PCTDD content easily satisfies the subjective component of the Katz test. Indeed, such content includes the most carefully guarded information we possess -- our Social Security or bank account numbers, our prescription information, and our passwords and PINs. This is precisely the type of information that financial institutions, as well as the Government itself, constantly caution us about safeguarding to prevent identity theft. When we use our telephones to check our account balances or transfer funds, and transmit carefully guarded personal identification information to do so, we expect that the information transmitted will remain private and will not be disseminated to the wider world. See Note, supra, at 1077-78 ("The type of information typically transmitted over the telephone by use of post-cut-through numbers is incredibly far-reaching: bank account numbers and codes, prescription identification numbers, paging messages, social security numbers, driver license numbers, airline flight information, credit card numbers, voicemail passwords, general account passwords, and responses to automated systems."). Amici doubt that anyone would use her telephone for such intimate purposes without this

expectation of privacy in mind.[4]

Second, this subjective expectation is surely one that "society recognizes as reasonable." The transmission of PCTDD content over the telephone is simply the contemporary substitute for the transmission of a human voice in a phone conversation:

> In the past, information carried in post-cut-through numbers was transmitted via voice communications over telephone systems. For instance, the information now dialed into a telephone to transfer money from one bank account to another used to be done by talking to a banker instead of using an automated system. The different method of communication does not change the type of information that is transmitted, nor should it change the type of protection that it receives.

Note, supra, at 1078. Because society recognizes an expectation of privacy in telephone conversations, see Katz, it must recognize the same in its functional equivalent, PCTDD content.

This Court should reject the Government's attempt to eliminate Fourth Amendment protection for PCTDD content. First, the Government's attempt to rely on Smith fails because the information at issue there -- pre-cut-through digits, or telephone numbers -- was merely routing information, not communications content. Smith explicitly declined to accord Fourth Amendment protection to pre-cut-through digits because they did not qualify as content, which

---

[4] Indeed, transmitting content via PCTDD is in some ways more private than transmitting content via the human voice. Unlike the phone conversation that took place in a public phone booth at issue in Katz, PCTDD content transmitted over the phone cannot be overheard by a bystander or otherwise readily disclosed to the public.

is of course implicated in Katz and in these applications. See 442 U.S. at 742 ("[A] pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communication.") (emphasis in original).[5]

Second, a phone company's rarely exercised capacity to monitor communications content (whether voice or digits) for the limited purpose of detecting fraud or other misuse does not eliminate a user's expectation of privacy in that content. If it did, then users would have no expectation of privacy in any communication conveyed over the telephone lines -- including the person-to-person telephone conversation protected by Katz. Caselaw confirms that limited access by others to a particular space -- such as a hotel room or rented apartment -- or channel of communication -- such as the telephone or Internet "wires" -- does not erode a person's expectation of privacy in that space or channel.

Finally, the Government badly misreads United States v. Miller, 423 U.S. 435 (1976), which is irrelevant here because the Government seeks to obtain information from the telephone company (via a pen/trap device), not from the party with whom the targeted user shares her PCTDD communications. It is simply not true that "[a]s a matter of law, no one has legitimate expectation of privacy

[5] Amici do not acknowledge that Smith was correct in holding that dialed phone numbers are not protected by the Fourth Amendment, but instead cite it only for the holding that the contents of communications are so protected.

in information that he voluntarily conveys to a third party." June 1st Br. 23. We demonstrate below that even if a caller has no reasonable expectation that the other party with whom she is communicating will not later disclose the shared information to others, she retains an expectation of privacy vis-a-vis the telephone company that society recognizes as reasonable and legitimate. As in Katz, the mere fact that communication between two parties is conveyed over wires owned by the phone company does not eliminate the parties' legitimate expectation of privacy in the content of that communication.

1. *Smith* Concerns Non-Content Routing Information, Not Communications Content.

Statutory surveillance law has historically distinguished between the contents of communications and non-content information associated with those communications. See Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 Ala. L. Rev. 9, 46-49 (2004). The electronic surveillance statutes thus require a heightened showing, above probable cause, before the Government may access communications content, 18 U.S.C. § 2518, and permit non-content dialing, routing, and addressing information to be acquired using pen registers that are available upon less than probable cause, 18 U.S.C. § 3123.

Content is defined broadly as "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8); see 18 U.S.C. § 3127(1) (adopting § 2510's definitions for

Pen/Trap Statute). For telephone calls, content thus refers to the substance of the call -- i.e., the substantive information transmitted between the caller and recipient. Non-content attribute information, in contrast, includes addressing or routing information concerning a particular communication. 18 U.S.C. § 3127(3) ("dialing, routing, addressing, or signaling information"). For telephone calls, that information has typically included "the telephone number dialed . . . , whether or not the call succeeded, its duration and its physical location." Freiwald, supra at 46; see also id. at 70-73 (analyzing the evolution of the content/non-content dichotomy).

The content of telephone calls has been accorded full Fourth Amendment protection since Katz, 389 U.S. 347, 353-54 (1967), which held that persons have legitimate privacy interests in the substance of their phone conversations and thus that the Government's warrantless eavesdropping was unconstitutional. Accord Berger, 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."). Non-content routing or addressing information, on the other hand, has not been accorded Fourth Amendment protection. In Smith, 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. No cognizable privacy interest exists in dialed numbers used to route a call, the Court explained, because a user knows that she must convey these numbers to the phone company in order to complete her call. Id. at 743-44.

Smith specifically distinguished Katz on the ground that pen registers capture only non-content routing information. As the Court explained, "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 continued, "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).").

Smith thus affirms Katz's holding that the content of phone communications are protected by the Fourth Amendment. Because PCTDD content (in the form of account numbers, PINs, passwords or prescription numbers, for instance) indisputably qualify as communications content -- i.e., as "information concerning the substance, purport, or meaning of [a] communication," 18 U.S.C. §

2510(8) -- they are entitled to the same constitutional protection as the voice content in Katz.[6]

2. The Phone Company's Limited Monitoring of Communications Content (to Investigate Fraud, Harassment or Misuse) Does Not Eliminate a User's Legitimate Expectation of Privacy in that Content.

The superficial similarity between PCTDD content and the telephone numbers dialed in Smith -- i.e., both are "dialed digits" -- does not require a different result. The petitioner in Smith had no reasonable expectation of privacy in the telephone numbers he dialed because he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its

---

[6] While conceding that "there is no question that PCTDD [include] content," the Government asserts that "the content in question is more limited in its range of expression than conversation between two human beings." June 1st Br. 8. It then suggests -- without any supporting argument -- that the alleged fact that "[t]he range of expression that can be conveyed by PCTDD content is limited" (because "PCTDD by definition consists merely of digits") somehow makes a difference. Id. 25.

The Court should quickly reject this attempt to denude communications content of constitutional protection because of its allegedly "less intimate" nature: There is no hierarchy of content from a constitutional perspective. E.g., Kyllo, 533 U.S. at 39 ("[L]imiting the prohibition of thermal imaging to [only imaging that revealed] 'intimate details'" would be both "wrong in principle [and] . . . impractical in application . . . ."); see also Arizona v. Hicks, 480 U.S. 321 (1987) (act of turning stereo equipment, merely to see a registration number, violated Fourth Amendment). The Government is also wrong on the facts, since among other things it concedes that the subset of PCTDD content represented by digits transmitted to display pagers can involve "elaborate codes" capable of conveying detailed messages. June 1st Br. 6-7 & 25. Twelve million people still use these devices. Id. 7. Thus, using pen/trap devices to capture PCTDD content will inevitably involve the interception of "elaborate codes."

equipment in the ordinary course of business." Smith, 442 U.S. 744; see also id. 742 (pen registers "routinely used" by phone companies to monitor telephone numbers); id. 742-43 (pen registers are "regularly employed" by phone companies "for a variety of legitimate business purposes"). This reasoning does not apply to PCTDD content because such information is not shared (by the user) with the phone company "in the ordinary course of business" and the phone company does not "routinely" or "regularly" monitor communications content.

The only information a user affirmatively shares with the telephone company is the routing data needed to complete a call on the control channel, not the information transmitted on the content channel (which engages after a call has been cut-through). E.g., June 1st Br. 9-10; see also Warshak v. United States, ___ F.3d ___, 2007 WL 1730094 at *10-11 (6th Cir. June 18, 2007) (explaining that the information addressed in Smith was "the specific information conveyed to the service provider, which in the telephone context excludes the content of the conversation"). Routing information is needed by the phone company to connect a call and properly bill customers. Note, supra, at 1078; Smith, 442 U.S. 742. PCTDD content, in contrast, is just like voice content: Although it travels through the phone company's lines (via the content channel), it is shared only with the intended recipient (e.g., a bank, pharmacy or credit card company). Although the telephone

company has the capacity to access PCTDD as part of a fraud or harassment investigation, it does not ordinarily monitor communications content traveling through the content channel -- whether in the form of human voices or in the form of dialed digits -- during the normal course of business. The monitoring "equipment is reserved for detection of calling fraud, harassment and similar misuse." June 1st Br. 24.

And to repeat: In the rare instances where a phone company uses that equipment to monitor or record information traveling over the content channel, the information may include both voice content and content in the form of PCTDD. See June 1st Br. 9 ("[I]f an originating provider suspects that a user is fraudulently obtaining service or misusing the service to harass another person, that provider may [] monitor and collect information traveling over the content as well as the control channel.").[7] That a phone company has the capacity to monitor voice communications, and does so occasionally, has long been known. See, e.g., Bubis v. United States, 384 F.2d 643, 648 (9th Cir. 1967) (discussing common-law "provider exception" allowing for eavesdropping by the phone

[7] The Government asserts without citing any authority that while a provider "may not need to record the user's oral conversations" even in these rare instances of fraud investigations, it will "typically" record PCTDD. June 1st Br. 10. This bald assertion, even if true, is irrelevant: The fact remains that telephone providers have the same capacity to access voice content that it does PCTDD content, and this limited access does not eliminate a user's expectation of privacy in either.

company that is reasonably necessary to effectively maintain the service or prevent its fraudulent use). The Supreme Court was certainly well aware of this. E.g., Smith, 442 U.S. 746 (explaining that voice communications are protected by the Fourth Amendment even though a "telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.") (Stewart, J., dissenting). And such an exception is built into the 1968 Wiretap Act (or "Title III"):

> It shall not be unlawful under this chapter for . . . a provider of wire or electronic communication service . . . to intercept, disclose, or use [a] communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service . . . .

18 U.S.C. § 2511(2)(a)(I). Nonetheless, of course, Katz remains good law and the Government cannot eavesdrop on telephone conversations without obtaining a Title III warrant.

The mere ability of a telephone provider to access communications content, in sum, does not eliminate Fourth Amendment protection for that content. The Government's reasoning that this limited access -- "reserved for detection of calling fraud, harassment and similar misuse," June 1st Br. 24 -- removes all Fourth Amendment protection must be rejected because it would also eliminate Fourth Amendment protection for voice calls. See Warshak, ___ F.3d at ___, 2007 WL 1730094 at *10 (If limited access

by provider eliminated user's privacy interest, then "phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them.").

In analogous contexts, courts have consistently and repeatedly held that persons retain a reasonable expectation of privacy in spaces even when other parties have a limited ability to access those spaces. See, e.g., Stoner v. California, 376 U.S. 483, 489 (1964) (defendant has Fourth Amendment-protected privacy interest in his hotel room despite his having given an "implied or express permission to such persons as maids, janitors or repairmen to enter [a] room in the performance of their duties") (internal citations and quotation marks omitted); Chapman v. United States, 365 U.S. 610, 616-18 (1961) (same regarding rented premises). More recently, the Sixth Circuit held that users of e-mails possess a reasonable expectation of privacy in e-mail messages that are "stored with, or sent or received through a commercial [Internet Service Provider or ISP]." Warshak, ___ F.3d at ___, 2007 WL 1730094 at *12. The ISP's ability to access a user's e-mail was for "limited circumstances, rather than wholesale inspection, auditing, or monitoring," the court explained, and therefore did

not eliminate the user's expectation of privacy. Id. at *13.

What Warshak held regarding e-mails applies equally to telephone content, including content in the form of dialed digits. As the court explained, "Like telephone conversations, simply because the phone company or the ISP could access the content of e-mails and phone calls, the privacy expectation in the content of either is not diminished, because there is a societal expectation that the ISP or the phone company will not do so as a matter of course." Id. at *11; see also id. at *14 ("Where the third party is not expected to access [the communications content] in the normal course of business, [] the party maintains a reasonable expectation of privacy [in that information] . . . ."); id. at *15 (Provider's "right to access [communications content] only in certain limited circumstances would not be sufficient" to overcome users's right to privacy). A user's expectation of privacy may be overcome only if, among other things, the service provider has "complete access" to the communications content in question "and [] actually relies on and utilizes this access in the normal course of business." Id. at *15 (emphasis added); accord United States v. Long, 64 M.J. 57 (Ct. App. Armed Forces 2006) (soldier had reasonable expectation of privacy in e-mail stored on Department of Defense computer despite DoD's ability to monitor it); United States v. Maxwell, 45 M.J. 406 (Ct. App. Armed Forces 1996) (officer had reasonable expectation of privacy in his AOL e-mails).

The Ninth Circuit relied on the same reasoning in United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007), concluding that the owner of a personal computer retained a reasonable expectation of privacy in it even though he attached it to a university computer network that allowed for "limited instances in which university administrators may access his computer in order to protect the university's system." "[T]he fact that others may have occasional access to the computer," the court held, "does not in itself extinguish privacy expectations." Id. at 1146-47. The Second Circuit likewise ruled that a Government employee had a reasonable expectation of privacy in the contents of his office computer even though support staff performed "infrequent and selective search[es] for maintenance purposes or to retrieve a needed document." Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001); see also id. at 74 (noting that outcome may have been different if there was a "general practice of routinely conducted searches of office computers").

In sum, the phone company's limited and rarely exercised ability to monitor telephone communications content -- whether voice content or PCTDD content -- to investigate fraud or other misuse does not remove that content from the Fourth Amendment's reach. "[T]here is a societal expectation that . . . the phone company [will not access the content of phone calls] as a matter of course," even though it may do so occasionally and for limited

purposes. Warshak, ___ F.3d at ___, 2007 WL 1730094 at *11.

3. *Miller* Is Irrelevant Because the Government Is Not Seeking Information from the Party with Whom the User Shared Private Communications Content.

Individuals intend to share PCTDD content only with the party they are calling, not the phone company. And the Government "cannot [] bootstrap an intermediary's limited access to one part of the communication (e.g., the phone number) to allow it access to another part (the content of the conversation)." Warshak, ___ F.3d at ___, 2007 WL 1730094 at *11.

Having failed in its effort to use the phone company as a bootstrap, the Government next attempts to use United States v. Miller, 423 U.S. 435 (1976), to achieve the same result. The Government notes that PCTDD content "consists mainly of information that at the time of the call is already a record of the organization (e.g., a PIN or account number), or that the organization for account-keeping purposes records at the time of the call." June 1st Br. 26. Citing Miller, the Government then asserts that "no person who volunteered such information to the organization before or during the call has a reasonable expectation that the organization will refrain from turning it over to law enforcement." Id.

That may or may not be true, but it is irrelevant to the matter at hand. The Government's applications "seek to use a pen register installed on the premises of the originating service

provider of a target telephone in order to acquire PCTDD." June 1st Br. 21 (emphasis added). A telephone user, as explained above, does not "volunteer" or otherwise share her communications content (whether voice or dialed digits) with that provider -- she only does so with the ultimate recipient of her calls (e.g., her bank, pharmacy or credit card company). The applications pending before the Court have nothing to do with those recipients. Miller, in contrast, concerned information obtained by the Government from a party with whom the defendant shared information.

Miller rejected the defendant's Fourth Amendment challenge arising from the Government's issuance of subpoenas to banks at which he maintained accounts. The banks did not object to the subpoenas and turned over the requested records to the Government in compliance with the subpoenas.

The Court rejected the defendant's constitutional argument, explaining that he did not have a cognizable privacy interest in "information [he] revealed to a third party and conveyed by [that party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in third party will not be betrayed." Miller, 425 U.S. 443 (citations omitted). A "depositor takes the risk, in revealing his affairs to another," the Court explained, "that the information will be conveyed by that person to the Government. United States v. White, 401 U.S. 745, 751-52

(1971)." Id. at 443.

In White, the Court held that no Fourth Amendment claim lies when an informant is wired during conversations with the defendant, because "however strongly a [person] may trust an apparent colleague, his expectations in this respect are not protected by the Fourth Amendment when it turns out that the colleague is a government agent regularly communicating with the authorities." White, 401 U.S. at 749. The Court specifically distinguished this situation -- where a party to a conversation with the defendant reveals that information to the Government -- from the situation in Katz, where the Government did not obtain information from a party to a conversation but simply eavesdropped on the conversation itself. The latter situation violated the Fourth Amendment (but the former did not), White explained, because it "involved no revelation to the Government by a party to conversations with the defendant . . . ." Id. (emphasis added); see also Hoffa v. United States, 385 U.S. 293 (1966) (no Fourth Amendment search when an individual tells the police about his conversations with defendant after they occurred).

Miller thus stands for the narrow proposition that a person cannot complain when information he voluntarily shares with another is subsequently turned over by that party or individual to the Government. See 425 U.S. at 441-42 ("The records . . . pertain to transactions to which the bank was itself a party."). Thus, a

person who uses the telephone to transmit communications content does not possess a "constitutionally protected expectation that a person with whom he is conversing will not then or later reveal the conversation to the police." White, 401 U.S. at 749. He retains a justified expectation, however, that the phone company will not do so. Katz, 389 U.S. at 353. As the Sixth Circuit explained:

> It is true [] that by sharing communications with someone else, the speaker or writer assumes the risk that it could be revealed to the Government by that person, or obtained through a subpoena directed to that person. The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise, phone conversations would never be protected, merely because the telephone company can access them . . . .

Warshak, ___ F.3d at ___, 2007 WL 1730094 at *10 (internal citation omitted). Miller is therefore irrelevant to the pending applications.

Miller additionally emphasized the voluntary nature of the bank's disclosure -- the records at issue there were not intercepted by the Government but turned over voluntarily by parties with whom the defendant voluntarily shared information (the banks did not move to quash the subpoenas). The case was thus "governed by the general rule that the issuance of a subpoena to a third party to obtain the records of that party does not violate the rights of a defendant." 425 U.S. at 444. Miller also carefully explained that "the documents subpoenaed are not respondent's 'private papers'" nor his "confidential

communications." Id. at 442. As the Court explained, "respondent can assert neither ownership nor possession" of the records turned over by the banks to the Government because "these are the business records of the banks," which "pertain to transactions to which the bank was itself a party" and contain only "information exposed to [the bank's] employees in the ordinary course of business." Id.

Miller in sum did not disturb Katz's general bar against warrantless Government interception of shared communications content by compelling the service provider to reveal this information. But permitting the Government to capture PCTDD content with a pen/trap device installed on the premises of the telephone company runs directly into this prohibition: The Government will be intercepting a person's "confidential communications" that are in no way "business records of [the phone company]" or otherwise shared with the phone company; and it will do so not by obtaining information from a party to the shared communication but from a non-party service provider. Katz bars such Government action absent at least a warrant issued upon a showing of probable cause.

D. The Doctrine of Constitutional Avoidance Counsels Rejection of the Government's Statutory Analysis.

As amicus FDNY argued in our original submission, this Court need not reach the constitutional question because the Pen/Trap Statute plainly does not authorize the Government to intercept communications content via a mere Pen/Trap Order. Amicus Br. 15-21

& 30-47. But even if this Court had some doubt on the statutory question, the "constitutional avoidance" canon of construction commends this Court to reject the Government's reading of the Pen/Trap Statute and deny its applications.[8] This interpretive rule provides that "where 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." Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. & Construction Trades Council, 485 U.S. 568, 575 (1988). It is based on the "reasonable presumption" that when there are "competing plausible interpretations of a statutory text," Congress likely "did not intend the alternative which raises serious constitutional doubts." Clark v. Martinez, 543 U.S. 371, 381 (2005).

As demonstrated above, serious Fourth Amendment problems would arise if this Court were to allow the Government to capture PCTDD content upon a mere assertion of relevance via a Pen/Trap Order. Even if this Court believed the statutory construction question to be debatable, therefore, the doctrine of constitutional avoidance counsels rejection of the Government's interpretation because it runs headlong into constitutional problems.

---

[8] The Government is fond of canons of construction, e.g., Jan. 19th Gov. Br. 10-11 (discussing four canons), but omits entirely this most pertinent one.

## Point II

### The Government's Statutory Analysis Fails Because § 3121(c) Sets Forth No "Condition Precedent" and Because There Is No Statutory Suppression Remedy.

Amicus FDNY demonstrated in our original submission that the Pen/Trap Statute plainly and clearly bars the Government from intercepting communications content through a Pen/Trap Order. Amicus Br. 15-21 & 30-47. We will not repeat that analysis here. However, two points raised in the Government's May 18th reply, which principally repeats the flawed statutory analysis set forth in its original January submission, warrant response. Amici now demonstrate, first, that § 3121(c), upon which the Government's claim of affirmative authority to "incidentally" capture PCTDD content rests, contains no "condition precedent" (allegedly authorizing content acquisition if the condition is not satisfied) but simply an unqualified bar on content acquisition. And even if it did, the Government's unargued-for assumption -- that the absence of the condition leads to authorization to acquire content -- is groundless.

We further show that the absence of a statutory suppression remedy, which the Government now must concede, undermines its construction of the Pen/Trap Statute. That reading had rested on two pillars -- § 3121's authorization of incidental acquisition of content through pen/trap devices, on the one hand, and § 2515's bar on the use of such content on the other. And that reading now

collapses with the disappearance of the second pillar: Surely Congress would not have neglected to enact a suppression remedy if it had intended to authorize the incidental capturing of PCTDD-content upon a mere claim of relevance.

A. Section 3121(c) Sets Forth No "Condition Precedent" Authorizing the Government to Capture Content via a Pen/Trap Order; and even if Section 3121(c) Is Read to Contain such a Condition, It Says Nothing about What Should Occur if the Condition Is Not Satisfied.

The Government's claim of affirmative authority to capture PCTDD content derives entirely from its "condition precedent" reading of § 3121(c). In a nutshell, the Government claims that § 3121(c) sets forth a "condition precedent" in the form of "technology reasonably available" capable of separating content from non-content and ensuring that the Government captures all possible non-content.[9] See May 18th Br. 4. If this condition

[9] The Government accuses amicus FDNY of "falsely" stating that the Government reads § 3121(c)'s reference to "technology reasonably available" to be limited to technology that can "perfectly distinguish content from content." May 18th Br. 4 & 4 n.2. Mysteriously, however, the Government offers no explanation for why or how this characterization is "false."

Amicus FDNY's characterization of the Government's view is not in any way false or inaccurate. We explained in our February submission that "the Government reads 'technology reasonably available'" in such a way that only "technology capable of perfectly sorting content from non-content (so that the Government acquires all possible non-content) [] qualif[ies]." Amicus Br. 34 (emphasis omitted). This description is based on the Government's own words. As it stated in its January submission, "If there is no TRA [technology reasonably available] that can make that distinction [between PCTDD non-content and PCTDD content] with complete accuracy, however, § 3121(c) only requires the government (continued...)

attains -- i.e., if such sorting technology is reasonably available -- then the Government must use it and not capture any content. Id. If this condition does not attain, however, the Government can go ahead and use a readily available technology even if it captures content. Id. ("To the extent that such technology exists, the government must use it. To the extent that it does not, § 3121(c) permits the government to access the content incidental to acquiring non-content."). This is the crux of the Government's reading:

> Whether "technology [is] reasonably available to" the government that would keep a pen register from confusing content with the non-content . . . determines whether the Pen/Trap Statute permits collection of content. If such technology exist, the government must use it. On the other hand, if there is no such "technology reasonably available," then the Pen/Trap Statute permits the pen register to access content incident to the device's collection of non-content.

June 1st Br. 11.[10]

---

[9] (...continued)
to operate the pen register using the TRA that exists . . . ."). This same insistence -- that the "TRA" mentioned in § 3121(c) refers only to technology capable of ensuring that the Government acquires all possible non-content from a pen/trap device -- is repeated in the DOJ memo. See DOJ Memo at 4 (describing TRA provision of § 3121(c) as "impos[ing] an affirmative obligation to operate a pen register or trap and trace device in a manner that . . . will minimize any possible over collection while still allowing the device to collect all of the limited information authorized") (emphasis added).

[10] The Government works mightily to fabricate a distinction between the "incidental" capturing of PCTDD content -- which it claims is permitted under § 3121(c) -- and the "intentional" interception of the same, which it concedes is barred by the (continued...)

Amicus FDNY has already pointed out numerous flaws with the Government's statutory analysis. Amicus Br. 30-47. However, there are two errors particular to the Government's "condition precedent" reading of § 3121(c): § 3121(c) by its plain language sets forth no "condition precedent" whatsoever, and even if it did, nothing warrants the Government's assumption that if the condition did not attain, it is free to capture PCTDD content.

Section 3121(c) of Title 18 states:

> **(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). On its face, therefore, § 3121(c) is a simple command, not a "if-then" conditional. The statute commands all "government agenc[ies]" authorized to install pen/trap devices to use available technology to "restrict" the information captured to routing and addressing

---

[10] (...continued)
Pen/Trap Statute. E.g., June 1st Br. 12 ("[W]hile § 3121(c) permits incidental access [to PCTDD content] . . . , a companion provision removes such content from the categories of evidence that the Pen/Trap Statute authorizes the government intentionally to target."). Of course, neither these terms nor a distinction between them exists in the Pen/Trap Statute, which simply prohibits the Government from using pen/trap devices to capture content, regardless of whether it is done intentionally or incidentally. The distinction is entirely of the Government's creation.

information "so as not to include the contents of any wire or electronic communications." The statute unambiguously states that Government agencies "shall use" such technology. It does not say, as the Government claims, that "if such technology is available, then it must be used" and content may not be captured. There is simply no conditional in § 3121(c).

Moreover, even if § 3121(c) could somehow be read to contain a conditional, it says nothing about what should result if such technology is not reasonably available -- i.e., if the "condition precedent" (or antecedent) does not attain. The Government simply assumes that if the antecedent -- TRA capable of sorting content from non-content -- does not attain (i.e., the TRA does not exist), then the consequent (the "then" part of the "if-then" conditional) also does not attain -- i.e., it can go ahead and "incidentally" capture content. But the Government offers no argument for why this is so; it simply assumes it.

This is a faulty assumption, both as a matter of logic and as a reading of § 3121(c). First, if the Government believes that the negation of the antecedent (its "condition precedent") in a conditional statement logically yields the negation of the consequent, it has committed a logical fallacy. In a conditional statement of the form "If P, then Q," logic instructs that if the antecedent P is true, then the consequent Q is true as well. (This is the foundational inference rule called "modus ponens." Donald

Kalish et al., Logic: Techniques of Formal Reasoning 15 (2d ed. 1980)). But what does logic dictate when the antecedent is not true or does not attain? The answer is that logic does not dictate anything: If the antecedent P does not attain, the consequent Q may or may not attain. Whether Q attains or not depends on facts, not logic. Take the following conditional as an example: "If Caesar committed suicide (P), then he is dead (Q)." If P is true, then Q is true (via modus ponens). However, if P is not true -- i.e., Caesar did not commit suicide (not P) -- then Q may or may not be true. Caesar could be alive (i.e., not dead, or not Q), or he could be dead (Q) but by means other than his own hand.[11]

A belief that the denial of an antecedent (P) logically yields the denial of the consequent (Q) is therefore a false one. Indeed, there is a name for it -- the "fallacy of denying the antecedent." Kalish et al., supra, at 40. Even if TRA did not exist, therefore, it does not follow logically that the Government would be freed from § 3121(c)'s plainly stated and unqualified restriction on capturing content.[12]

---

[11] History of course tells us that even though Caesar did not die by his own hand (not P), he is indeed dead (Q).

[12] The Government repeats this fallacy in its June 1st Brief. After stating that "there is no 'technology reasonably available to' the government that permits it to distinguish PCTDD non-content from content," (i.e., not P), the Government leaps to its desired conclusion (not Q) as if it were logically ordained: "Accordingly, § 3121(c) permits the government to access PCTDD content incidental to collecting non-content, the statute's condition precedent to a (continued...)

Second, the Government's assumption regarding what should occur if TRA is not available -- i.e., that it be permitted to capture PCTDD content -- is a terrible one in light of the plain language of the Pen/Trap Statute. Given the explicit bar on content acquisition set forth in the final sentence of § 3121(c), the much better inference is that the Government should not be permitted to capture content even if TRA does not exist. This is especially so given that § 3121(c) uses the terms "pen register" and "trap-trace device," which are defined elsewhere in the Pen/Trap Statute as devices that do not "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 . . .

---

[12] (...continued)
contrary outcome -- that the contemplated 'technology reasonably available' actually exists -- having not been satisfied." June 1st Br. 14.

18 U.S.C. § 3127 (2007). Whether TRA exists or not, therefore, Congress's intent should be clear: No content can be captured by pen/trap devices.[13]

B. The Lack of an Enforceable Suppression Remedy Fatally Undermines the Government's Statutory Analysis.

In its original submission, the Government asserted that the plain language of the relevant statutes, along with the canons of construction, "require[d]" this Court to construe the statutes in the following two-pronged manner:

> **(a)** to permit a pen register to access PCTDD content incidental to collecting non-content, when there is no "technology reasonably available" to avoid the incidental access, see 18 U.S.C. § 3121(c), but **(b)** to preclude the government from using that content, because at the time a device access it, the device is not functioning as a "pen register" within the definition of 18 U.S.C. §

[13] There are two additional counterintuitive implications of the Government's "condition precedent" argument. That neither of these conclusions is remotely plausible is further reason to reject the Government's reading. First, the Government reads § 3121(c) as a delegation by Congress -- to the telecommunications industry -- of the critical issue of the degree of privacy protection due citizens. That is, whether the Government can obtain one's PINs and credit-card account information upon a mere unreviewable assertion of relevance depends on whether the telecommunications industry has developed the appropriate "sorting" filter. Second, under the Government's reading, the Government has every incentive to discourage the development of accurate filters (capable of sorting PCTDD content from non-content). After all, the Government acquires much more information when the technology does not exist than when it does.

Neither of these outcomes is plausible. Surely Congress would not delegate the issue of privacy protection to the telecommunications industry; nor would it create a disincentive to the development of more accurate sorting technology. That the Government's reading of § 3121(c) necessarily yields these results is a reductio ad absurdum of that reading.

> 3127(3) and accordingly, the content is subject to 18 U.S.C. § 2515's ban on use, absent separate authorization under Title III.

Government Brief of January 19, 2007 ("Gov. Br.") 11-12 (bold added). This twin-pillared reading of the relevant statutes -- as permitting "incidental" interception of PCTDD content in § 3121(c) but barring its use in § 2515 -- is repeated throughout the Government's brief. E.g., id. 3 ("Although the Pen/Trap Statute authorizes such incidental access [to PCTDD content], the government is barred from using both the content in issue, as well as it [sic] fruits, unless that content was acquired in accordance with . . . 18 U.S.C. § 2515."); id. 4 (same); id. 6 (same); id. 18 (same).

That § 2515 (allegedly) barred the use of PCTDD content was a critical component of the Government's statutory analysis, since the Pen/Trap Statute itself says nothing about barring the use of content "incidentally" acquired through a pen/trap device against the target of the investigation. This was a potential fatal flaw in the Government's reading because persons have reasonable expectations of privacy in the content of their communications and, therefore, if Congress had intended to allow the "incidental" capturing of content through pen/trap orders (issued upon a bare assertion of relevance), it would have enacted a remedy barring the affirmative use of this information. To plug this hole in its statutory argument, the Government pointed to § 2515: There is no

need to worry about the Government misusing the passwords, prescription information, and PINs it intercepts through a Pen/Trap Order, it assured this Court, because such content "would be subject to suppression" under § 2515. Gov. Br. 18.

As amicus FDNY pointed out in our February submission, this resort to § 2515 was a newfound strategy for the Government, which previously proposed only an unenforceable voluntary pledge, in the form of an internal DOJ memo, as the solution to the problematic use of improperly captured PCTDD content. See 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 (attached as Exhibit 1 to May 18th Brief). In that memo, the DOJ stated 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." Id. 4. Like all internal DOJ memos, however, it was "limited to improving the internal management of the Department" and created no enforceable rights whatsoever in third parties:

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

person or entity, with the Memorandum.

Id. 5; accord United States v. Ivic, 700 F.2d 51, 64 (2d Cir. 1983) ("[N]on-compliance with internal departmental guidelines is not, of itself, a ground on which defendants can complain.").

That only self-policing prevented Government abuse of communications contents acquired through a Pen Register Order severely weakened its reading of the Pen/Trap Statute. This is obviously why the prosecutor in this particular case chose at first not to inform this Court about the DOJ memo, and to rely instead on § 2515 as solving the suppression dilemma.

But as we demonstrated in our February submission, this prosecutor's reading of § 2515 contradicted the DOJ's own view of the statute, as well as every reported decision on this issue. See generally Amicus Br. 40-46. Simply put, § 2515 does not apply to electronic communications, see, e.g., United States v. Forest, 355 F.3d 942, 949 (6th Cir. 2004); United States v. Steiger, 318 F.3d 1039, 1050 (11th Cir. 2003); Steve Jackson Games, Inc. v. United States Secret Service, 36 F.3d 457, 461 n.6 (5th Cir. 1994); United States v. Meriweather, 917 F.2d 955, 960 (6th Cir. 1990), and the Government's own view is that PCTDD fall in this category.

The Government's May 18th Brief acknowledges its mistaken reading of § 2515, though the concession is buried on page 9 of a 15-page submission. Predictably, the Government now trots out the previously unmentioned DOJ memo as sufficing to support its

delicate statutory construction. May 18th Br. 9. Surprisingly, however, the Government rewrites history by dramatically downplaying the important role played by § 2515 in its original analysis. Contradicting its own repeated reliance on § 2515 in its principal submission of January 2007, see supra, the Government now claims that "[w]hether a remedy exists to redress unpermitted use of PCTDD content [] has no bearing on how the canons of construction require §§ 3121(c) and 3127(3) to be harmonized." May 18th Br. 9 (emphasis added). Indeed, the Government goes so far as to suggest that "the existence of a remedy for unpermitted use of PCTDD" content is not even "material" to the question that must be answered by this Court. Id.

The Court should see this sudden amnesia for what it is: A desperate attempt to rescue a fatally flawed reading of the statute. The Government was originally correct in attempting to find a statutory suppression remedy (even if it did not exist) for improperly captured PCTDD content. After all, the lack of such a remedy is compelling evidence that Congress never intended to allow the Government to use pen/trap devices to capture PCTDD content. That Congress would rely instead on an unenforceable pledge by the DOJ makes no sense. Unfortunately for the Government, no statutory suppression remedy actually exists.

We emphasize two additional points about the Government's current discussion of the DOJ memo. First, on an initial read of

the Government's May 18th brief, the Government appeared to be claiming that its pledge not to use the captured communications content for "affirmative investigative purposes" was somehow enforceable in the particular applications before this Court. The Government distinguished the DOJ memo and emphasized that "this Office" -- the U.S. Attorney's Office in the Eastern District of New York -- included a "representation" in every pen/trap application that essentially repeated the relevant portion of the DOJ memo. May 18th Br. 10. The prosecutor implied that the inclusion of this "representation" in the applications somehow made a difference -- i.e., that his Office's not-to-use pledge was binding. Id. Contrasting the Department's memo with the Eastern District's "representations", the prosecutor explained:

> By its express terms, the DOJ PCTDD Policy Memorandum establishes no remedy. But as amicus was in all probability unaware, it is this Office's standard procedure in any application . . . to make the . . . representation [that it would not affirmatively use PCTDD content] . . . .

May 18th Br. 10 (emphasis added); see also id. 10 n. 4 (similarly distinguishing DOJ memo from the EDNY USAO's practice of "implement[ing]" it by including the no-use "representation" in its pen/trap applications). As the prosecutor further stated, "at minimum, the standard representation in our applications provides colorable grounds for redress." Id.

But on a closer examination, the suggestion of enforceability is an illusion -- the prosecutor never actually commits to the

proposition that his "representations" to the Court are enforceable. (Even assuming that an individual Assistant United States Attorney has the authority to overrule DOJ policy and the DOJ memo's explicit statement of unenforceability). "Colorable" is the classic substance-less qualifier in this context -- it sounds as if the prosecutor is pledging something when he is not.

The deception continues when the Government writes, "We have no doubt that were the government to fail to honor that commitment [as set forth in the "representation"], amicus would insist that, as to any intercepted party, such a failure would require that any content that the government used and any other evidence obtained as a result be suppressed." Id.; see also id. 9 (noting that "amicus itself would argue that such a remedy is in place"). But that is of course totally irrelevant. The question is not what "amicus" would like, but whether the Government would agree that suppression is required in light of its "representations." Since the Government refuses to commit to the enforceability of these representations, the Court should treat them in the same manner as the DOJ memo: A meaningless and unreviewable statement of intent, and nothing more.[14]

---

[14] In the Government's more recent brief of June 1st, which principally addresses the Fourth Amendment problem raised by its reading of the Pen/Trap Statute, the Government asserts that "Congress[] [has] amend[ed] the Pen/Trap Statute so that it not only (a) authorizes recording of PCTDD non-content, but also (b) conditionally permits the government incidental access to PCTDD (continued...)

Second, amici emphasize that even under the Government's own policy, the Government can keep, categorize, and store all communications content it obtains from pen/trap devices, and may use this information in any manner it deems appropriate, so long as it is not used -- in its own opinion, subject to no review whatsoever -- in an "affirmative investigative" manner. The DOJ memo is explicit on this point: "[N]othing in this Memorandum should be construed to preclude an agency from maintaining a record of the full information obtained by the agency from a pen register or trap trace device." DOJ Memo 5 n. 2. Thus, the Government could "retain a file copy of all of the information it received from a pen register or trap and trace device" for perpetuity, including passwords, account information, and PINs, and use this vast trove of information in any manner it desired so long as the use did not qualify as -- again, in accordance with the DOJ's own, unreviewable judgment -- an "affirmative investigative" use. Id.

---

[14] (...continued)
content while (c) withholding authorization to use such content . . . ." June 1st Br. 28 (emphases added). Congress has said nothing about "withholding authorizing to use such content," as the Government well knows.

The same falsehood is repeated later: "[B]y permitting incidental access to PCTDD content but not authorizing its use under the Pen/Trap Statute, Congress effectively precluded application of the plain view doctrine to such content." Id. 30-31 (emphases added). And again: "[I]n balancing the interests of individuals and law enforcement, Congress noticeably favored the former by limiting the class of PCTDD output available for investigative use under the Pen/Trap Statute to PCTDD content [sic]." Id. 31 (emphasis added).

5.

In sum, the Government now offers nothing to assure this Court that PCTDD content captured through a mere assertion of relevance will not be used by the Government for any purpose it deemed appropriate. This failure is reason enough to reject the Government's statutory analysis.

**CONCLUSION**

This Court should therefore deny the Government's applications. The plain language of the Pen/Trap Statute prohibits the Government from capturing communications content through pen/trap devices, which in any event would be barred by the Fourth Amendment.[15]

---

[15] The Government's claim that the sky will fall if a search warrant is required to obtain PCTDD content, see, e.g., June 1st Br. 33-34 (rejection of Government's applications would create "safe havens for criminal activity and . . . provide wrongdoers at random with cover . . . . The consequences to the public from this outcome would be severe."), should be quickly rejected. As the Supreme Court stated four decades ago, "we cannot forgive the requirements of the Fourth Amendment in the name of law enforcement." Berger, 388 U.S. at 62; see also United States v. Karo, 468 U.S. 705, 718 (1984) ("The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement.").

Moreover, amici's argument is not that the Government may never obtain the desired information, only that a Pen/Trap Order is not sufficient. As amicus EFF has explained, "[a] pen/trap order that excludes PCTDD will reveal whether the surveillance target is 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." Amicus Br., Exh. D at 10-11. Alternatively, "the Government can obtain a wiretap order as to the primary carrier."
(continued...)

For the foregoing reasons, amici respectfully submit 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
July 16, 2007

Respectfully submitted,

FEDERAL DEFENDERS OF NEW YORK, INC.
APPEALS BUREAU

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

ELECTRONIC FRONTIER FOUNDATION
Kevin Bankston, Esq.
454 Shotwell Street
San Francisco, CA 94110
Tel.: (415) 436-9333 x 126

[15] (...continued)
Id.

**CERTIFICATE OF SERVICE**

I certify that a copy of this Memorandum of Law has been served by e-mail and Federal Express 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
July 16, 2007

_____
**YUANCHUNG LEE**