UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF APPLICATIONS OF THE UNITED STATES OF AMERICA FOR ORDERS (1) AUTHORIZING THE USE OF A PEN REGISTERS AND TRAP AND TRACE DEVICES AND (2) AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION	:	06 Misc. 547 (JMA) 06 Misc. 561 (JMA) 07 Misc. 120 (JMA)

GOVERNMENT'S SUPPLEMENTAL MEMORANDUM OF LAW DEMONSTRATING THAT INCIDENTAL ACCESS TO POST-CUT-THROUGH DIALED DIGIT CONTENT UNDER THE PEN/TRAP STATUTE IS CONSTITUTIONAL

ROSLYNN R. MAUSKOPF
United States Attorney
Eastern District of New York
156 Pierrepont Street
Brooklyn, New York 11201

JED DAVIS
Assistant U.S. Attorney
(Of Counsel)

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF APPLICATIONS OF THE UNITED STATES OF AMERICA FOR ORDERS (1) AUTHORIZING THE USE OF A PEN REGISTERS AND TRAP AND TRACE DEVICES AND (2) AUTHORIZING RELEASE OF SUBSCRIBER INFORMATION	:	06 Misc. 547 (JMA) 06 Misc. 561 (JMA) 07 Misc. 120 (JMA)

GOVERNMENT'S SUPPLEMENTAL MEMORANDUM OF LAW DEMONSTRATING THAT INCIDENTAL ACCESS TO POST-CUT-THROUGH DIALED DIGIT CONTENT UNDER THE PEN/TRAP STATUTE IS CONSTITUTIONAL

PRELIMINARY STATEMENT

The government respectfully submits this memorandum of law in further support of its application for authorization pursuant to the Pen Register and Trap and Trace Statute, 18 U.S.C. §§ 3121 et seq. ("Pen/Trap Statute") to use pen registers to record post-cut-through dialed digits ("PCTDD") dialed by specified telephones (the "subject telephones").

By Order dated May 7, 2007, the Court directed the government to brief "the issue of whether the Fourth Amendment acts as an absolute bar to Government access, pursuant to the Pen/Trap Statute, of post-cut-through dialed digits that may contain content." We understand the Court's directive to assume, as our previous submissions show, that the Pen/Trap Statute permits the government in the course of collecting PCTDD non-content incidentally to access -- but not to use -- PCTDD content, when no

"technology [is] reasonably available to" the government to avoid that access. 18 U.S.C. § 3121(c).

The Fourth Amendment imposes no absolute ban on the Pen/Trap Statute so operating. A search or seizure pursuant to the Pen/Trap Statute violates the warrant requirement of the Fourth Amendment only if the search or seizure invades the user of the subject telephone's reasonable expectation of privacy. Smith v. Maryland, 442 U.S. 735 (1979). No such violation occurs unless the user of the telephone has "'an actual (subjective) expectation of privacy," and that expectation is "'one that society is prepared to recognize as "reasonable."'" Smith v. Maryland, 442 U.S. at 740, quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

As shown below, the instant applications comport with the Fourth Amendment because there is no reasonable expectation of privacy with respect to PCTDD content. The applications do not impinge on any actual expectation of privacy because telephone users typically understand that if they transmit PCTDD content by the same means as they dial a call -- by entering touchtones on their telephones --they assume the risk that their providers will collect all such dialed-digits. Moreover, no such subjective expectation with respect to PCTDD content can properly be

recognized by society as "reasonable." The balance of individual and government interests favors incidental access to content under the terms of the instant applications, because:

(a) A telephone user likewise assumes the risk that the provider through whom the user originates a call will record and disclose PCTDD content as well as PCTDD non-content;

(b) PCTDD content is by nature marginally communicative and largely composed of material as to which the caller assumes the risk that the intended recipient has already recorded or may record it in the ordinary course of business;

(c) Congress struck a special balance in the Pen/Trap Statute between the government's right to obtain and use PCTDD non-content and preventing pen registers from being used to acquire PCTDD content for investigative purposes. That balance is entitled to deference;

(d) Overruling Congress' determination to permit incidental access to PCTDD content would have a consequence that society cannot reasonably be required to bear: it would place PCTDD non-content beyond the reach of criminal investigation except when the government could satisfy Title III's far more demanding requisites with respect to PCTDD content at the same time as the government collected PCTDD non-content pursuant to the Pen/Trap Statute.

I.
THE NATURE OF THE PROPOSED INCIDENTAL ACCESS TO CONTENT AND THE STATUTES AND DOJ POLICIES PURSUANT TO WHICH IT IS SOUGHT

A. PCTDD Content & Non-Content

When a person initiates a telephone call, all of the digits that he thereafter enters on his telephone keypad are transmitted to the originating switch of a service provider (the "originating provider"). PCTDD are digits that a user dials after the initial call setup is completed, or "cut-through" from originating switch to the next switch in the sequence needed to connect a call. The next switch and any subsequent switches may all be owned by the originating provider (e.g., Verizon) or, as is likely in the highly competitive U.S. market, consist of a switching chain in which each successive switch is owned by different providers (e.g., T-Mobile, followed by Sprint, followed by a prepaid calling card service).

In either event, the transmission of post-cut-through digits starts with the user's telephone and immediately thereafter passes to the originating switch of the originating provider. If any other providers carry the call, the originating provider passes the PCTDD to the next provider in the sequence.

1. PCTDD Non-Content

PCTDD non-content consists of digits that a user enters on his keyboard and transmits to his originating provider and on which the originating or a subsequent provider in the sequence

depends in order to route and address a call. For example, in instances in which the originating switch requires only the initial part of that number (e.g., the first 6 digits) to identify the next switch to which a call should be routed, PCTDD non-content includes the tail end of a standard 10-digit telephone number (e.g., the last 4 digits).[1]

Likewise important in criminal investigations, the PCTDD non-content that a user enters and transmits through his originating provider may also include digits intended to be used by a calling card service for call processing and signaling purposes. For example, the access codes and destination telephone numbers that a caller enters, then transmits through an originating provider to a calling card access line, are PCTDD non-content. The U.S. market for domestic and international calling card services has grown exponentially. See, e.g., Atlantic-ACM, "Prepaid Calling Cards: Market Dynamics and Forecast" (2003) (reporting the U.S. market to have a value of $3.7 billion, to have experienced compounded annual growth of 25.4% between 1995 and 2002). Accordingly, so too has the volume of PCTDD non-content that customers of such services transmit through their originating providers.

[1] In other words, any 10-digit telephone number that a subject telephone dials at the outset of a call may be only partially revealed by pre-cut-through dialed digits, in which case identifying the full 10-digit telephone number would require access as well to post-cut-through dialed digits.

The volume of PCTDD non-content has also significantly expanded as many organizations in the United States have shifted their telephone service to private branch exchange systems ("PBXs"). See, e.g., "PBX Market Gets Ready To Shift Gears," Business Communications Review (2000) (describing large, maturing market in which suppliers earned $5 million in revenues from sales in the U.S. both to large and small companies). A PBX comprises telephone switching and associated computer equipment that unlike previous generations of office telephone systems, the organization owns and maintains on its premises. A PBX typically supports one or more "trunk" lines, e.g., the main telephone number of a company through which a caller can dial numerous internal extensions. Accordingly, as the PBX market has grown, so too has the volume of PCTDD non-content occasioned by telephone users calling a trunk line, then entering on their keyboards digits corresponding to the respective internal extensions to which they wish to connect.

2. PCTDD Content

Of course, it is also possible for a telephone user to transmit content using PCTDD. Initially, such a capability was limited to the "display" pager context, in which a user would dial the number that paging service assigned to such a pager and upon connecting, enter digits that the service would transmit for display on the device. The possible permutations that a user may enter are vast and therefore, so too are the various digital codes

conveying communicative content (e.g., "911 202-616-0000") that a caller may enter.

In recent years, however, demand for paging services in the U.S., and thus, transmission of PCTDD content through them, has fallen sharply with the spread of competing technologies. The competing technologies include wireless telephones with caller-ID, call logging and personal telephone book capabilities, which supplant the need for callers to identify themselves through callback number or pager codes. Pager has also been displaced by telephone-based text-messaging and email, with which it is far easier for users to engage in a broad range of expression than it is coded pager messages. See, e.g., "Why Carriers Must Push New Services, Subscriber Gear," Wireless Data News (January 28, 2004) (reporting that due to competition from other wireless products, number of pager subscribers in United States dropped from 45 million in 1999 to 12 million in 2003).[2]

With the decline in pager use, a significant volume of PCTDD content remains, created mainly by telephone users interacting with automated operator systems. Such systems employ pre-recorded voice messages that prompt users to request information or transactions and that also report the results of requests

[2] As the Court is aware, a pen register collects PCTDD using processes separate from those used to collect routing and addressing information or content with respect to telephone-based text-messages and e-mails. In other words, collection of PCTDD does not enable collection of text messages or e-mails.

or transactions. A caller transmits PCTDD content from his keypad and through his service provider to an automated operator system in order to identify himself or make a request. For example, a person may call his bank's automated service line, identify himself by dialing his bank account number and/or passcode and, when asked to choose from options, choose the option number corresponding to a request for his current account balance.[3]

While there is no question that PCTDD of either kind constitutes "content," it is likewise evident that the content in question is more limited in its range of expression than conversation between two human beings. For instance, a caller to a bank automated operator is likely to be able to use PCTDD content to request his account balance, but not to be able to request an explanation of the more arcane question of how to redeem savings bonds.

Moreover, in the many cases in which callers convey PCTDD content to automated operators at organizations at which they maintain accounts, the content either already is or is about to become records of the organizations. In other words, PCTDD content often carries with it a greater risk of recording by the recipient than other forms of conversation. For example, a bank passcode entered by a caller is PCTDD content, but it is also already a

[3] Many such automated telephone services, however, are increasingly being displaced by comparable Internet-based services.

record of the bank, which it uses to verify the caller's claim to be an authorized accountholder. In addition, for security purposes, the bank is likely to keep a record reflecting the time that the verified accountholder logged-in by means of PCTDD. Similarly, if a verified accountholder dials PCTDD to request to transfer a specified amount between accounts, the bank may make and keep an entry reflecting the content conveyed by the digits as part of the bank's records for that account.

3. All PCTDD Is Subject To Recording By The Originating Provider

PCTDD non-content and PCTDD content are both subject to recording by the originating provider, and on the same channel. Typically, an originating provider of telephone service sets up a call by means of two channels, a "control channel" and a "content" channel. The control channel handles routing, addressing and other signaling information, including pre-cut-through digits. Notwithstanding its name, the content channel not only carries substantive communications, including PCTDD content, but also routing and addressing information, including PCTDD non-content, such as the tail-end of a 10 digit number (see above) or the telephone number that a caller seeks to reach through a calling card service.

For its own legitimate business purposes, an originating provider may record both the pre-cut-through digits that a caller transmits via the provider's control channel and the PCTDD, whether content or non-content, that the same caller transmits via the

provider's content channel. A provider often records pre-cut-through digits for billing and network planning purposes. More importantly for the purposes of the instant discussion, if an originating provider suspects that a user is fraudulently obtaining service or misusing the service to harass another person, that provider may also monitor and collect information traveling over the content as well as the control channel.[4] While, a provider investigating such suspected fraud or harassment may not need to record the user's oral conversations, typically its investigation will include the use of pre-existing facilities to record and decode all PCTDD, both content and non-content.

B. The Statutory and Regulatory Framework That Governs The Instant Applications

1. The Pen/Trap Statute

The government seeks authorization pursuant to the Pen/Trap Statute to install and use pen registers to acquire digits dialed by the subject telephones, including PCTDD. The Pen/Trap Statute authorizes the government to install and operate a pen register, provided that (among other things) it certifies to a

[4] 18 U.S.C. § 2511(2)(a)(i) specifically permits employees of providers "to intercept, disclose or use" a wire or electronic communication "in the course of his employment or while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of rights or property of the provider of that service." (emphasis added)

Court that "the information likely to be obtained is relevant to an ongoing criminal investigation." 18 U.S.C. § 3122(b).

The current version of the Pen/Trap Statute empowers the government both to acquire via pen register and to use in its investigation any digits that a caller may enter to process and transmit calls. The same statute establishes ground rules governing circumstances in which it is difficult for the government to know in advance of reviewing pen register output whether content is commingled with the non-content in the digit stream that a device or process acquires. Specifically, 18 U.S.C. § 3121(c) requires that the government:

> 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). Whether "technology [is] reasonably available to" the government that would keep a pen register from confusing content with the non-content that is the device's principal object determines whether the Pen/Trap Statute permits collection of content. If such technology exists, 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.

But while § 3121(c) permits incidental access in the absence of the specified technology, a companion provision removes such content from the categories of evidence that the Pen/Trap Statute authorizes the government intentionally to target. The Pen/Trap Statute defines a "pen register" to include any "device or process which records or decodes dialing, routing, addressing or signaling information transmitted by" a telephone, "provided however, that such information shall not include the contents of any communication." 18 U.S.C. 3127(3). Accordingly, when such a government-operated device or process records or decodes non-content routing, addressing or similar information, it is functioning as a "pen register" within the statutory definition. On the other hand, if at some other time, the same device or process accesses content, it is not functioning as a pen register and accordingly, its output during that interval is excluded from the class of data that the Pen/Trap Statute permits the government intentionally to seek.

2. DOJ Regulations

On May 24, 2002, DOJ issued a policy memorandum establishing the Department's procedures with respect to the risks that a pen register may collect content in the form of dialed digits and an agency might thereafter use that content for investigative purposes. A true and correct copy of that memorandum

was previously submitted as Exhibit 1 to the government's reply in the principal briefing (hereafter "DOJ PCTDD Policy Memorandum").

DOJ promulgated the memorandum in response to the enactment in 1994 of § 3121(c)'s "technology reasonably available clause" and the addition in 2001 to § 3121(c) and § 3127(3) of language expressly disfavoring the collection of content via pen register. DOJ PCTDD Policy Memorandum at 1-4. The memorandum:

> a. Directs members of the Department to assure that investigating agencies "use 'technology reasonably available"' to "minimiz[e] any possible over-collection of" content "while still allowing a device to collect all of" the authorized non-content;
>
> b. Directs members of the Department, when "reasonably available technology" cannot avoid "incidental collection of content" to make "[n]o affirmative investigative use" of that content unless such use is permitted by the constitution and otherwise authorized by law; and
>
> c. Directs members of the Department to coordinate within components of the Department to assure that determinations of whether access to content is at issue apply the definition of content codified within Title III: "'content' . . . 'include[s] any information concerning the substance, purport or meaning of [a] communication' 18 U.S.C. § 2510(8)."

DOJ PCTDD Policy Memorandum at 4-5.

3. The Instant Applications Comply With The Pen/Trap Statute and DOJ Policies

The pending applications seeking authorization to acquire PCTDD adhere to the above provisions of the Pen/Trap Statute as well as the directive of the DOJ PCTDD Policy Memorandum. The government has represented in its applications (at ¶ 8 of each) and

thereafter submitted evidence in connection with hearing that demonstrates that there is no "technology reasonably available to" the government that permits it to distinguish PCTDD non-content from content before a pen register collects both. Accordingly, § 3121(c) permits the government to access PCTDD content incident to collecting non-content, the statute's condition precedent to a contrary outcome -- that the contemplated "technology reasonably available" actually exist --having not been satisfied.

The DOJ PCTDD Policy Memorandum expressly recognizes, however, what 18 U.S.C. §§ 3121(c) and 3127(3) jointly imply: the conditional permission that § 3121(c) confers on the government incidentally to access content is subject to the provisions of § 3127(3) that authorize targeting only of PCTDD non-content. Under the memorandum (at 4-5), the government must avoid use of such content, except under limited constitutional exceptions or as otherwise permitted by law. In the instant applications (at ¶ 8 of each) and indeed, in all current applications, this Office commits to fulfill this objective by means of the following representation to the Court:

> the government represents that if the present pen register incidentally collects any "content," such "content" will not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security.

Accordingly, before the government makes investigative use of any PCTDD, it must confirm that what it seeks to use is

PCTDD non-content. This may require identifying the use that the communication service that ultimately receives the PCTDD makes of it. For example, if the telephone number receiving the PCTDD is 1-800-CALL-ATT, it will be relatively easy to determine that the PCTDD that followed were digits utilized in processing and transmitting a call via calling card. But in other circumstances, the function that the PCTDD digits serve cannot be known unless the government learns the lexicon of the automated telephone service that received those digits, and what the digits signify within the lexicon. Thus, for example, with respect to a call to a store's automated service, an agent could not know that the PCTDD was used to convey content (e.g., the number of the caller's account at the store) rather than non-content (e.g., a request to connect to an internal store extension) until he ascertained how the store's automated operator interpreted the digits received and thus, the content that they conveyed.

In the first instance, it is responsibility of the government to determine how to probe whether PCTDD is content or non-content. Under Dalia v. United States, 441 U.S. 238 (1979), "[i]t is generally left to the discretion of" officers executing a search warrant to determine the details of how best to proceed with the performance of a search authorized by warrant, subject, of course, to the general Fourth Amendment protection 'against unreasonable searches and seizures, and accordingly "to later

judicial review as to its reasonableness." 441 U.S. 257-58. This rule governs applications made pursuant to the Pen/Trap Statute, since Dalia "has [as much] force in the context" of lawful orders to acquire evidence based on a showing "more lenient than for criminal search warrants," as it does in the criminal context, Donovan v. Enterprise Foundry, Inc., 751 F.2d 30, 36 (1st Cir. 1984). Accordingly, the specifics of how the government fulfills the objective established by the Pen/Trap Statute and the DOJ PCTDD Policy Memorandum not to use content is entrusted to the government at the current (investigative) stage and on any review triggered by a motion to suppress, by the courts. Dalia, 441 U.S. 257-58.

II.
THE FOURTH AMENDMENT PERMITS THE GOVERNMENT UNDER THE PEN/TRAP STATUTE TO ACCESS PCTDD CONTENT INCIDENT TO ACQUIRING PCTDD NON-CONTENT

A. Smith, Katz and Miller Are The Guideposts That Determine Whether Any Expectation Of Privacy In PCTDD Content Is Reasonable

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures" and requires that search warrants be issued only "upon probable cause, supported by Oath or affirmation and particularly describing the persons or things to be seized." In general, courts evaluate whether the government's access or acquisition of evidence without a search warrant is "reasonable" under the Fourth Amendment by "'examining

the totality of the circumstances." United States v. Knights, 534 U.S. 112, 118 (2001). This reasonableness inquiry requires "assessing on the one hand the degree to which [a search without a warrant] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate government interests." Id. at 118.

Smith v. Maryland, 442 U.S. 735 (1979), together with two other cases on which Smith depends, Katz v. United States, 389 U.S. 347, 361 (1967) and United States v. Miller, 425 U.S. 435 (1976), provide the crucial analytic framework for balancing individual privacy and legitimate governmental interests. In Smith, petitioner had been convicted of robbery based on evidence derived from a pen register on his home phone number. The police had obtained the pen register without a warrant and installed it at phone company offices. The issue on appeal to the Supreme Court was whether petitioner had possessed a reasonable expectation of privacy in numbers dialed from his home, thereby rendering the installation of the pen register a "search" under the Fourth Amendment that was invalid for lack of a warrant. 442 U.S. at 737-38.

Smith held that petitioner had not possessed a reasonable expectation of privacy in the numbers that he dialed and accordingly, no "search" for which the Fourth Amendment requires a

warrant had occurred. 442 U.S. at 739-745.[5] In reaching this conclusion, Smith placed principal reliance on Katz, lauding it as the "lodestar" with which to "determin[e] whether a particular form of electronic surveillance is a 'search' within the meaning of the Fourth Amendment." Smith, 442 U.S. At 739.

Katz established a two-pronged inquiry for deciding whether a person has a reasonable expectation of privacy (in that case, holding that such a person can reasonably expect privacy with respect to his calls from a public telephone booth). As explained by Justice Harlan in his concurring opinion, the first prong requires asking if the affected party, by his conduct "exhibited an actual (subjective) expectation of privacy." Katz, 389 U.S. at 361. The second prong requires asking if that party's subjective expectation of privacy is "one that society is prepared to recognize as reasonable." Id. at 361.

Applying Katz's two-part test, Smith held that neither a subjective nor objective expectation of privacy obtains with respect to the warrantless acquisition via pen register of dialed

---

[5] The Supreme Court remarked in Smith that its focus on whether there was or was not a reasonable expectation of privacy in dialed telephone numbers reflected the limits of the then-extant telephone system, in which telephone numbers could be used only as "'a means of establishing communication,'" rather than as a means to express the substance of a communication, 442. U.S. 735 (citation omitted). As shown below Smith's approach is likewise appropriate to gauge reasonable expectations of privacy in the current telephone system, which does permit callers to convey substance through dialed digits.

telephone numbers. As to the subjective prong, Justice Blackmun, writing for the majority, emphasized as follows:

> [W]e doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. . . .
>
> Telephone users . . . typically know . . . that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes. Although subjective expectations cannot be scientifically gauged, it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret.

Smith, 442 U.S. at 742 (emphasis added). Notably, in support of the conclusion that a service provider not only could but often did record dialed telephone numbers for legitimate business purposes, the Court cited as common knowledge that providers recorded those dialed digits both for billing purposes and "'for the purposes of detecting fraud[,] preventing violations of law,'" and "to aid in the identification of persons making annoying or obscene calls." Id. at 742-743 (quoting citation omitted).

Moreover, Smith held, even if a person actually believed that the telephone company would keep private the phone numbers that he transmitted to it by dialing, such an expectation was not one that society was prepared to recognize as reasonable. For to do so would be at odds with a countervailing principle that Miller exemplifies and that effectively aids law enforcement: "a person

has no legitimate expectation of privacy in information that he voluntarily turns over to third parties." Smith, 442 U.S. at 743-44.

Just as "a bank depositor has no 'legitimate "expectation of privacy"' in financial information 'voluntarily conveyed to . . . banks and exposed to their employees in the ordinary course of business,'" Smith, 442 U.S. at 744 (quoting Miller), the petitioner in Smith had no such legitimate expectation in "numerical information" that "he voluntarily conveyed . . . to the telephone company and 'exposed' . . . to its equipment in the ordinary course of business." Id. Rather, "petitioner assumed the risk that the [telephone] company would reveal to police the numbers he dialed." Id. Moreover, whether it was the routine practice of the telephone company to record the same dialed digits that a pen register acquired was immaterial. For "petitioner assumed the risk that" numeric information would be divulged to police" in any instance that he voluntarily conveyed to a provider that "facilities to record it and that it was free to record." Id. at 745.

B. Telephone Users Have No Reasonable Expectation Of Privacy In The Incidental Access To PCTDD Content Proposed Here

For much the same reasons no search warrant is required under Smith to operate a pen register to record dialed telephone numbers, no search warrant is required to authorize the incidental access to PCTDD content that the government seeks here. As demon-

strated below, no reasonable expectation of privacy exists with respect to PCTDD content under either the subjective or objective prong of the Katz test. Moreover, as in Smith, a principal ground that precludes treating such an expectation as reasonable (albeit in this case one ground among several) is the rule established by Miller: a person who voluntarily conveys information to a third party assumes the risk that the third party will record and thereafter disclose it to law enforcement. Since there is no reasonable expectation of privacy, the incidental access to PCTDD content is not a "search" within the meaning of the Fourth Amendment. Accordingly, the Fourth Amendment permits the proposed operation without a warrant of the pen registers under authority of the Pen/Trap Statute. Katz, 442 U.S. at 739-41.

1. No Claim Of A Subjective Expectation Of Privacy Is Sustainable

Each of the instant applications seeks to use a pen register installed on the premises of the originating service provider of a target telephone in order to acquire PCTDD. Because each of these cases is in the investigative stage, it is unknown whether any user will argue not to have understood the risk he assumed by dialing digits on a telephone line connected to his originating provider. As in Smith, however, it is already obvious that no such claim withstands scrutiny.

The telecommunications market has evolved since that decision, so that a typical call is not carried solely by a single, originating provider, but rather, by the originating provider and additional providers to whom it forwards information. Yet it remains as obvious today as it was when Smith was decided that "[a]ll telephone users realize that they must" 'convey'" to their originating providers the digits that they dial. Id. at 742. Accordingly, each user of the current telephone system must know that the digits that he enters, including PCTDD, pass to his originating provider.

Moreover, currently, just as when Smith was decided, a user "typically know[s] that the [originating provider] has facilities for recording" the digits that he dials and "does in fact record this information for a variety of legitimate business purposes." Id. at 743. The advent of PCTDD content requires no modification to the Supreme Court's approach or holding, since it was based not merely on the fact that originating providers record dialed digits not only for billing purposes, but also to investigate fraudulent or harassing use of its telephone service. Id. at 742-43. As previously explained the facilities that originating providers have and use today to combat fraud and harassment include equipment that records all PCTDD.

Accordingly, it is "too much to believe that telephone users . . . harbor any general expectation that" the digits that

they dial, including PCTDD content "will remain secret," Smith, 442 U.S. at 743. The basics of telephone use -- that when one dials, one is transmitting digits to at minimum, one's originating provider -- and the obvious capability of that provider to record it rule out any other conclusion.

2. An Expectation Of Privacy In The Subject PCTDD Content Is Not One That Society Is Prepared To Recognize As Reasonable

a. Under Miller, A Caller Bears The Risk That A Provider Will Disclose PCTDD

The same facts that make any subjective expectation a non-starter also demonstrate that any expectation of privacy in PCTDD content is objectively unreasonable. As a matter of law, no one has legitimate expectation of privacy in information that he voluntarily conveys to a third party. Rather, he "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government," even if "the information is revealed on the assumption that it will be used for only a limited purpose and the confidence placed in the third party will not be betrayed." Miller, 425 U.S. at 443, quoted in Smith, 442 U.S. at 744.

As in Smith, any user of the current telephone system "voluntarily convey[s] numerical information to" his originating provider and 'expose[s]' that information to" that provider's "equipment in the ordinary course of business. Smith, 442 U.S. at 744. The user's assumption of the risk encompasses the full scope

of information for which the provider "ha[s] facilities for recording and that it [is] free to record." Id. at 745. As previously explained, providers in the current system have equipment that records all PCTDD without discrimination between content and non-content. Moreover, while that equipment is reserved for detection of calling fraud, harassment and similar misuse, Miller teaches that a person who entrusts a third party with information assumes all consequences within the scope of a potential betrayal of trust by the third party.

Accordingly, any user who elects by means of his keyboard to convey PCTDD content contemporaneous with PCTDD non-content has no reasonable expectation that the provider receiving the PCTDD will refrain from recording all of it and disclosing it to law enforcement. Miller, 425 U.S. at 443.

b. An Expectation Of Privacy In Most PCTDD Content Is Otherwise Suspect Under Miller

In "assess[ing] the degree" to which access to PCTDD content may "intrud[e] upon an individual's privacy," against legitimate government interests, United States v. Knights, 534 U.S. at 118, the Court may also consider whether a caller has evinced a lack of expectation in that content's privacy by disclosing it to parties in addition to his originating provider. As explained below, much if not all of the PCTDD content for which the government seeks permission incidentally to access comprises

information that under Miller, the caller may have assumed the risk of disclosure to law enforcement by such other parties by the time those calls occur, if not by the originating party, then by the ultimate intended recipient of the information.

The range of expression that can be conveyed by PCTDD content is limited because PCTDD by definition consists merely of digits. Instead of being able to arrange words into sentences to convey virtually any message, a caller transmitting content by means of PCTDD is limited to the far smaller class of numeric codes that the intended automated recipient is programmed to understand (e.g., to understand the entry of the number "2" as a request for directions to a store or of the digits "1000" to request trains departing at or about 10:00 A.M.). Thus, in many contexts in which PCTDD content is used, it is either impossible or at minimum, extremely difficult to communicate anything intimate.

A notable exception, of course, are pager calls, in which the caller and those she calls may have previously agreed upon more elaborate codes (e.g., "007" to signify to a recipient the police have arrived, or "1-411" for a mother to communicate to her son that he should call her). The frequency and volume of paging messages, however, have dropped as most users have migrated to other platforms. Accordingly, the government believes that the PCTDD content that the pen register would be most likely to access in the course of seeking non-content are digits that a caller

transmits to the automated operator of a business or other service organization with whom the caller maintains an account. As previously explained, PCTDD content entered in such contexts 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 .

Under Miller, 425 U.S. at 442-44, 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. Obviously, a caller's assumption of that risk is distinct from his assumption of the risk that the originating provider will disclose the same information. When, as is likely to occur here, however, a caller assumes both risks, the risk that he runs with respect to the recipient organization is further proof that he cannot reasonably expect that the digits that transmits to the provider for forwarding to that organization will remain confidential.

c. Congress' Balancing Of Individual And Governmental Interests Is Entitled To Deference

Whether an expectation of privacy is "one that society is prepared to recognize as 'reasonable,' Katz, 389 U.S. at 361, requires courts to consult "sources outside of the Fourth Amendment, either by reference to concepts of real or personal

property or understandings that are recognized and permitted by society." Rakas v. Illinois, 439 U.S. 128 note 12 (1979). In Smith, for example, the "understanding" on which the Supreme Court relied to hold that a person has no legitimate expectation of privacy in the numbers that he dials was Miller's assumption of the risk doctrine.

Legislation that is the focus of a Fourth Amendment inquiry, however, is itself another important source of society's essential "understandings," especially legislation regulating electronic surveillance. In general, a "heavy presumption of constitutionality" attaches to the "'carefully considered decision of a coequal and representative branch of [g]overnment." Dep't of Labor v. Triplett, 494 U.S. 715, 721. Moreover, this presumption is especially strong when the constitutionality of "an Act of Congress . . . turns on what it is 'reasonable'" under the Fourth Amendment, United States v. Di Re, 332 U.S. 581 (1948), and in particular, to evaluating electronic surveillance statutes for the purposes of that Amendment. As the Fourth Circuit explained in United States v. McNulty, 47 F.3d 100 (1995):

> [C]ourts should be cautious not to apply [Katz] in a manner that nullifies the balance between privacy rights and law enforcement needs struck by Congress . . . . Decisionmaking in this area demands a comprehension of complex technologies . . . . As new technologies continue to appear in the marketplace and outpace existing surveillance law, the primary job of evaluating their impact on privacy rights and of updating the law must

> remain with the branch of government designed to make such policy choices, the legislature.

McNulty, 47 F.3d at 105-06.[6]

As shown below, Congress' amendment of 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 content while (c) withholding authorization to use such content entails precisely the kind of balancing of personal and governmental interests in a complex telecommunications matter that is entitled to deference.

First, Congress has predicated permission for any incidental access on an express condition precedent: whether there exists "technology reasonably available to" the government to avoid such access. See 18 U.S.C. § 3121(c). When such technology exists, the government must use it to restrict a pen register to recording non-content, in deference to the interests of the user of the target telephone. When, however, no such "technology [is] reasonably available to" the government, the balance under the Pen/Trap Statute shifts, permitting the government as it seeks PCTDD non-content via pen register incidentally to access PCTDD content, Id., but expressly withholding authorization to target

---

[6] Thus, for example, in McNulty and Price v. Turner, 260 F.3d 1144, 1158-49 (9th Cir. 2001), courts deferred to Congress' decision by Congress to exclude from the requirements of Title III interceptions of wire communications emanating from the radio portion of a cordless telephone.

that content under the language of 18 U.S.C. § 3127(3) directing that a device "shall not" be counted as a "pen register" when it acquires content.

Second, by withholding authorization for content to be targeted under the Pen/Trap Act, Congress imposed unusual restrictions on the government's latitude to investigate. As the DOJ PCTDD Policy Memorandum and our representations to effectuate it demonstrate, statutory permission incidentally to access content without authorization to use it means the government must avoid such use. As shown below, this cabins the potential focus of the investigation to a substantially greater degree than is the case with comparable searches of premises authorized on a showing of less than (criminal) probably cause and that involves similarly voluminous, commingled documents, some of which falls within the specified scope of a court order and some of which does not.

"In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are in fact, among the papers authorized to be seized." Andresen v. Maryland, 427 U.S. 463, 482 1976); accord United States v. Consolidation Coal, 560 F.2d 214, 219-221 & note 5 (6th Cir. 1978) (upholding regulatory search "to locate objects of . . . inquiry" that were "intermingled in mine operators' files"), vacated on other grounds, 436 U.S. 942 (1978), reinstated 579 F.2d 1011 (6th Cir. 1978).

In most instances, however, the latitude that the government has to assess the full range of evidence acquired "at least cursorily," Andresen, supra, may be expanded for investigative purposes pursuant to the plain view doctrine.[7] If the acquiring agency has lawful access to the space searched, and at the time of their discovery, the documents were in plain view when discovered and their inculpatory nature "immediately apparent," they are available for investigative use. See United States v. Rude, 88 F.3d 1538, 1551-1552 (9th Cir. 1996) (relying on Horton v. California, 496 U.S. 128, 136 (1990)); United States v. Rude, 986 F. Supp. 163, 169 (S.D.N.Y. 1997) (same). Thus, for example, a person who voluntarily commingles materials from his separate firm in the same space in which another, closely-regulated company with which he is associated does business, runs the risk that regulators searching for files from the other company will obtain files from his own firm for use in their investigation. United States v. Chuang, 897 F.2d 646, 651 (2d Cir. 1990).

In contrast, by permitting incidental access to PCTDD content but not authorizing its use under the Pen/Trap Statute,

---

[7] The plain view doctrine applies to court-ordered administrative and "special needs" searches a showing, just as it does to search warrants in criminal cases. See, e.g., Palmieri v. Lynch, 392 F.3d 73, 81 (2d Cir. 2004) (environmental agency entitled to enter residential grounds to inspect dock in plain view); Platteville Area Apartment Ass'n v. City of Platteville, 179 F.3d 574, 579-80 (7th Cir. 1999) (housing inspectors who lawfully entered dwelling entitled to look for signs of occupancy code violations in plain view).

Congress effectively precluded application of the plain view doctrine to such content. It does not matter if a caller elects in a given call to commingle PCTDD content and non-content in the same (electronic) space or that the content's bearing on a criminal case may be "immediately apparent" to a reviewing agent. Except in life-threatening circumstances, once that agent, in the exercise of the government's discretion,[8] has analyzed the content sufficient to identify it as such, examination must end. For in 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.

d. To Overrule Congress With Respect To PCTDD Content Would Render PCTDD Non-Content Unreasonably Inaccessible To Law Enforcement

We respectfully submit that the consequence of rejecting Congress' decision to permit incidental access to PCTDD content the Pen/Trap Statute furnishes yet another ground for concluding that an expectation of privacy in PCTDD content is not one that society is prepared to recognize as reasonable: it would effectively make Title III the arbiter of whether the government is allowed to record PCTDD non-content.

The Pen/Trap Statute is principally addressed to the collection of "dialing, routing, addressing, and signaling

[8] See above discussion at 16.

information utilized in the processing and transmitting of wire or electronic communications." 18 U.S.C. § 3121(c). It authorizes collection of that information, including PCTDD non-content, upon the government's certification to a court that the evidence will likely be relevant in an ongoing criminal investigation. 18 U.S.C. § 3122(b). By contrast, Title III governs the interception and use the contents of wire and electronic communications. Title III authorizes such interception and use only upon a showing that probable cause exists to believe that a person is or persons are committing a crime and that communications concerning that offense will be obtained from the proposed interception and that normal investigative methods have not succeeded, are futile or too dangerous. 18 U.S.C. § 2518(3).

With respect to PCTDD, the Pen/Trap Statute and Title III operate independent of each other, so long as either of the two eventualities contemplated by § 3121(c) unfolds. Regardless of whether the government can meet the requisites of Title III to intercept and use PCTDD content, it can still obtain PCTDD non-content, provided it can certify relevance and either (i) there is "technology reasonably available" to cull PCTDD content from non-content, see 18 U.S.C. § 3121(c) or (ii) in the absence of such technology, § 3121(c) permits incidental access to content to proceed.

But as demonstrated at an earlier hearing, because the contemplated technology does not in fact exist, it is the second scenario that actually obtains. Accordingly, were § 3121(c)'s provision for incidental access to be found unconstitutional, the government's ability to obtain PCTDD non-content under the Pen/Trap Statute would depend on whether the government could meet the heavy burdens of Title III.

A functioning pen register could not avoid accessing PCTDD content that came its way, but § 3121(c) would not permit access to content. Thus, for the government lawfully to operate its pen register to acquire both PCTDD non-content and content, would require it to obtain concurrent authorization to record PCTDD non-content under the Pen/Trap Statute and to intercept PCTDD content under Title III. In many instances, however, the government would lack the extensive proof that Title III requires. And lacking concurrent authorization under Title III and the Pen/Trap Statute to collect PCTDD, the government could not collect any PCTDD non-content -- let alone PCTDD content.

The consequences to the public from this outcome would be severe. As previously explained, PCTDD non-content is principally composed of the information that callers transmit to calling card services and PBXs, as well as the tail-ends of standard-10 digit telephone numbers that originating providers did not need to pass the call to subsequent providers. In other words, law enforcement

would have no contemporaneous means of identifying (a) the telephone numbers that targets called through calling card access lines, both internationally and domestically, (b) the internal extensions that targets dialed at PBXs and (c) the complete 10-digits of numbers that the targets called.

We respectfully submit that such an outcome is not one that society can reasonably be required to bear to protect an expectation of privacy that as explained above, is in other respects, also highly questionable. Katz, 389 U.S. at 361. When the government lacks contemporaneous access to PCTDD non-content, calling card access lines and PBXs become safe havens for criminal activity and 10 digit telephone numbers provide wrongdoers at random with cover -- and society bears the cost of the government's inability to use constitutionally unprotected call processing information to investigate the underlying criminal activity. Accordingly, the balance of public and individual interests clearly favors upholding the incidental access to PCTDD without authorization of use that Congress established under the current Pen/Trap Statute in its current form.

CONCLUSION

For all of the above reasons, the Court should grant the government's request to permit the subject pen registers to acquire PCTDD non-content and incidentally to access but not to use PCTDD content.

Dated: Brooklyn, New York
June 1, 2007

Respectfully submitted,

ROSLYNN R. MAUSKOPF
United States Attorney
Eastern District of New York
One Pierrepont Plaza
Brooklyn, New York 11201

JED DAVIS
Assistant U.S. Attorney
(718) 254-6298