UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

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

----------X

A P P E A R A N C E S:

Jed Davis
Scott Klugman
Assistant U.S. Attorneys
1 Pierrepont Plaza
Brooklyn, New York 11201
Attorneys for the United States

Yuanchang Lee, Of Counsel
Federal Defenders of New York, Inc.
Appeals Bureau
52 Duane Street, 10th Floor
New York, New York 10007
Attorney for Amicus Curiae

AZRACK, United States Magistrate Judge:

The United States Attorney for the Eastern District of New York (the "Government") has made an ex parte application for the installation and use of a pen register under the Pen/Trap Statute, 18 U.S.C. §§ 3121-3127. In the application, the Government requested access to all dialed digits, including post-cut-through dialed digits, even if such digits may contain the contents of a telephone communication. This Court granted the application in part, but denied access to any post-cut-through dialed digits. In response to the Government's request, I agreed to reconsider the partial denial.

Federal Defenders of New York was requested to file an *amicus* brief on the issue and did so.[1]

This issue is a matter of first impression in this Circuit, although courts in Texas and Florida have addressed it and ruled that post-cut-through dialed digits ("PCTDD") may not be obtained with a pen register order. See In the Matter of the Application of the United States of America, 441 F. Supp. 2d 816, 818 (S.D. Tex. 2006) ("In re U.S. (S.D. Tex.)"); In the Matter of the Application of the United States of America, No. 06-MJ-1130 (M.D. Fla. June 20, 2006) ("In re U.S. (M.D. Fla.)"), affirming In re U.S., No. 06-MJ-1130 (M.D. Fla. May 23, 2006). This Court agrees with the decision rendered by both those courts, but for different reasons. Insofar as the issue has been addressed in dicta by the D.C. Circuit and a Massachusetts district court, those references also lend support to my decision. See United States Telecom Ass'n v. F.C.C., 227 F.3d 450, 462 (D.C. Cir. 2000); In re Application of the United States, 396 F. Supp. 2d 45, 48 (D. Ma. 2005).

I. BACKGROUND

In layman's terms, a pen register is a device capable of recording all digits dialed from a particular telephone. In 1979, the Supreme Court held that Government installation and use of such a device does not constitute a search within the meaning of the Fourth Amendment. Smith v. Maryland, 442 U.S. 735 (1979). The Court reasoned that pen registers do not implicate the Fourth Amendment because there is no legitimate expectation of privacy in the information they collect. Id.

---

[1] In its July 16, 2007 Supplemental Memorandum of Law, *amicus* added an additional contributor as a signatory, the Electronic Frontier Foundation ("EFF"). The Government notes EFF's appearance on the brief in its July 31, 2007 Sur Reply and states that: "EFF has not sought permission to appear as amicus in this case, nor did Federal Defenders make any such request on EFF's behalf." (Gov. Sur Reply dated July 31, 2007 ("Gov. Sur Reply") at 1.) Although *amicus* surely should have petitioned the Court to add EFF as a signatory to its brief, the Court sees no harm in allowing the submission, especially considering EFF's appearance as *amicus* in at least one similar case in another district. See In re U.S. (S.D. Tex.), 441 F. Supp. 2d at 818.

at 744. After Smith v. Maryland, Congress enacted laws to govern Government use of pen registers. See Electronic Communications Privacy Act ("ECPA") of 1986, Title III, § 301 (codified as amended at 18 U.S.C. §§ 3121-3127 ("Pen/Trap Statute").[2] The statute has since been amended twice.

Telephone use has expanded rapidly since the constitutionality of pen registers was examined in 1979. Today, Americans regularly use their telephones not just to dial a phone number, but to manage bank accounts, refill prescriptions, check movie times, and so on.

Dialed digits can now be categorized in a number of ways. "Post-cut-through dialed digits" ("PCTDD"), the subject of the instant application, "are any numbers dialed from a telephone after the call is initially setup or 'cut-through.'" In re U.S. (S.D. Tex.), 441 F. Supp. 2d at 818. In most instances, any digit dialed after the first ten is a PCTDD. "Sometimes these digits transmit real information, such as bank account numbers, Social Security numbers, prescription numbers, and the like." Id. In such circumstances, PCTDD contain the "contents of communication." Id. (citing U.S. Telecom, 227 F.3d at 462). At other times, PCTDD "are other telephone numbers, as when a party places a credit card call by first dialing the long distance carrier access number and then the phone number of the intended party," id., or when an extension number is dialed.

At issue are the parameters of the federal statute governing pen registers. The Government contends that pen register authorization entitles it to all digits dialed from a target telephone, including PCTDD that may include content. The Government maintains that federal law requires it

---

[2] Although this opinion addresses Government use of pen registers, it should be noted that the Pen/Trap Statute also applies to trap and trace devices. A trap and trace device functions much like a pen register, but it records information passing in the opposite direction. That is, a trap and trace device shows what numbers call a specific telephone, i.e. all incoming phone numbers. A pen register, on the other hand, shows what digits a phone has dialed, i.e. all outgoing phone numbers.

only to minimize the collection of content using reasonably available technology. If no technology exists that can sort content from non-content, the Government argues it is entitled to access all digits dialed subject only to Department of Justice ("DOJ") guidelines, which forbid the use of content gathered with a pen register absent extenuating circumstances, and federal wiretap laws. (See Gov. Supp. Mem. of Law 12-16.) For the sake of clarity, I will refer to the Government's position as the "minimization theory." Because the Government's position belies statutory interpretation and would violate the Fourth Amendment, the application is denied.

II. DISCUSSION

A. The Statutory Scheme

In order to examine the Pen/Trap Statute as it exists today, it is helpful to understand its genesis. In 1986, seven years after Smith v. Maryland upheld the constitutionality of pen registers, Congress enacted legislation which set forth the procedure the Government must follow and the burden it must meet to install and use one. 18 U.S.C. § 3122(a). The statute continues to express a general prohibition against the installation or use of a pen register without a court order. 18 U.S.C. § 3121(a). The standard for obtaining a court order is far from burdensome. An attorney for the Government must make an application for authorization to install and use a pen register "in writing under oath or equivalent affirmation, to a court of competent jurisdiction." 18 U.S.C. § 3122(a)(1). Such an application need only contain: "(1) the identity of the attorney for the Government or the State law enforcement or investigative officer making the application and the identity of the law enforcement agency conducting the investigation; and (2) certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency." 18 U.S.C. § 3122(b). Upon a finding that this burden has been met, the court "shall

enter" such an order. Id. This minimal requirement seems to reflect the premise that pen registers were once unable to record the contents of any communication, and instead could record only call processing information, which, pursuant to Smith v. Maryland, was deemed to encompass a less important privacy interest. 442 U.S. at 741.

1. The Original Pen/Trap Statute

Although the authorization procedure has not changed since the Pen/Trap Statute was initially enacted, the relevant definitions have. The original Pen/Trap Statute defined a pen register as follows: "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line." ECPA § 301, enacting 18 U.S.C. § 3126(3), recodified at 18 U.S.C. § 3127(3) by P.L. 100-690, § 7092 (1988). On its face, this statute authorized the recording of all digits dialed. That it was possible for the content of communications to be included in that definition was likely not contemplated. See H.R. Rep. No. 99-647, at 78 (1986) (A pen register "does not [record] the contents of a communication, rather it records the numbers dialed."); S. Rep. 99-541, at *10 (1986) ("[Pen registers] capture no part of an actual telephone conversation, but merely the electronic switching signals that connect two telephones."); see also People v. Bialostok, 610 N.E.2d 374, 378 (N.Y. 1993) ("The traditional pen register was, to a large extent, self-regulating. Neither through police misconduct nor through inadvertence could it reveal to anyone any information in which the telephone user had a legitimate expectation of privacy."); In re U.S. (S.D. Tex.) at 821.

2. CALEA

In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"), which amended the Pen/Trap Statute. The purpose of CALEA was "to make clear a telecommunications carrier's duty to cooperate in the interception of communications for Law Enforcement purposes, and for other purposes." 141 Cong. Rec. H113-05 (Oct. 25, 1994). CALEA was intended "to preserve the Government's ability, pursuant to court order or other lawful authorization, to intercept communications involving advanced technologies such as digital or wireless transmission modes, or features and services such as call forwarding, speed dialing and conference calling, while protecting the privacy of communications and without impeding the introduction of new technologies, features and services." H.R. Rep. 103-827(I), 103d Cong., 2d Sess. at 9 (Oct. 4, 1994).

CALEA added a new provision to the Pen/Trap Statute that imposed a limitation on the Government's use of a pen register. The new provision mandated that "[a] Government agency authorized to install and use a pen register . . . shall use technology reasonably available to it that restricts the recording or decoding . . . to the dialing and signaling information utilized in call processing." 18 U.S.C. § 3121(c) (1994) (emphasis added).

After CALEA was enacted, the Government argued that a pen register order authorized a law enforcement agency to receive all PCTDD, subject only to CALEA's requirement that the agency use "technology reasonably available to it" to avoid processing digits that are content. 18 U.S.C. § 3121(c) (1994). In 2000, the D.C. Circuit noted in dicta that "[n]o court has yet considered that contention . . . and it may be that a Title III [wiretap] warrant is required to receive all post-cut-

through digits." U.S. Telecom, 227 F.3d at 462.[3]

3. The USA PATRIOT Act

After September 11, 2001, Congress passed the USA Patriot Act, which amended the Pen/Trap Statute to read as it does today. See Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001 ("the "Patriot Act"), Pub. L. No. 107-56, 115 Stat. 272. The Patriot Act modernized the Pen/Trap Statute to accommodate wireless and internet-based technology. Instead of "a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line," the definition of a pen register now reads: "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 . . . ." Patriot Act § 216 (amending 18 U.S.C. § 3127(3)). Moreover, the Patriot Act added a clause at the end of the definition which reads, "provided, however, that such information shall not include the contents of any communication . . . ." Id. (emphasis added).

The § 3121(c) limitation provision was also amended by the Patriot Act. The limitation now commands the Government to use "technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing, routing, addressing, and signaling

---

[3] This case was an appeal of a 1999 Federal Communications Commission ("FCC") ruling on CALEA's proposed technical standards (referred to as the "J-Standard"), finding among other things that the J-Standard must include the capability for "post-cut-through dialed digit extraction." In re U.S. (S.D. Tex.), 441 F. Supp. 2d at 820 (citing In the Matter of Communications Assistance for Law Enforcement Act, 1999 WL 674884, 14 F.C.C.R 16794 (1999).

information utilized in the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c) (emphasis added). Thus, as the statute now reads, there are two specific proscriptions against the recording of communications content. Moreover, the Patriot Act amendments explicitly incorporated the Title III definition of "contents," as described below. See 18 U.S.C. § 3127(a) (referencing 18 U.S.C. § 2510).

4. Title III

Unlike pen registers, Government-conducted wiretaps are governed by Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III"), as amended, 18 U.S.C. § 2510 et seq. Federal wiretaps implicate the Fourth Amendment; thus, a showing of probable cause is required for their installation. See Katz v. United States, 389 U.S. 347, 353-54 (1967). In addition, Title III sets out specific procedures and requirements for their use.

Title III requires that the Government obtain a court order (known as a "Wiretap Order") before its agents are permitted to "intercept" the "content" of an individual's "wire communications" with an "electronic, mechanical or other device." 18 U.S.C. § 2510 (definitions); 18 U.S.C. § 2511 (generally prohibiting interception); 18 U.S.C.A. § 2518 (describing application and court order for interception). The term "contents" of communication is defined as "includ[ing] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8).

A federal court may issue a Wiretap Order "if it determines, on the basis of the facts submitted by the applicant, that there is probable cause to believe (1) that an individual was committing, had committed, or is about to commit a crime; (2) that communications concerning that crime will be obtained through the wiretap; and (3) that the premises to be wiretapped were being used for criminal

purposes or are about to be used or owned by the target of the wiretap." United States v. Diaz, 176 F.3d 52, 110 (2d Cir. 1999) (citing 18 U.S.C. § 2518(1)(b)(i), (3)(a), (b), (d)). The applicable standard for probable cause is the same as the standard for a search warrant, which is established if the "totality-of-the-circumstances" indicates a probability of criminal activity. Id. (citations omitted). The applicant must also demonstrate the inadequacy of other investigative procedures. 18 U.S.C. § 2518(1).

Title III also contains an exclusionary rule that prohibits the Government from making use of the contents of a communication obtained in violation of Title III. 18 U.S.C. § 2515. Under the Government's minimization theory, any content obtained with a pen register is suppressible subject to Title III's exclusionary rule.

B. Statutory Interpretation

To determine the parameters of the Pen/Trap Statute, statutory interpretation is necessary. As in all statutory construction cases, the language of the statute is the starting point. Barnhart v. Sigmon Coal Co., Inc., 534 U.S. 438, 450 (2002). Legislative history and canons of statutory interpretation will also be utilized.[4]

1. Statutory Text

"The first step [in statutory construction cases] is to determine whether the language at issue has a plain and unambiguous meaning with regard to the particular dispute in the case. The inquiry

---

[4] Ordinarily a court will seek to interpret an ambiguous statute using established canons of statutory interpretation before resorting to legislative history. See, e.g., U.S. v. Boccagna, 450 F.3d 107, 114 (2d Cir. 2006) (citing Daniel v. Am. Bd. of Emergency Medicine, 428 F.3d 408, 423 (2d Cir. 2005) ("Only if we conclude that statutory language is ambiguous "do we resort . . . to canons of construction and, if the meaning [still] remains ambiguous, to legislative history.")). Canons of construction will be utilized, but for the sake of organization, I will first look to legislative history.

ceases if the statutory language is unambiguous and the statutory scheme is coherent and consistent." Id. (internal citations and quotation marks omitted).

There are two pertinent definitions to be examined. A pen register is defined by statute as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." 18 U.S.C. § 3127 (emphasis added). On its own, this provision appears unambiguous in its proscription against the collection of any content.

Section 3121(c) of the Pen/Trap Statute clouds this lucidity. Section 3121(c) is labeled a "limitation" to the above definition. It reads: "A government agency authorized to install and use a pen register . . . 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 to not include the contents of any wire or electronic communications." 18 U.S.C. § 3121(c) (emphasis added). It is undisputed that PCTDD can and often do include such content. SeeU.S. Telecom, 227 F.3d at 462; In re U.S. (S.D. Tex.), 441 F. Supp. 2d at 823. The Government has successfully demonstrated that no technology exists which would enable the Government to separate all PCTDD containing content from that not containing content while giving the Government access only to the former.[5]

Read together, these provisions are ambiguous. The definition provision unconditionally

---

[5] On December 13, 2006, this Court held an ex parte hearing in which the Government convinced the Court that no technology is reasonably available which is capable of sorting PCTDD containing content from those not containing content without giving the Government access to content.

forbids the collection of content, while the limitation provision seems to mandate only the use of "reasonably available technology" in order to prevent its collection. Read together, a contradiction arises: if no content can be collected, then what is the purpose of the reasonably available technology requirement?

2. Legislative History

Because the statute in question is ambiguous, a court may also look to legislative history to determine the intent of Congress.[6] Auburn Hous. Auth. v. Martinez, 277 F.3d 138, 144 (2d Cir. 2002). Both the Government and *amicus* refer the Court to a variety of isolated passages in support of their respective interpretations of the statute.

The Government argues that legislative history from both 1994 and 2001 supports its minimization theory. Their position is that the 1994 "technology reasonably available" provision establishes only a content minimization requirement and that the 2001 Patriot Act amendments do not alter that scheme. The Government thus contends that the phrase was "intended to permit access to dialed-digit content incidental to the recording of dialed-digit non-content, provided that the [G]overnment keeps the recording of such content to a practical minimum by means of 'technology reasonably available' to it." (Gov. Mem. of Law 26.) In support of this argument, they offer the following statement by CALEA bill sponsor Senator Patrick Leahy:

"[This subsection] requires government agencies installing and using pen register

---

[6] Because In re U.S. (M.D. Fla.) found the "plain" interpretation of the Pen/Trap Statute to "flatly prohibit[] the interception of communication content by pen registers," it did not examine legislative history. No. 06-MJ-1130, at 5. In re U.S. (S.D. Tex.) examined the legislative history and found that it supported its view that the statute unambiguously forbids the collection of any PCTDD that may contain content. 441 F. Supp. 2d at 824-26 (finding the "minimize content, but allow all non-content" reading of the statute to be "admittedly one possible way to read § 3121(c)," but ultimately finding it implausible).

> devices to use, when reasonably available, technology that restricts the information captured by such device to the dialling [*sic*] or signaling information necessary to direct or process a call, excluding any further communications conducted through the use of dialled [*sic*] digits that would otherwise be captured."

140 Cong. Rec. S11045-05, *S11059. In addition, the Government cites the 1994 Senate and House reports, which contain the following sentence: "the bill requires law enforcement to use reasonably available technology to minimize information obtained through pen registers." S. Rep. 103-402, at 18; H.R. Rep. 103-827(I) at 17.

Viewed in isolation, particularly the word "minimize," these statements do appear to support the Government's theory. Yet, adjacent comments by Senator Leahy point to a different conclusion. Senator Leahy's 1994 statements repeatedly describe the bill as one that stringently protects privacy: "The bill []protects privacy by requiring telecommunications systems to protect communications not authorized to be intercepted and by restricting the ability of law enforcement to use pen register devices for tracking purposes or for obtaining transactional information." 140 Cong. Rec. 11055, at 11056.

The priority of privacy is further evidenced in Senator Leahy's statements concerning the 2001 Patriot Act amendments. Rather than endorsing the Government's view, Senator Leahy's statements express concern that courts will erroneously grant the Government access to content with only pen register authorization. Senator Leahy specifically states that he is "concerned about the FBI and Justice Department's insistence over the past few years that the pen/trap devices statutes be updated with broad, undefined terms that continue to flame concerns that these laws will be used to intercept private communications content." 147 Cong. Rec. S10990, *S11000 (Oct. 25, 2001). Although he worries that courts have been left with "little or no guidance of what is covered by

'addressing' or 'routing,'" Senator Leahy finds it an "improvement" that "the Administration agreed that the definition should expressly exclude the use of pen/trap devices to intercept 'content,' which is broadly defined in 18 U.S.C. 2110(8)." Id.

Perhaps most persuasive of all, Senator Leahy recognized the unconstitutionality of collecting content with a pen register: "When I added the direction on use of reasonably available technology . . . to the pen register statute as part of [CALEA] in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere relevance standard." Id.; In re U.S. (S.D. Tex.), 441 F. Supp. 2d at 821 (quoting same). Senator Leahy's recognition that collection of content is unconstitutional is important. We must assume Congress would not want to enact unconstitutional provisions, Clark v. Martinez, 543 U.S. 371, 381-382 (2005), and there is no indication of Congressional intent to the contrary, see supra Part II.B.3.

This Court is not persuaded by the Government's argument that Senator Leahy's statements demonstrate Congress' intent to allow incidental access to content. Although it is notoriously difficult to surmise intent from legislative history, see, e.g., Frank G. v. Board of Educ. of Hyde Park, 459 F.3d 356, 374 (2d Cir. 2006) (quoting Piper v. Chris-Craft Indus. Inc., 430 U.S. 1, 26 (1977)) ("[r]eliance on legislative history in divining the intent of Congress is, as has often been observed, a step to be taken cautiously"), when examined in totality, the legislative history supports the denial of the instant application.

3. Canons of Statutory Interpretation

Legislative history fails to fully clarify the ambiguity created by the text of the Pen/Trap Statute. Where the terms of a statute are ambiguous, traditional canons of statutory construction should also be relied upon to resolve the ambiguity. Frank G. v. Board of Educ. of Hyde Park, 459

F.3d at 370 (citing United States v. Peterson, 394 F.3d 98, 105 (2d Cir. 2005)). Submissions by Government and *amicus* urge the Court to apply a variety of such canons.

The Government exhorts the application of four canons of construction: (1) the whole act rule; (2) the two acts rule; (3) the rule against implied repeals; and (4) the rule against superfluity. The whole act rule requires that a statutory provision be "interpret[ed] . . . in a way that renders it consistent with the tenor and structure of the whole act or statutory scheme of which it is a part." United States v. Pacheco, 225 F.3d 148, 154 (2d Cir. 2000) (citations and quotation marks omitted). The two acts rule applies similarly. It states: "The courts are not at liberty to pick and choose among congressional enactments, and when two statutes are capable of co-existence, it is the duty of the courts, absent a clearly expressed congressional intention to the contrary, to regard each as effective. [Thus,] '[w]hen there are two acts upon the same subject, the rule is to give effect to both if possible . . . .'" Morton v. Mancari, 417 U.S. 535, 551 (1974) (quoting United States v. Borden Co., 308 U.S. 188, 198 (1939)).

Permitting the Government to access the content of telephone communications without a Wiretap Order is not consistent with the statutory scheme of the Pen/Trap Statute or Title III. Rather, read together, the acts distinguish sharply between the content of communications and non-content call processing information. Moreover, that Title III exists is evidence of Congress' intent to protect the content of telephone communications from Government intrusion. "The legislative purpose [behind Title III] is plain: 'The protection of privacy was an overriding congressional concern.'" United States v. Amanuel, 418 F. Supp. 2d 244, 248 n. 4 (W.D.N.Y. 2005) (citing Gelbard v. United States, 408 U.S. 41, 46 (1972). The Government's arguments to the contrary are unavailing.

The rule against implied repeals is likewise unconvincing. The Supreme Court has stated that "[r]epeals by implication are not favored." Morton v. Mancari, 417 U.S. 535, 549 (1976). Yet, there is no evidence that Congress intended to give the Government access to the content of communications when it enacted the "technology reasonably available" provision in 1994. Thus, the addition of the "shall not include the contents" phrase was not an implied repeal of anything.

The rule against superfluities does give me pause. This rule provides: "A statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." Duncan v. Walker, 533 U.S. 167, 174 (2001). The phrase counseling the Government to use "technology reasonably available . . . so as not to include the contents of . . . communications," 18 U.S.C. § 3121(c), is superfluous if the ban on content acquisition is absolute. These conflicting provisions are the cornerstone of the ambiguity at issue in the instant application. However, while the rule against superfluities is a guiding factor to be considered, it is not dispositive. On the contrary, it must be considered in light of all the other tools of interpretation and, as such, it is not overly persuasive. The rule against superfluities describes the instant ambiguity, it does not resolve it.

Despite the Government's insistence to the contrary, the most applicable canon of statutory construction is that of constitutional avoidance. This longstanding canon instructs courts to "avoid making unnecessary constitutional pronouncements if a reasonable interpretation of the statute would obviate the constitutional difficulties." Lo Duca v. United States, 93 F.3d 1100, 1110 (2d Cir. 1996) ("[W]e are instructed to construe federal statutes to avoid constitutional infirmity . . . ."); see also Seminole Tribe of Florida v. Florida, 517 U.S. 44, 182 (1996) ("Our longstanding practice is to read ambiguous statutes to avoid constitutional infirmity."); Edward J. DeBartolo Corp. v. Florida Gulf

Coast Building & Constr. Trades Council, 485 U.S. 568, 575 (1988) ("'every reasonable construction must be resorted to, in order to save a statute from unconstitutionality'") (quoting Hooper v. California, 155 U.S. 648, 657 (1895)).

The doctrine of constitutional avoidance "is a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." Clark v. Martinez, 543 U.S. 371, 381-82 (2005) (citations omitted). This canon is "a means of giving effect to congressional intent, not of subverting it." Id. In the instant case, the doctrine is particularly compelling. The Supreme Court has long held that the Fourth Amendment bars the Government from obtaining the contents of communication without a showing of probable cause. Katz, 389 U.S. 347. Because the Government's reading of the Pen/Trap Statute would violate this long-standing principle, the instant application must be denied.

4. The Fourth Amendment

The Government's interpretation of the Pen/Trap Statute impermissibly strains statutory language and legislative history, but more importantly, it creates serious constitutional problems. No federal statute, however interpreted, can trump the Fourth Amendment.

The Fourth Amendment prohibits unreasonable searches and seizures. Thus, before performing a search or seizure, the Government generally must demonstrate probable cause and obtain a search warrant. See, e.g., Cassidy v. Chertoff, 471 F.3d 67, 74 (2d Cir. 2006). In order to trigger the protections of the Fourth Amendment, a person must manifest a subjective expectation of privacy in the target of the Government's search that society accepts as objectively reasonable. California v. Greenwood, 486 U.S. 35, 39 (1988) (citations omitted).

It is well-settled that the protections of the Fourth Amendment apply to electronic eavesdropping of private conversations. See Berger v. New York, 388 U.S. 41, 57-60 (1967) (finding New York's electronic eavesdropping statute facially unconstitutional due to its lack of adequate Fourth Amendment safeguards); Katz, 389 U.S. at 353 (finding a reasonable expectation of privacy in the content of telephone calls made from a closed phone booth). On the other hand, pen registers fall outside the province of the Fourth Amendment because phone users do not have a reasonable expectation of privacy in the numbers they dial to connect a phone call. Smith, 442 U.S. at 734-44. The Government argues that this Court should extend the reasoning of Smith.

1. Reasonable Expectation of Privacy

"In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is Katz v. United States, 389 U.S. 347 (1967)." Smith, 442 U.S. at 739. Under Katz, the Supreme Court has "uniformly [] held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' 'reasonable,' or a 'legitimate expectation of privacy that has been invaded by government action." Id. at 740 (citations omitted). In the instant application, the Government argues that individuals have no such reasonable expectation of privacy in their PCTDD and, therefore, the Fourth Amendment does not bar their incidental access.

Smith provides the backbone of the Government's argument. In holding that Government use of a pen register did not invoke the protections of the Fourth Amendment, the Supreme Court distinguished its opposite holding in Katz: "[A] pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications." Smith v. Maryland, 442 U.S. at 741. The Court continued: "These devices . . . disclose only the telephone

numbers that have been dialed – a means of establishing communication. Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." Id. (quoting United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

While individuals may not have a reasonable expectation of privacy in the numbers that they dial to connect a phone call, the content they communicate over a phone line in the form of PCTDD is different. Technology has transformed the way Americans use phone lines. Now, instead of a human operator, individuals are asked to relay information to a machine by way of PCTDD in order to process requests and obtain information. When this communication includes content, it is the functional equivalent of voice communication and is protected by Katz and its progeny as such. Moreover, the information that is often transmitted via PCTDD is often sensitive and personal. Bank account numbers, pin numbers and passwords, prescription identification numbers, social security numbers, credit card numbers, and so on, all encompass the kind of information that an individual wants and reasonably expects to be kept private.

2. Assumption of Risk

The Government also argues that there is no reasonable expectation of privacy in PCTDD because the information is voluntarily conveyed to a third party, the telephone company. This assumption of risk argument has been adopted by the Supreme Court in a variety of contexts. See, e.g., United States v. Miller, 425 U.S. 435, 442-44 (1976) (no legitimate expectation of privacy in bank records); Couch v. United States, 409 U.S. 322, 335-36 (1973) (no legitimate expectation of privacy in financial records submitted to taxpayer's accountant); United States v. White, 401 U.S. 745, 752 (1971) (no legitimate expectation of privacy in taped conversations to third party). It was

also a component of the majority's reasoning in Smith.

"In Smith, the Court noted that all telephone users realize that they must 'convey' telephone numbers to the telephone company so that their calls can be completed, that records of their calls are kept for billing purposes, and that such records can be used to detect fraud and harassment and thus [are] potentially available to law enforcement and other investigators." Beckwith v. Erie County Water Authority, 413 F. Supp. 2d 214, 223 (W.D.N.Y. 2006) (citing Smith, 442 U.S. at 742). When the petitioner in Smith "used his phone, [he] voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed." Smith, 442 U.S. at 744. Under this logic, even if a person harbored some subjective expectation that the phone numbers he dialed would remain private, this expectation is not "one that society is prepared to recognize as reasonable." Katz, 389 U.S. at 361.

Miller also addresses the Fourth Amendment and the risk assumed when information is conveyed to an institutional third party. 425 U.S. 435. In Miller, the Supreme Court rejected a defendant's challenge to the use of grand jury subpoenas to obtain banking records from his bank, concluding that no legitimate expectation of privacy existed in the contents of the bank records. Id. at 442. An individual "takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government." Id. at 443. The Court reasoned: "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business." Id. at 442 (emphasis added).

The Government argues for an extension of the logic behind these cases, but ignores the

important distinctions between them and the instant application for PCTDD. Unlike the dialed digits discussed in Smith and the bank records addressed in Miller, PCTDD are not kept in the "ordinary course of business," see Smith at 744 and Miller at 442, nor do they appear on a user's monthly bill. The Government argues that these distinguishing facts are inconsequential and that by dialing digits into a phone, a telephone user has "assumed the risk" that the telephone company, capable of accessing all digits dialed, will do just that and relinquish the information to the Government.

The Sixth Circuit recently spoke to this issue in the context of email content and held that: "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." Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007). However, "[t]he same does not necessarily apply . . . to an intermediary that merely has the ability to access the information sought by the government." Id. Indeed, the "assumption of risk" so trumpeted by the Government, is far from absolute. "Otherwise 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." Id. These consequences of an extension of the assumption of risk doctrine are not acceptable under the Fourth Amendment. A caller "'is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,' and therefore cannot be said to have forfeited his privacy right in the conversation." Warshak, 490 U.S. at 470 (citing Katz, 389 U.S. at 352). The same can be said for PCTDD that contain content.

Warshak holds that only when an institution "actually relies on and utilizes [] access [to

information] in the normal course of business" does the supplier of that information forfeit his reasonable expectation of privacy. Id. 476. By this standard, telephone users have a reasonable expectation of privacy in their PCTDD. However, even disregarding Warshak, the Government's argument fails. As reflected in the statutory analysis, the most important distinction is between communications content and non-content, not that which defines the ordinary course of business.

C. Level of Intrusion

"Courts judge the reasonableness of a search 'by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate governmental interests.'" Cassidy v. Chertoff, 471 U.S. at 652-53 (citing Vernonia Sch. Dist. v. Acton, 515 U.S. 646, 652 (1995) (internal quotation marks omitted)). Thus, the level of intrusion is a factor to be considered when addressing constitutionality under the Fourth Amendment.

"[S]uspicionless searches . . . are highly disfavored since they dispense with the traditional rule that a search, if it is to be deemed reasonable, must be either supported by a warrant based on probable cause, or justified by evidence establishing individualized suspicion of criminal misconduct." United States v. Amerson, 483 F.3d 73, 77-78 (2d Cir. 2007) (citing City of Indianapolis v. Edmond, 531 U.S. 32, 37 (2000) ("A search or seizure is ordinarily unreasonable in the absence of individualized suspicion of wrongdoing.")). Government installed pen registers were held to be permissible warrantless searches in Smith because, by their nature (their inability to collect content), they were minimally intrusive. Today's pen registers, as advocated by the Government in the instant application, have the potential to be much more intrusive than when their constitutionality was first examined. The evolution of technology and the potential degree of intrusion changes the analysis.

D. Pager Clones and Hybrid Communications

The case of digital-display pagers supports this conclusion. Such pagers, popular in the 1990s, are devices for personal use that are capable of receiving numeric transmissions. "[T]he basic intended function of these pagers was to receive telephone numbers that were then to be called by the pager custodian" in return. Brown v. Waddell, 50 F.3d 285, 287 (4th Cir. 1995). However, "they could actually receive and display combinations of up to 24 (or 25) numbers and dashes in a single transmission" and were often used to communicate substantive messages. Id. at 287-92. Thus, like PCTDD, pagers may contain hybrid communications of both content and non-content.

In Brown, the Fourth Circuit examined the Government's use of pager clones pursuant to the Pen/Trap Statute. The clones "allowed [the Government] to receive any numeric messages sent to the defendant's pagers at the same time that they were received and displayed on her pagers." Id. at 287. The Brown Court held that this technique "cannot be considered the use of a 'pen register' within the meaning of the [Pen/Trap Statute]." Id. at 294.[7]

Important to the Court's reasoning was that the information gathered "surely would have to be limited to raw telephone numbers to retain pen register status." Id. at 293. The Court stated: "That a digital display pager has the capacity to receive . . . coded substantive messages . . . is what makes the interception subject to the authorization requirements of [Title III]." Id. at 294 n. 11. Case law in the Second Circuit demonstrates agreement with the proposition that a showing of at least probable cause is required for pager clone authorization. See, e.g., United States v. Gambino,

---

[7] The Second Circuit has not had occasion to address the issue in Brown, but at least one court in the Southern District of New York treated the case positively in dicta. United States v. Reyes, 922 F. Supp. 818, 837 n. 20 (S.D.N.Y. 1996).

No. 04 CR 687, 1995 WL 453318, at *3 (S.D.N.Y. Aug. 1, 1995); United States v. Persico, No. 92 CR 351, 1994 WL 36367, at * 14 (E.D.N.Y. Jan. 28, 1994).

5. Congress' Role in Updating Statutes as Technology Evolves

Courts have long struggled with issues concerning the application of the Fourth Amendment to new technologies. Here, modern technology in the form of automated telephone systems have changed the collection capabilities of pen registers. However, the change in technology does not alter the mandates of the Fourth Amendment. The content of private communications remains protected. To read the Constitution more narrowly is to ignore the role that PCTDD and automated telephone systems have come to play in private communication. See similarly, Katz, 389 US at 352.

I am sympathetic to the Government's pleas of necessity. That there is no technology available that can sort content from non-content is unfortunate, but it is not for this Court to fashion a solution. Rather, this is an issue for Congress to address, particularly in light of sophisticated criminals who will soon be wise, if they are not already, to this investigative loophole. Despite the investigative benefit which would come from access to all PCTDD, the Government cannot bootstrap the content of communications, protected by the Fourth Amendment, into the grasp of a device authorized only to collect call-identifying information. Until the Government can separate PCTDD that do not contain content from those that do, pen register authorization is insufficient for the Government to obtain any PCTDD.

III. CONCLUSION

Because the Government's request for access to all post-cut-through dialed digits is not clearly authorized by the Pen/Trap Statute, and because granting such a request would violate the Fourth Amendment, the Government's application is denied.

SO ORDERED.

Dated: September 18, 2007
Brooklyn, New York

JOAN M. AZRACK
UNITED STATES MAGISTRATE JUDGE