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)

GOVERNMENT'S MEMORANDUM OF LAW IN SUPPORT
OF ITS REQUESTS FOR AUTHORIZATION TO ACQUIRE
POST-CUT-THROUGH DIALED DIGITS VIA PEN REGISTERS

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

JED DAVIS
SCOTT KLUGMAN
Assistant U.S. Attorneys
(Of Counsel)

TABLE OF CONTENTS

APPENDIX

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)

GOVERNMENT'S MEMORANDUM OF LAW IN SUPPORT OF ITS REQUESTS FOR AUTHORIZATION TO ACQUIRE POST-CUT-THROUGH DIALED DIGITS VIA PEN REGISTERS

PRELIMINARY STATEMENT

The government respectfully submits this memorandum of law in 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 a pen register to record post-cut-through dialed digits ("PCTDD") dialed by a specified telephone (the "subject telephone").

PCTDD are digits that a user dials after the initial call setup is completed, or "cut-through" from an originating telephone switch to the next switch in the sequence needed to connect a call.[1] Some PCTDD consists of digits that are

[1] A switch is a sophisticated computer capable of connecting numerous calls at any given time. In the current telephone system, a call may pass through a number of different switches, any of which may be owned by a carrier or entity different than the others. The originating switch may be a computer owned and controlled by the carrier serving the telephone (e.g., Verizon) or it may be a "private branch

unrelated to the content of the call, that is, digits that are unrelated to "the substance, purport, or meaning" of the call. See 18 U.S.C. §§ 2510(8), 3127(1). These "non-content PCTDD" typically consist of digits that are necessary to route and address a call and include other telephone numbers and access codes that a user enters after the initial call setup. For example, and as is often important in criminal investigations, the access codes and telephone numbers that a user enters after his call is cut-through to a calling card service constitute non-content PCTDD. Other forms of PCTDD, however, may convey communicative content ("PCTDD content"). For example, a user may generate PCTDD content, after he is cut-through to his bank's telephone system and enters his account number.

Since 1994 and continuing under amendments to the Pen/Trap Statute that were enacted in 2001, Congress has authorized the government to use a pen register to access content, provided that if there is "technology reasonably available to it that restricts" to non-content the information that the pen register accesses, the government must use that technology. See 18 U.S.C. § 3121(c) (1994 & 2001). When no such technology is "reasonably available," however, Congress has authorized the government to obtain content incidental to a pen

---

exchange" ("PBX") that is controlled by the entity (e.g., the U.S. Attorney's Office or a law firm) from whose internal telephone system a call originates.

register's acquisition of non-content ("incidental access to content"). Although the Pen/Trap Statute authorizes such incidental access, the government is prohibited from using both the content in issue, as well as it fruits, unless that content was acquired in accordance with Title III of the Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351 ("Title III"). See 18 U.S.C. § 2515.

The instant briefing is necessitated by a recent out-of district decision that construes 18 U.S.C. § 3121(c) together with 18 U.S.C. § 3127(c), which defines a "pen register" for the purposes of the Pen/Trap Statute. Simultaneous with the 2001 amendments to 18 U.S.C. § 3121(c), Congress added language at the end of § 3127(c), so that it now states that the information that a pen register acquires "shall not include the contents of any communication."

In a case of first impression, a magistrate judge in Houston has held that notwithstanding § 3121(c)'s "technology reasonably available" clause, the amendment to 18 U.S.C. § 3127(3) prohibits all incidental access to content, even when there is no technology reasonably available that can avoid it. See In the Matter of the Application of the United States of

America . . ., 441 F. Supp.2d 816 (S.D. Tx. 2006) (hereafter the "Houston Decision").[2]

The Houston Decision fundamentally misconstrues 18 U.S.C. §§ 3121(c) and 3127(3). The discussion below sets forth the statutes in issue (Point I), followed by a discussion of the cardinal rules of statutory construction that apply (Point II). Point III demonstrates how those rules and alternatively, those rules as resolved by legislative history, require that 18 U.S.C. § 3121(c) and 18 U.S.C. § 3127(3) be read in pari materia to permit a pen register incidental access to content, so long as (a) no technology is reasonably available to avoid it, and (b) pursuant to 18 U.S.C. § 2515, the government makes neither direct nor derivative use of content thereby obtained. Based on the prior points, Point IV summarizes how the holding of the Houston Decision misconstrues the text and disregards both the

---

[2] Prior to the Houston Decision, two courts in dicta had questioned whether the government could ever permissibly acquire PCTDD absent an eavesdropping warrant. As reflects the fact that in neither case was the issue necessary to decide, both decisions nowhere mention, let alone evaluate, 18 U.S.C. § 3121(c). See FCC v. United States v. United States Telecommunications Ass'n, 227 F.3d 450, 462 (D.C. Cir. 2000) ("[I]t may be that a Title III warrant is required to receive all post-cut-through digits) (under Communications Assistance To Law Enforcement Act, FCC required to reconsider whether service providers must develop capability to acquire PCTDD in response to court orders); In Re Application Of The United States On [xxxx] Internet Service Provider/User Name [xxxx@xxx.com], 396 F. Supp.2d 45, 48 (D. Mass 2005) (where government sought a pen/trap on an email account, not a phone, expressing skepticism that "anyone [would] doubt" that amended 18 U.S.C. § 3127(3) prohibits a pen register from ever accessing PCTDD content).

controlling canons and legislative history, all of which result in that decision stopping short of answering the question that as a matter of law it was required to have answered in order to determine whether the government was entitled incidentally to access PCTDD: whether there is technology reasonably available to the government that can reliably separate PCTDD content from PCTDD non-content. The government has previously furnished evidence ex parte and under seal that we respectfully submit demonstrates that in fact, no such technology is reasonably available to the government. Because it is not, the Pen/Trap Statute permits the subject pen registers to access PCTDD content incidental to acquiring PCTDD non-content.

I. Pertinent Statutory Provisions

A. Title III (1968)

In enacting Title III, Congress established a new statutory framework of standards, limitations, and procedure the government must follow in order to be authorized to intercept and use the content of (among other things) wire communications. Under Title III, all such interceptions must (among other things) be either consensually authorized, or judicially authorized upon a showing by the government of probable cause to believe that the instrument to be monitored has been and will continue to be used to commit crimes, that there is accordingly probable cause to believe eavesdropping will reveal evidence of such crimes and

that less intrusive means of investigation have failed or are reasonably likely to fail. See 18 U.S.C. § 2518(3)(a)-(d).

Since Title III's inception, 18 U.S.C. § 2515 has contained the following comprehensive prohibition on use by the government of the contents of wire communications in the event they are acquired without Title III's requisites for interception having been satisfied:

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

18 U.S.C. § 2515 (West. 2006).

Accordingly, 18 U.S.C. § 2515 precludes the government from making direct or derivative use of the contents of intercepted wire communications except as authorized by Title III (and/or the national security statutes that it incorporates by reference). By the same token, 18 U.S.C. § 2515 vests persons intercepted in violation of Title III with the right to suppress any interceptions offered against them.[3]

---

[3] By contrast, since inception in 1986, there has bee no mandate to suppress processing information obtained pursuant to the Pen/Trap Statute if its requirements are not met. United States v. Thompson, 936 F.2d 1249, 1249-50 (11th Cir. 1991); accord United States v. Fregoso, 60 F.3d 1314, 1320-21 (8th Cir. 1995)

B. The Original Pen/Trap Statute (1986)

The Pen/Trap Statute was originally enacted in 1986 as part of the Electronic Communication Privacy Act, Pub. L. No. 99-508 ("ECPA"). As it has since inception, the Pen/Trap Statute authorizes "attorney[s] for the government" to apply for an order authorizing or approving "the installation and use of a pen register or a trap and trace device" ECPA § 301 (enacting 18 U.S.C. § 3122(a)). Upon a finding that such an attorney for the government "has certified that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation, a court "shall enter" such an order. Id. (enacting 18 U.S.C. § 3123(a)(1)) (emphasis added).

From 1986 until the 2001 amendments (see below), the Pen/Trap Statute defined a pen register as follows:

> . . . Definitions for chapter
>
> As used in this chapter . . .
>
> (3) The term "pen register" means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached...

ECPA § 301, enacting 18 U.S.C. § 3126(3), recodified at 18 U.S.C. § 3127(3) (emphasis added) by P.L. 100-690, § 7092 (1988).

C. Original 18 U.S.C. § 3121(c) (1994)

In 1994, Congress amended the Pen/Trap Statute, pursuant to the Communications Assistance for Law Enforcement

Act, P.L. 103-414 (1994) ("CALEA"). CALEA added a new provision, codified at 18 U.S.C. § 3121(c), that imposed a limitation on the government's use of a pen register, as follows:

> Limitation – A Government agency authorized to install and use a pen register under this chapter or under State law shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

CALEA, Pub. L. No. 103-414, § 207 (1994)(emphasis added).

D. The 2001 Amendments To §§ 3121(c) and 3127(3)

In 2001, following the 9/11 terrorist attacks, Congress enacted the Patriot Act.[4] The Patriot Act revised the electronic surveillance laws in a number of respects, including but not limited to the Pen/Trap Statute. Among other things, the Patriot Act modernized the Pen/Trap Statute to accommodate wireless and Internet-based technology, neither of which had been specifically addressed by ECPA in 1986 or by CALEA's 1994 amendments to the Pen/Trap Statute. In addition, the Patriot Act also altered the definition of "pen register" in pertinent part as follows:

> . . . Definitions for chapter
>
> As used in this chapter . . .
>
> (3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted

[4] "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," Pub. L. No. 107-56, 115 Stat. 272 (2001).

> 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....

Patriot Act § 216 (amending 18 U.S.C. § 3127(3)) (emphasis added). At the same Congress amended the "limitation" set forth at 18 U.S.C. § 3121(c), to read:

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

Patriot Act § 216 (amending 18 U.S.C. § 3121(c)) (emphasis added).[5]

[5] By adding the terms "routing [and] addressing information," to both § 3121(c) and § 3127, the Patriot Act made clear, among other things, that Pen/Trap Statute's not only governs telephonic data encompassed by "dialing and signaling information necessary to call processing" (former § 3121(c)) and "numbers dialed or otherwise transmitted" (former § 3127(3)), but also extends to non-telephonic forms of communication, such as email messages sent via Internet. For example, by adding the "routing [and] addressing information," the amendments establish the Pen/Trap Statute's jurisdiction over devices that detect what Internet Protocol ("IP") address is assigned to a user sending email over the Internet, since Internet service providers rely on IP addresses to route outgoing email and to establish a return address for replies.

II. Governing Principles Of Statutory Construction

The starting and sometimes the ending point for construction of a statute is it text. If the meaning of the text is plain, the statute must be construed according to the text's unambiguous terms and no further analysis is warranted. Rubin v. United States, 449 U.S. 424, 430 (1981). If, however, the words of the statute are ambiguous, a court must attempt to interpret that text with no extrinsic aids, except canons of statutory construction. Daniel v. American Board of Emergency Medicine, 428 F.3d 408, 423 (2d Cir. 2005). If canons alone fail to cure the ambiguity, the Court must consult legislative history to ascertain if legislative history alone or in combination with canons dispels it. Id.

In this case, the applicable canons and related rules with respect to legislative history are as follows:

A. A statutory provision must 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) (citation omitted) (the "whole act" rule); and as a corollary,

B. "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)), sometimes referred to as the "rule against superfluities";[6]

[6] See 2A N. Singer Statutes and Statutory Construction § 46.06, pp. 181-86 (rev. 6th ed. 2000).

C. "Repeals by implication are not favored." Morton v. Mancari, 417 U.S. 535, 549 (1976). Implying that one provision (e.g., the 2001 amendments) repeals another that regulates the same subject (e.g., § 3121(c) as first enacted in 1994) is only permissible if the two competing provisions regulate the same subject, are in "irreconcilable conflict" and statutory language, legislative history or other evidence demonstrated "clear and manifest" congressional intention to repeal. Radzanower v. Touche, Ross, Co., 426 U.S. 148, 154 (1976);[7] and conversely,

D. Absent "clear and manifest evidence" from statutory language, legislative history or other evidence, a court is obliged "'[w]hen there are two acts upon the same subject . . . to give effect to both if possible.'" Mancari, 417 U.S. at 551 (quoting United States v. Borden Co., 308 U.S. 188, 198 (1939)) (emphasis added);[8]

As shown below, the above principles require that the Court construe the Pen/Trap Statute (a) to permit a pen register to access PCTDD content incidental to collecting non-content, when there is no "technology reasonably available" to avoid the incidental access, see 18 U.S.C. § 3121(c), but (b) to preclude the government from using that content, because at the time a device accesses it, the device is not functioning as a "pen

---

[7] See, e.g., United States v. Rodriguez, 480 U.S. 522, 524-525 (1987) (legislative history inconsistent with implied repeal); Capitol Records, Inc., 372 F.3d 471,480 (2d Cir. 2004) (same); see also Billing v. Credit Suisse First Boston, Inc., 426 F.3d 130, 165 (2d Cir. 2005) (evidence supporting implied repeal includes but is not necessarily limited to statutory wording and legislative history).

[8] The above rule and its corollary apply with just as much force when two competing provisions are enacted simultaneously as when there was a long interval between enactment of the one statute and enactment of the other. Auburn Housing v. Martinez, 277 F.3d 138, 145-146 (2002).

register" within the definition of 18 U.S.C. § 3127(3) and accordingly, the content is subject to 18 U.S.C. § 2515's ban on use, absent separate authorization under Title III. Such a reading gives appropriate effect both to § 3121(c)'s "technology reasonably available" ("TRA") clause and to 18 U.S.C. § 3127(3) and avoids reading the TRA clause to be superfluous or implying its repeal in the absence of clear and manifest evidence. And in any event, such a reading is compelled by legislative history that shows Congress to have specifically intended the 1994 legislation to authorize incidental access to content and the 2001 legislation to preserve the authorization enacted in 1994.

III. Application Of Governing Principles

A. On Its Face, § 3121(c) Authorizes Incidental Access To Content, If There Is No TRA That Can Avoid It

Since 1994, 18 U.S.C. § 3121(c) has included an express clause that with respect to any pen register, obligates the government to use "technology reasonably available to it that restricts the recording or decoding of . . . electronic or other impulses" to those constituting "information utilized" to process wire or electronic communications ("processing information"), such as dialed digits used to connect calls. See CALEA § 207; Patriot Act § 216. When in 2001 it added the phrase "so as not to include the contents of any wire or electronic communications," to the end of § 3121(c), Congress merely made explicit

what § 3121(c) had already plainly implied: to the extent that "reasonably available" technology enables a pen register seeking non-content to restrict recording to non-content, it tends ("so as") not also to record ("not to include") content.

In other words, from inception in 1994 and continuing after the 2001 amendments, the essential language of 18 U.S.C. § 3121(c) has not changed. It is expressed in the clause requiring the government to use "technology reasonably available to it" to restrict a pen register's collection to processing information. Under that clause, the permitted scope of operation of a pen register varies with the TRA's "restrict[ive]" capability, i.e., how well it prevents a pen register as that device monitors for and records processing information from also acquiring content.

If there is TRA that enables a pen register to distinguish the processing information that is its target from contemporaneously-transmitted content, § 3121(c) requires the government to use that technology and as result acquire only the non-content. If there is no TRA that can make that distinction with complete accuracy, however, § 3121(c) only requires the government to operate the pen register using the TRA that exists -- even though the pen register may also obtain some content as it pursues processing information.

Thus, provided the government uses what technology is reasonably availably to avoid incidental access to content, 18 U.S.C. § 3121(c) permits a pen register incidentally to access the remainder that TRA cannot avoid. The telephone pen registers sought in the instant case illustrate the point. The state of technology reasonably available to the government includes improved capacity to prevent a pen register from collecting voice content at the same time as it collecting processing information.[9] As demonstrated by our other submissions, however, the TRA has no concomitant capability to avoid the risk that a pen register collecting PCTDD non-content may also access PCTDD content. Accordingly, if the government uses what technology is reasonably available, which avoids collection of voice content, it has satisfied 18 U.S.C. § 3121(c)'s precondition to incidental access to the remaining content, namely, PCTDD content.

---

[9] The prior generation of pen registers were operated by government technicians and could be modified by them to access and record voice content as well as digits that a caller enters using touch-tones. See, e.g., United States v. Love, 859 F. Supp. 725, 732-733 (S.D.N.Y. 1994) (no grounds under federal law to suppress pen register fruits, absent evidence that pen register had been so converted); People v. Bialostok, 80 N.Y.2d 738, 740-46 (1993) (New York statute precluded operation of convertible pen register in unconverted mode absent order supported by probable cause authorizing use of eavesdropping device). By contrast, under subsequently-developed designs, pen registers are provider-controlled and can only recognize and record touch-tones, not voice content. In some limited instances, the newer voice-content minimizing designs are not available. In this case, however, they are and are being used (the court having previously authorized the requested pen registers to operate except with respect to access to PCTDD).

B. The Canons Require Construing § 3127(3)'s Text Consistent With § 3121(c)'s Limited Authorization Of Incidental Access To Content

1. § 3127(c) Is Susceptible To Two Conflicting Interpretations

Prior to the 2001 amendments, a device qualified as a "pen register," so long as it "record[ed] or decod[ed] electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line." 18 U.S.C. § 3127(3) (West 2000) (emphasis added). Thus, under the prior statutory definition, a device was functioning as a pen register so long as it acquired dialed digits, be they pre-cut-through (non-content), PCTDD non-content -- or PCTDD content. By contrast, after the Patriot Act, 18 U.S.C. § 3121(3) in relevant part defines a pen register as "a device or process which records or decodes dialing, routing, addressing and signaling information transmitted by an instrument from which a wire . . . communication" is transmitted, but "such information shall not include the contents of any communications." 18 U.S.C. § 3127(3) (West 2006) (emphasis added).

The above language can be read two different ways. One interpretation is that the "shall not" clause means only that a device or process "shall not" qualify as a "pen register" -- and therefore does not so qualify -- at any juncture that it accesses PCTDD content. In other words, such a device or process is not functioning as a "pen register" within the meaning of § 3127(3)

anytime such access occurs. The "shall not" clause, however, does not control the ambit of the definition, insofar as a device or process that collects content is also collecting non-content. Thus, a device or process that records non-content "dialing" information, e.g., directly-dialed telephone numbers or PCTDD non-content, is functioning as a "pen register" under the statutory definition at the time the device or process records that information. Moreover, that device or process meets the statutory definition at the time such non-content is recorded, regardless of whether at other times, the same device or process monitoring the same target telephone obtains content, with or without requisite authorization.

The second possible interpretation of 18 U.S.C. § 3127(3) is that the "shall not" clause that was added in 2001 excludes from the definition of "pen register" any device or process that ever accesses content, without regard to whether the device or process at other times collects non-content. Thus, under this reading, a device or process that is authorized solely by the Pen/Trap Statute is subject to a "proscription against content [that] is unqualified." Houston Decision, 441 F. Supp.2d at 823.

2. § 3127(3) Must Be Read Consistent With § 3121(c)'s Conditional Authorization Of Incidental Access To Content, Subject To § 2515's Prohibition On The Content's Use

Both of the above interpretations are plausible, provided one reads the text of 18 U.S.C. § 3127(3) in isolation. The canons of construction, however, require that § 3127(3) be interpreted in the broader context of the Pen/Trap Statute and Title III. Those rules compel resolution of § 3127(3)'s ambiguity in favor of the interpretation that recognizes a device or process to qualify as a pen register when it collects non-content, even if at other times, it is accessing content.

As further explained below, that interpretation is congruent with 18 U.S.C. § 3121(c) in particular and the electronic surveillance provisions of the Pen/Trap Statute and Title III in general. Thus, it satisfies the whole act rule because it is "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 at 154. By contrast, any interpretation that treats 18 U.S.C. § 3123(7) as a blanket "proscription" against a pen register accessing content is at odds with both the rule against superfluities and the rule against implied repeal.

18 U.S.C. § 3121(c) obligates the government to use technology reasonably available to restrict a "pen register" to collecting processing information. Accordingly, to the extent

that TRA permits, § 3121(c) serves to minimize the frequency with which a device that collects non-content and is therefore a pen register under § 3127(3), also acquires content. To the extent that the technology is not reasonably available to keep a "pen register" from accessing content in the course of collecting non-content, § 3121(c) creates a safe harbor that permits the incidental access to occur.

Because that safe harbor extends only to access, no conflict inheres between the interpretation of § 3127(3) that counts a device as a "pen register" at the time it collects non-content, but not at any moment that it incidentally accesses content. When the government applies for and receives authorization to use a "pen register" by certifying the likely relevance of that device's output (see 18 U.S.C. § 3123(c)), its license to use the result is limited to non-content processing information within the definition of § 3127(3) contemplates. Moreover, were the government to seek to use content that had been incidentally-accessed pursuant to § 3121(c), any "part of the contents of such communication[s] and [any] evidence derived therefrom" would be subject to suppression, absent separate authorization based on consent, or on an order issued based on probable cause, exhaustion and the other requisites of Title III. See 18 U.S.C. § 2515.

By contrast, an interpretation that construes 18 U.S.C. § 3127(3)'s "shall not" clause to remove from the ambit of that statute any device or process that acquires content -- ever -- does not withstand scrutiny. Rather, any such interpretation conflicts with the canons of construction because it ignores language to the contrary in § 3121(c). Under § 3121(c), whether a device may access content incident to collecting content depends on whether or not "technology reasonably available" exists to avoid the collection. If such TRA exists, the government must use it. If not, the incidental access is permitted.

Reading § 3127(3) to impose an outright ban on access to content would mean that the question of what technology is reasonably to prevent such access is irrelevant. Rather, the government would be required to use any means at its disposal to exclude content (e.g., PCTDD content) from the data that a device collects in searching for non-content (e.g., PCTDD non-content). If no such means existed (as is the case with respect to PCTDD here), § 3127(3) would proscribe that device from being used to seek that (PCTDD) non-content at all.

"To read out of a statutory provision a clause setting forth a specific condition or trigger to the provision's

applicability," however, "is an entirely unacceptable method of construing statutes"). Natural Resources Defense Council v. United States, 822 F.2d 104, 112-113 (D.C. Cir. 1987). Accordingly, in this case, reading the words "reasonably available" out of § 3121(c) violates both the rule against superfluities and the rule against implied repeal.

The first canon requires construing the Pen/Trap Statute "upon the whole," so that "if it can be prevented, no clause [or] sentence shall be superfluous, void or insignificant." Duncan v. Walker, 533 U.S. at 174. As demonstrated above, construing 18 U.S.C. § 3127(3) to define a device as a "pen register" when it collects non-content but not when it collects content, prevents the outcome that the rule against superfluities condemns: nullifying the words "reasonably available" in § 3121(c) by construing § 3127(3) to ban a device from ever accessing content under authority of the Pen/Trap Statute.

The analysis and therefore the outcome are similar under the canon against implied repeal. In the absence of an "irreconcilable conflict" between the meaning of two statutes that regulate the same subject and "clear and manifest" evidence that one statute was intended to repeal the other, Radzanower v. Touche, Ross, Co., 426 U.S. at 154, a court is required "to give effect to both, if possible." Morton v. Mancari, 417 U.S. at

549. As demonstrated above, no irreconcilable conflict exists. Rather, any putative conflict between § 3127(3) and the technology reasonably available clause of § 3121(c) is avoided if § 3127(3) is interpreted to mean that the statute's definition of a "pen register" is satisfied by a device when it collects non-content, regardless of whether at other times it accesses content.

Nor is there persuasive evidence in the Pen/Trap Statute, let alone "clear and manifest evidence," that the Patriot Act's amendment of § 3127(c) was intended impliedly to repeal § 3121(c)'s pre-existing permission of incidental access to content in the absence of technology reasonably available to avoid it.[10] As previously explained, the essential language of § 3121(c) has remained unchanged since 1994 with respect to use of pen registers on telephones. At inception, § 3121(c) conditioned permission for incidental access to content on the absence of "technology reasonably available that restricts" such a device to collection of "dialing" and related processing information. See CALEA § 207. The text of § 3121(c) was not materially unchanged by the addition of the phrase "so as to not

[10] As detailed at Point III.C.1. below, implied repeal is likewise precluded by statements in 2001 by Senator Leahy, the principal drafter of both the 1994 and 2001 legislation, demonstrating that he did not believe the Patriot Act's amendments effected any material change with respect to the Pen/Trap Statute limitation on a device incidentally accessing content.

include . . . contents," for that merely highlighted what § 3121(c) already implied: technology reasonably available that can restrict a pen register to collecting processing information serves to avoid access to content. Thus, the sole statutory indicia of implied repeal is the "shall not" clause added to § 3127(3) in 2001. That is hardly sufficient to imply repeal, for as shown above, § 3127(3) is also susceptible to a contrary interpretation that is consistent with § 3121(c)'s TRA clause. Since the contrary interpretation enables a court "to give effect" to both statutes, it is that construction which a court must adopt. Morton v. Mancari, 417 U.S. at 551.

C. Legislative History Confirms Congress Intended In 1994 To Permit Incidental Access To Content, To Be Minimized To The Extent That TRA Allows, And Intended In 2001 To Preserve That Permission

Legislative history should be used to construe a statute only when the statute's text and contextual analysis that applies canons do not entirely dispel ambiguity. Daniel v. American Board of Emergency Medicine, 428 F.3d at 423. While we submit that the prior discussion sufficiently demonstrates the correct construction of 18 U.S.C. §§ 3121 and 3127(3), legislative history proves it beyond any doubt.

1. The 1994 Enactment Established TRA As The Sole Criterion To Determine When Incidental Access Is Permitted

18 U.S.C. § 3121(c) was originally proposed by Senator Patrick Leahy, chairman of the Senate Judiciary Subcommittee on

Technology and The Law, as part of S.2375, the "Digital Telephony Act of 1994." See 140 Cong. Rec. 11055, at 11059 (August 9, 1994) (see Ex. 1 hereto). Most of S.2375's provisions, including the proposed § 3121(c), were eventually incorporated in CALEA. The Senator's introductory remarks included a sectional summary. Significantly, in that summary, he stated as follows:

> [This subsection] requires government agencies installing and using pen register 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. 11055, at 11062 (emphasis added).

Thus, the primary architect of § 3121(c) explicitly acknowledged that the provision keyed both prevention and permissible occurrences of incidental access by the government of PCTDD content to the "reasonable availab[ility]" of filtering technology. "When" such technology is reasonably available, the government is required to deploy it to avoid accessing PCTDD content (i.e., "further communications conducted through the use of dialled digits"). "When" it is not, however, the statute permits the "otherwise" scenario to unfold, in which the government is allowed to access PCTDD content as a necessary incident of acquiring "dialling or signaling information necessary to direct or process a call.

The statements of bill sponsors are entitled to significant weight, albeit not always as much weight as reports by Congressional committees on the same legislation.[11] Here, however, the Senate and House committee reports accompanying CALEA adopted the Senator Leahy's statement word-for-word. See S. Rep. 103-402, at *31 (1994)(excerpted at Ex. 2 hereto); H.R. Rep. 103-827(I) at *32 (1994) (excerpted at Ex. 3 hereto).

Moreover, the 1994 Senate and House reports each contain an additional sentence that compels the conclusion that § 3121(c) is permissive with respect to incidental access to content, absent "technology reasonably available" to filter content from non-content PCTDD. That sentence states that § 3121(c) is intended to "requir[e] law enforcement to use reasonably available technology to minimize information obtained through pen registers" (emphasis added). See S. Rep. 103-402, at 18; H.R. Rep. 103-827(I) at 17.

Well in advance of the 1994 enactment, the term "to minimize" had acquired a specific meaning under the electronic surveillance laws. 18 U.S.C. § 2518(5) of Title III of Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Statute") provides in relevant part that wiretap orders require interceptions "be conducted in such a way as to minimize the

---

[11] United States v. International Union (UAW-CIO), 352 U.S. 567, 585 (1957); accord Banco Nacional de Cuba, 383 F.2d 166, 177 (2d Cir. 1967).

interception of communications not otherwise subject to interception under" Title III (emphasis added). Under well-established precedent, the quoted provision "does not forbid the interception of all nonrelevant conversations, but rather, instructs the agents to conduct the surveillance in such a manner as to minimize the interception of such conversations," which is to be adjudged under a standard of reasonableness. Scott v. United States, 436 U.S. 128, 140 (1978); accord United States v. Turner, 528 F.2d 143, 156 (1975) (§ 2518 "requires that measures be adopted to reduce the extent of such interception to a practical minimum while allowing the legitimate aims of the Government to be pursued.")

The drafters of § 3121(c) were undoubtedly aware of what "to minimize" means under 18 U.S.C. § 2518(5).[12] In any event, the law presumes that they knew it when they used the term "to minimize" in the 1994 Congressional reports.[13] Title III's

---

[12] CALEA's principal purpose was "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), at 9.

[13] As a matter of law, they are presumed to have been

> (a) knowledgeable about existing laws pertinent to later-enacted legislation, (b) aware of judicial interpretations given to sections of an old law incorporated into a new one, and (c) familiar with previous interpretations of specific statutory language.

minimization clause permits the interception and recording of noncriminal conversations incidental to monitoring for criminal conversations, provided that agents take reasonable steps, see Scott v. United States, to keep the interceptions of the noncriminal conversations to a practical minimum, see United States v. Turner. Accordingly, 18 U.S.C. § 3121(c) was intended to permit access to dialed-digit content incidental to the recording of dialed-digit non-content, provided that the government keeps the recording of such content to a practical minimum by means of "technology reasonably available to" it. Because the Senate and House reports also show that the drafters understood that there would be occasions "when" no such technology would be reasonably available (see Exs. 2 and 3), they further establish that Congress intended in that event to permit incidental access.

2. Congress Intended In 2001 To Preserve The Safe Harbor For Incidental Access That It Had Originally Established In 1994

The Patriot Act contains no definitive Congressional committee report on its amendments to the Pen/Trap Statute.[14]

United States v. Bonanno Organized Crime Family of La Cosa Nostra, 879 F.2d 20, 25 (2d Cir. 1989) relying, respectively, on Goodyear Atomic Corp. v. Miller, 486 U.S. 174, 184-185 (1988); St. Regis Mohawk Tribe v. Brock, 769 F.2d 37 (2d Cir. 1985); and Blitz v. Donovan, 740 F.2d 1241, 1245 (D.C. Cir. 1984).

[14] H.R. 2975, a predecessor bill on which the House Judiciary Committee reported on October 11, 2001, contemplated similar changes. The bill proposed that §§ 3121(c) and 3127(c)

Accordingly, the next best source of authority to a committee report are the statements of Chairman Leahy, who was the primary architect of the final Senate bill. See, e.g., United States v. International Union (UAW-CIO), 352 U.S. at 585. Senator Leahy's remarks show that the Patriot Act's addition of express references to "contents" in both 18 U.S.C. §§ 3121(c) and 3127(3) was not intended to effect any substantive change to the minimization approach that he had helped devise in 1994, predicated on whether technology was reasonably available to avoid incidental access. Rather, Senator Leahy assumed that the government would continue incidentally to access content, and therefore added the express references in order to assure that courts would more closely examine whether technology is "reasonably available" to facilitate the recording of permitted non-content without incidental collection of content.[15]

---

be updated to cover pen registers on communication instruments other than traditional telephones, modernized with language similar to that ultimately adopted (e.g. by defining pen registers to include "processes" or "device" that record or decode "dialing," "routing" and other information from such devices.) The accompanying report, however, merely cursorily states that "[t]he [proposed] amendments reinforce the statutorily prescribed line between a communication's contents and non-content information, a line identical to the constitutional distinction drawn by the U.S. Supreme Court in Smith v. Maryland, 442 U.S. 735, 741-43 (1979)." 107 H.Rep. 236, Part 1, at 51 (October 11, 2001).

[15] Two other legislators, Senator Hatch, the ranking minority member of the Judiciary Committee; and Senator Feinstein made comments that may be read to disagree with Senator Leahy's. See 147 Cong Rec. S10990 (Oct. 11, 2001), at S10691 ("[pen register] orders do not allow law enforcement to eavesdrop on or

On October 25, 2001, Senator Leahy appeared before the Senate to make final remarks before the vote on the Patriot Act. See 147 Cong. Rec. S10990, at S10990-11015, annexed as Ex. 4 hereto. Among other things, the Senator detailed the considerations that had shaped his work on the proposed revisions to the Pen/Trap Statute. See Ex. 4. at S10999-11000, S11006. Senator Leahy stated that among his goals in negotiating revisions of the Pen/Trap Statute were (1) to modernize it to cover computer-based applications, (2) to obviate the need for

---

read the content of communication [sic]") (Senator Feinstein); Id. at S10561 ("The legislation . . . would make clear that Federal judges [have] pen register authority . . . [over] more modern modes of communication, such as email and instant messaging. . . . [T]he bill does not allow law enforcement to receive the content of [a] communication, but they can receive the addressing information to identify the computer or computers a suspect is using to further his criminal activity") (Senator Hatch). These remarks are annexed hereto as Ex. 5. Neither statement proves that the Patriot Act was intended to repeal the permission that § 3121(c) had theretofore established with respect to a pen register's incidental access to PCTDD content. Senator Leahy, who as shown below very clearly understood not repeal was in the offing, was the primary drafter of the Patriot Act. His remarks are therefore entitled to substantially greater weight than any others'. In addition, Senator Hatch's statement appears only to refer to disallowance of interception of content with respect to "more-modern" computer-based communications, such as email and instant messaging ("IM"), and not to the issue of incidental access to (telephonic) PCTDD. Moreover, there is no impediment to construing the Pen/Trap Statute "not [to] allo[w] law enforcement to receive the content of" a computer-based communication, while "allow[ing]" incidental access to PCTDD content. In contrast to PCTDD, typically, there is no technological impediment to segregating email or IM addressing information from its companion content. Thus, under § 3121(c), properly construed, access to the content of computer-based communications typically is not permitted under § 3127(c) because there is TRA to avoid it, whereas incidental access to PCTDD content is permitted because no comparable technology exists to avoid it.

redundant applications by authorizing nationwide service of orders; and (3) "to update the judicial review procedure" to increase "judicial discretion in reviewing the justification for the order." Ex 4. at 10999.

The Senator emphasized that while his first two goals had been met by the proposed legislation, the goal of "meaningful judicial review" in large part had not. Id. Nevertheless, at the conclusion of his statement, Senator Leahy stressed that he supported the Patriot Act as "a good bill," a "balanced bill" and one that established necessary "checks and balances." Id. at 11015. What is plain from the intervening text is that while the Senator would have preferred to amend the pen register procedure to require more probing judicial review of incidental access to content, he had acquiesced in limited revisions to the Pen/Trap Statute that left intact the government's permission for such access, subject to the condition that, if reasonably available, the government must instead use filtering technology.

Senator Leahy criticized the amendments to the Pen/Trap Statute on several fronts, including the issue of incidental access to content. According to the Senator, he had drafted the original version of 18 U.S.C. § 3121(c) in 1994 out of concern that pen register "devices collected content and such collection was unconstitutional on the mere relevance standard." Ex 4. at

S11000.[16] In June 2000, however, the Justice Department advised the Senate Judiciary Committee that no technology had been developed that could reduce incidental access to dialed-digit content. Rather, according to the June 2000 communication from the Justice Department, pen registers

> "'do capture all electronic impulses transmitted by the facility on which they are attached . . . .],'" and
>
> ""there has been no change . . . that would better restrict the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing."

Id. (quoting June 2000 letter from Justice Department) (emphasis added).

In his October 25, 2001 remarks, Senator Leahy asserted that the Patriot Act contained an "important" response to the above state of affairs, namely, the amendment to 18 U.S.C. § 3121(c) that makes explicit the implication that the purpose of requiring the government to use "reasonably available technology"

---

[16] Thus, Senator Leahy impliedly confirmed that 18 U.S.C. § 3121(c) as originally enacted was intended to function as a minimization scheme similar to the one in Title III. Enacting a standard that permits incidental content recording in the absence of technology reasonably available to filter it obviously did nothing to raise the government's burden above mere relevance. The 1994 enactment, however, comported with Fourth Amendment principles by permitting such recording only to the extent that technology could not be used to prevent it -- in much the same way that the Fourth Amendment and 18 U.S.C. § 2518(5) permit incidental recording of non-pertinent conversations to the extent that reasonable precautions, such as "spot-monitoring" cannot prevent it.

to restrict recording to non-content was "'so as not to include . . . conten[t].'" Ex 4. at S11000.

Senator Leahy emphasized, however, that the amendment would not regulate incidental content recording to the degree that he would have preferred. In particular, he explained, for several years he had backed a proposal "[d]ue in significant part to the fact that pen/trap devices in use today collect 'content,'" but Congress had rejected that approach. Ex 4. at S11000 (emphasis added). The rejected proposal would have raised the government's burden of production on pen register applications from mere certification of relevance (see 18 U.S.C. § 3121(b)(2)) to an obligation to articulate relevance to the courts. Ex 4. at S11000. The Senator opined that increasing the required showing in this manner would have promoted "meaningful judicial review and accountability," that "[p]erhaps" would cause the government to take " the statutory direction [sic] [to foster filtering technology] more seriously and actually implement it." Id.

For the purposes of the instant application, Senator Leahy's criticisms of the amendments to 18 U.S.C. § 3121(c) -- and the government -- are at least as important for what they do not say as for what they criticized the Patriot Act for not doing. The Senator did not claim that under his preferred approach or as amended by the Patriot Act, the Pen/Trap Statute

would eliminate or even substantially curtail the prevailing state of affairs in which pen registers acquire all electronic impulses, non-content or otherwise, from the facility to which they are attached. Had he believed that either would effectively outlaw incidental content absent the deployment of technology, he most certainly would have said so. In reality, however, his remarks show the Patriot Act merely amended the Pen/Trap Statute to state more clearly that the government's obligation to use filtering technology if and when it is reasonably available is aimed at reducing incidental access to content. While this change may well focus the attention of the bench on whether the technology is reasonably available, the change authorizes narrower judicial intervention than Senator Leahy had sought. Plainly, it falls far short of permitting, let alone requiring courts to ban incidental access to content on the mere grounds that filtering technology is not being used.

IV. The Houston Decision Is Fundamentally Flawed

Only by serial errors in reasoning does the Houston Decision conclude that 18 U.S.C. § 3127(3) as amended prohibit a device or process from accessing content under authority of the Pen/Trap Statute. The most and generic critical error is discussed at length above: namely, that construing § 3127(3) to impose a blanket prohibition requires reading the operative words "reasonably available" out of the companion language of 18

U.S.C., § 3121(c). There are, however, related errors, the skein of which more precisely maps how the Houston Decision goes awry:

A. The Decision Ignores § 3127(c)'s Ambiguity.

Not once does the Houston Decision even consider the possibility, let alone the reality, that the "shall not" clause of § 3127(c) is susceptible to two, mutually antagonistic interpretations, only one of which is an "unqualified" proscription against content. 441 F. Supp.2d at 823. Rather, the decision simply assumes that a definition that specifies what a "pen register" does when functioning as such -- "recording or decoding dialing [or other processing] information" -- and further states that such information "shall not include" content -- means that a device or process that sometimes acquires processing information and sometimes content is never a "pen register." As explained above, the assumption is not self-proving. Rather, it must be tested against the competing interpretation that recognizes a device or process to be functioning as a pen register at those times that it is recording non-content and not to function as such when it accesses content. Moreover, testing also requires comparing both interpretations to determine which is more consistent with § 3127(3)'s "technology reasonably available" clause. As explained above, the interpretation that recognizes that a device is a pen register

whenever it collects non-content, regardless of whether at other times it access content, wins that comparison.

B. The Decision Fails To Heed Its Own Invitation To Consider Legislative History.

In discussing § 3121(c), the Houston Decision starts from the proposition that the statute does no more than impose on the government an obligation that it "shall use technology" to operate an already-authorized pen register. 841 F. Supp.2d at 824. As a preliminary matter, this assertion flatly ignores the words "reasonably available to" the government that condition whether or not the government must filter content. Thereafter, the Houston Decision concedes that § 3121(c) may be read to permit incidental access to content to the extent that TRA cannot avoid it, but ignores its own invitation further to evaluate the merit of that interpretation.

Specifically, the decision admits that "one possible way" to read § 3121(c) is that it requires "'minimiz[ing] content'" only to the extent that TRA permits, while "allow[ing] all non-content," 841 F. Supp.2d at 824-825. More importantly, it characterizes as "curious" why Congress "did not explicitly declare content digits as fair game." Id. at 824. As demonstrated above, the 1994 legislative history resolves any question on that score, for it demonstrates that Congress clearly did intend content digits to be accessible when no TRA exists to avoid the access. Notwithstanding its own query, however, the

Houston Decision contains not one word about the 1994 legislative history. Indeed, the decision reads as if it was prepared with no consideration whatsoever of CALEA's history. Had that history been considered, the holding of the case would likely have been very different. Rather, it would have had to consider whether such an implication was justified, inter alia, by "clear and manifest evidence" establishing that the Patriot Act amendments to the Pen/Trap Statute were intended to repeal § 3121(c) in its original form. Radzanower v. Touche, Ross, Co., 426 U.S. at 154. Likewise conspicuously absent from the Houston Decision, moreover, are key portions of Senator Leahy's statement in 2001, that had they been considered, would -- or at least should -- have prevented the decision from implying that the Patriot Act was intended to rescind the permission that the Pen/Trap Statute previously conferred with respect to incidental access to content. In particular, the Houston Decision fails to mention, let alone weigh, the remarks in which Senator Leahy acknowledged that although pen registers currently "'do capture all electronic impulses,'" and the FBI had reported that there had been no improvement in technological capacity, the Patriot Act did no more than encourage "meaningful judicial review," and did not in fact ban all incidental access. Ex. 4 at *S11000.

C. The Decision Misapprehends The Canons

In the Houston case, the government likewise argued that reading § 3127(3) to prohibit all incidental access to content violated the rule against superfluities by nullifying the phrase "reasonably available" in § 3121(c). The Houston Decision rejected the argument on the grounds that the "operative canon is not the rule against superfluity, but rather the rule that statutory provisions be construed in harmony with one another. 441 F. Supp.2d at 825. As a matter of law, however, these canons are not severable, but rather expressions of the same principle.

"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. at 174 (emphasis added). Thus, if it is possible to reconcile two statutes that are otherwise in conflict by giving effect to every one of their words, that is how they must be harmonized. Id. The Houston Decision, however, "harmonizes" its reading of § 3127(3) as an unyielding proscription against access to content by insisting that the "so as not to include . . . content" clause is likewise an "unqualified content proscription." 441 F. Supp.2d. at 825. That is not a persuasive argument. As previously explained, the "so as" clause merely describes § 3121(c)'s tendency when "technology [is] reasonably available" to avoid incidental access to content.

In other words, the "so as" clause is subordinate to the "technology reasonably available" clause. Accordingly, when it purports to locate the same "proscription" in § 3121(c) as it insists inheres in § 3127(c), the Houston Decision in so sense "harmonizes" statutes in the manner that the canons require. Rather, it violates the whole act rule and rule against superfluities by refusing to give the words "reasonable available" in § 3121(c) any effect.

D. The Canon of Constitutional Avoidance Cannot Cure the Decision's Predicate Misconstructions.

At its conclusion, the Houston Decision asserts that construing the Pen/Trap Statute not to permit any incidental access to content is also justified by the canon of constitutional avoidance. 441 F. Supp.2d at 836-37. The decision correctly describes that rule as one that "compels a court to construe a statute in a manner which avoids serious constitutional problems, unless such a construction is plainly contrary to the intent of Congress." Id. at 836-837 (citing Edward J. Bartolo Corp. v. Florida Gulf Coast Building & Construction Trades Council, 485 U.S. 568, 575 (1988)).

The Houston Decision's reliance on that canon is misplaced, however, because the decision ignores legislative history that demonstrates that Congress's intent plainly contradicts the decision's construction of the Pen/Trap Statute. Passing the deficiencies of the decision's analysis of the

statutes' ambiguity and the decision's efforts to resolve it, the Houston Decision gives no consideration whatsoever to the legislative history from 1994 and though it considers some of Senator Leahy's 2001 remarks, it disregards the most important ones. (See Point IV.B. above)

As explained at Point III.C. above, the legislative history from 1994 demonstrates that Congress made a knowing choice to modify the Pen/Trap Statute to add a content minimization provision analogous to the provisions of Title III governing minimization of nonpertinent content. The legislative history of the Patriot Act shows that Congress intended in that 2001 legislation to retain the same minimization standard. That standard, of course, is set forth at 18 U.S.C. § 3121(c), which requires the government to use technology reasonably available, when it exists, to avoid incidental access to content, but permits the incidental access when it does not.

Accordingly, the canon against constitutional avoidance cannot cure the Houston Decision's statutory misinterpretations. The intent of Congress is not "plainly contrary" to permitting the government incidental access to content, Bartolo Corp. 485 U.S. at 575. Rather, the evidence of intent shows Congress to have intentionally permitted the access to the extent when there exists no technology reasonably available than can minimize it.

That is, moreover, an entirely reasonable choice in accord with the Fourth Amendment. Scott v. United States, 436 U.S. at 140.

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
January 19, 2007

Respectfully submitted,

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

JED DAVIS
(718) 254-6298
SCOTT KLUGMAN
Assistant U.S. Attorneys
(718) 254-6461
(Of Counsel)

EXHIBIT 1

Excerpts From Senator Leahy's Remarks 8/9/94
(Pertinent portions in **bold**)

CONGRESSIONAL RECORD -- Senate

Tuesday, August 9, 1994
(Legislative day of Monday, August 8, 1994)

103rd Congress 2nd Session

140 Cong Rec S 11055

REFERENCE: Vol. 140 No. 109

TITLE: STATEMENTS ON INTRODUCED BILLS AND JOINT RESOLUTIONS

TEXT:

[*S11055]

By Mr. LEAHY:

S. 2375. A bill to amend title 18, United States Code, to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes; to the Committee on Commerce, Science, and Transportation.

THE DIGITAL TELEPHONE ACT OF 1994

Mr. LEAHY. ;Mr. President, there was a time when law enforcement, if they wanted to listen in to what criminals were saying, the local sheriff could drive down the road, climb on the top of his car, plug a couple alligator clips on to a telephone wire, put on the earphones and know what was being said.

A lot has changed since that time. One of the things that changed, of course, is that we passed legislation laying out who could eavesdrop, when they could listen in and who could be eavesdropped on. We made it very clear: You had to apply to a court and get a warrant. We set good standards to protect your privacy, my privacy, the privacy of everybody in this country. So the standards are there, but the alligator clips have changed.

Now, with digital transmissions, if you were to go down and listen in on a phone line, you probably would just hear a loud buzz. A drug dealer in Boston, MA, who wants to talk with a supplier in Dade County, FL, may pick up a cellular phone that may send out a digital signal, which is nothing more than ones and zeros. This conversation may go through a half-dozen different linkages. It may go any way but a straight line from Boston to Florida, and a lot of it could be over fiber optic cables. And even if you could find the right cable, even if you could find the one conversation out of several thousand conversations carried over the same cable that was the one the court order allowed you to tap, you might hear nothing but a buzz. That is not going to help much to catch that drug kingpin or to stop that kidnapping or to stop a planned assassination or stop any other serious felony.

Because of this loss of ability to keep up with technology, Louis Freeh, the FBI Director, said, ''The number one law enforcement, public safety, and

national security issue facing us today'' is preserving the ability to conduct wiretaps.

So what I am doing is introducing a bill that will give our law enforcement agencies back the confidence that when they get a wiretap order, they will be able to do their jobs and carry out the order. This will allow wiretaps under court orders to be able to be used even with the new digital technology and other emerging telecommunications technologies. This bill will not impede new technologies but ensure they will not confound legitimate law enforcement needs.

Now when this was first proposed-first in the last administration and early on in this administration-I opposed the idea, because it appeared to me that not only were there inadequate safeguards to protect the individual privacy of all of us, but I was very concerned that it was going to set up the Justice Department as some kind of a traffic cop on new technologies.

One of the things that allows us to compete with the rest of the world, especially in our ability to export, is the genius of our technology and our ability to fashion new technology. I was concerned that we would no longer be able to do so and that the Justice Department could say, ''Hold it, we don't want you to put in speed dial, we don't want you to put in call forwarding or anything else because it doesn't fit what we want.''

This worried me, because, unfortunately, the Federal Government has adamantly and steadfastly stayed 10 to 15 years behind most emerging technologies. We have seen it here in the Senate, where we have had to use antiquated computer systems. We have seen it at the Department of Defense, where they have communications systems that look like they are something out of World War II and not out of the Star Wars they talk about.

Private industry has gone way ahead of the Federal Government in technology and computers and telecommunications, and I did not want it held back.

So what we have done now is put together a bill-Congressman Edwards, in the House, and myself-that will help law enforcement. But it also contains important expansions of privacy protection for transactional information, mobile phone communications, certain radio-based communications, and will not impede technology.

Regarding the issue of digital telephony, it should be noted we came an enormous way after countless meetings and literally hundreds of hours of work by people in the private sector, law enforcement, FBI Director Freeh, Members of the House and Senate and staff. But throughout all of this, the person who worked tirelessly and was involved in every single part of it was, and is, attorney Beryl Howell of the Judiciary Committee staff assigned to my Subcommittee on Technology and the Law.

Beryl Howell is a former prosecutor from the U.S. attorneys office in New York. She is a tremendous litigator, brilliant lawyer, and I think it is safe to say that without her work and her dedication, we would not be introducing this bill today.

Now that the crime conference is concluded, we expect to be considering the conference report shortly. The crime bill does not confront what Louis Freeh, the FBI Director, has identified as ''the number one law enforcement, public safety, and national security issue facing us today.''

That issue is wiretaps, and law enforcement's losing battle to keep up with new technologies that undermine its capability to use this powerful tool in its crime-fighting arsenal.

There is no doubt that wiretaps can produce powerful evidence against our most dangerous criminals. Instead of making deals with other criminals, or putting innocent bystanders at risk in order to have witnesses who can testify about a defendant's crimes, the police use wiretaps to catch and convict criminals with secretly taped words from their own mouths.

But the FBI and other law enforcement agencies have told Congress that their ability to use this tool is being undercut by new communications features and services that were designed with no thought as to how they might affect law enforcement.

Over the past few months, I have worked closely with Representative Don Edwards , chairman of the House Judiciary Subcommittee on Civil and Constitutional Rights, to write the bill I introduce today that addresses the No. 1 problem facing law enforcement today. Industry groups, privacy and civil liberties experts, and the FBI have worked diligently with us in this effort, and I applaud them for undertaking this difficult task. I look forward to hearing from these groups at a joint hearing with Don Edwards ' Subcommittee this Thursday, with a view to making this bill even better.

My goal in this legislation is to assist legitimate law enforcement needs without jeopardizing privacy rights or frustrating the development of new communications technologies or the competitiveness of America's high-technology industry. I believe this bill achieves that goal.

This is not the first time that Congress has had to take a close look at the wiretap statute to take into account developments in communications technology and the structure of the telecommunications industry. We last did so in 1986 when we passed the Electronic Communications Privacy Act.

This law extended the reach of the Federal wiretap law, and its privacy protections, to electronic mail and [*S11056] computer-to-computer communications.

In February, FBI Director Freeh came to me and other Members of Congress to consult about a proposal to revise our wiretap law anew in the face of the increasing pace of advances in telecommunications technology and impediments to execution of court-ordered wiretaps. The Clinton administration followed up last March by sending Congress proposed legislation that made significant improvements to an earlier Bush administration draft proposal. We have built on those improvements to address the significant concerns that remained.

First, to ensure law enforcement's continued ability to conduct court-authorized wiretaps in light of new and emerging digital technologies, the bill sets forth four wiretap capability requirements that telecommunications carriers would be required to meet. This means that when the phone companies set about designing and deploying new services or features, they must consider law enforcement's needs among the numerous other factors that go into such designs.

Just as phone companies make sure that when they plug-in new services, the phone system is not shorted-out, so too we do not want to shortchange the American people's need for effective law enforcement.

Second, on the privacy front, the bill expands privacy and security protections for our telephone and computer communications in ways that were first recommended to me by a privacy and technology task force I organized in 1991. The protections of the Electronic Communications Privacy Act are extended to cordless phones and certain data communications transmitted by radio.

In addition, this bill increases the protection for transactional data on electronic communications services by requiring law enforcement to get a court order for access to those records.

The bill further 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. Finally, the bill improves the privacy of mobile phones by expanding criminal penalties for stealing the service from legitimate users.

Third, to encourage innovation in telecommunications services, the bill states expressly that law enforcement agencies may not require the specific design of telecommunications systems or features, nor prohibit adoption of any such design, by any telecommunications provider.

The bill sets up a mechanism for ensuring law enforcement's wiretap capability needs while at the same time deferring to industry to decide how best to meet law enforcement's wiretap needs. No Government official will be put in charge of the future of our telecommunications industry.

This legislation leaves it to industry in the first instance.

But I also do not want industry and law enforcement representatives to get together in some back room and figure out how to wiretap America. It is important that this process be subject to public scrutiny, oversight, and accountability. This bill accomplishes this by requiring any standards or technical requirements that industry adopts to ensure wiretap capability be publicly available.

Furthermore, this bill avoids putting industry in the position of guaranteeing wiretap capability, with failure punished by stopping a service or feature that consumers want. If industry is ready to deploy a new phone feature or service, but cannot yet figure out how to give law enforcement access for lawful wiretaps, a court must take that into consideration and may not stop deployment of the service. On the other hand, if industry can fix the service to assist law enforcement, it must do so.

This bill preserves a legitimate law enforcement tool without jeopardizing privacy rights or frustrating innovation and the development of new technologies or undercutting the competitiveness of America's high-technology industries.

Mr. President, I ask unanimous consent that the legislation and a section-by-section analysis be inserted in the Record .

There being no objection, the material was ordered to be printed in the Record , as follows:

EXCERPT BREAK

Sectional Summary

The bill consists of the following ten sections:

Sections 1 through 4 deal with law enforcement's wiretap capability and capacity needs.

Sections 5 through 7 expands the privacy protection of the Electronic Communications Privacy Act to cover cordless phones and certain radio-based communications, and Section 8 makes a technical correction to that law.

Section 9 improves the privacy and security of communications over cellular telephones by prohibiting the fraudulent alteration of such telephones for the purpose of stealing service.

Section 10 protects the privacy of electronic communications by requiring a court order for the disclosure of transactional data and by limiting the use of pen registers that intercept information other than dialing or signalling information.

EXCERPT BREAK

Section 9. Clone phones. This section amends the Counterfeit Access Device law to criminalize the use of cellular phones that are altered, or ''cloned,'' to allow free riding on the cellular phone system. Specifically, this section prohibits the use of an altered telecommunications instrument, or a scanning receiver, hardware or software, to obtain unauthorized access to telecommunications services. A scanning receiver is defined as a device used to intercept illegally wire, oral or electronic communications. The penalty for violating this new section is imprisonment for up to fifteen years and a fine of the greater of $50,000 or twice the value obtained by the offense.

Section 10. Transactional data. Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers, subsection (a) eliminates the use of a subpoena by law enforcement to obtain from a provider or electronic communication services the addresses on electronic messages. In order for law enforcement to obtain such information, a court order is required.

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a [*S11062] subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against ''fishing expeditions'' by law enforcement. Under the intermediate standard, law enforcement must show facts which establish why such records are relevant and material to an ongoing criminal investigation.

Law enforcement could still use a subpoena to obtain the name, billing address, and length of service of a subscriber to or customer of such service and the type of services the subscriber or customer utilized.

Subsection (b) requires government agencies installing and using pen register devices to use, <u>when reasonably available</u>, technology that restricts the information captured by such device to the dialling or signaling information necessary to direct or process a call, excluding any further communications conducted through the use of dialled digits that would otherwise be captured.

EXHIBIT 2

Excerpts from Senate Report accompanying CALEA
(pertinent portions in **bold**)

S. REP. 103-402
S. REP. 103-402, S. Rep. No. 402, 103RD Cong., 2ND Sess. 1994, 1994 WL 562252 (Leg.Hist.)
(Cite as: S. REP. 103-402)

*1 THE DIGITAL TELEPHONY BILL OF 1994
SENATE REPORT NO. 103-402
October 6, 1994
[To accompany S. 2375, as amended]

The Committee on the Judiciary, to which was referred the bill (S. 2375) to make clear a telecommunications carrier's duty to cooperate in the interception of communications for law enforcement purposes, and for other purposes, having considered the same, reports favorably thereon with an amendment and recommends that the bill, as amended, do pass.

* * *

*17

***

THE LEGISLATION ADDRESSES PRIVACY CONCERNS

Since 1968, the law of this Nation has authorized law enforcement agencies to conduct wiretaps pursuant to court order. That authority extends to voice, data, fax, E-mail and any other form of electronic communication. The bill will not expand that authority. However, as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.

In the 8 years since the enactment of ECPA, society's patterns of using electronic communications technology have changed dramatically. Millions of people now have electronic mail addresses. Business, nonprofit organizations and political groups conduct their work over the Internet. Individuals maintain a wide range of relationships on-line. Transactional records documenting these activities and associations are generated by service providers. For those who increasingly use these services, this transactional data reveals a great deal about their private lives, all of it compiled in one place.

In addition, at the time ECPA was enacted, the portion of the communications occurring between the handset and base unit of cordless telephones was excluded from its privacy protections. The 1991 Privacy and Technology Task Force found that:

[t]he cordless phone, far from being a novelty item used only at "poolside," has become ubiquitous. *** More and more communications are being carried out by people [using cordless phones] in private, in their homes and offices, with an expectation that such calls are just like any other phone call.

*18 Therefore, S. 2375 includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the Government's current surveillance authority. Specifically, the bill:

1. Eliminates the use of subpoenas to obtain E-mail addresses and other similar transactional data from electronic communications service providers. Currently, the Government can obtain transactional logs containing a person's entire on-line profile merely upon presentation of an administrative subpoena issued by an investigator without any judicial intervention. Under S. 2375, a court order would be required.

2. Expressly provides that the authority under pen register and trap and trace orders cannot be used to obtain tracking or location information, other than that which can be determined from the phone number. Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information. **Further, the bill requires law enforcement to use reasonably available technology to minimize information obtained through pen registers.**

***

***

SECTION 10. TRANSACTIONAL DATA

Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers, subsection (a) eliminates the use of a subpoena by law enforcement to obtain from a provider of electronic communication services the addresses on electronic messages. In order for law enforcement to obtain such information, a court order is required.

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable-cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

Law enforcement could still use a subpoena to obtain the name, address, telephone toll billing records, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized.

Subsection (b) requires government agencies installing and using pen register devices to use, <u>when reasonably available</u>, technology that restricts the information captured by such device to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured.

EXHIBIT 3

Excerpts from House Report accompanying CALEA
(pertinent portions in **bold**)

H.R. REP. 103-827(I)
H.R. REP. 103-827(I), H.R. Rep. No. 827(I), 103RD Cong., 2ND Sess. 1994, 1994 U.S.C.C.A.N. 3489, 1994 WL 557197 (Leg.Hist.)
(Cite as: H.R. REP. 103-827(I), 1994 U.S.C.C.A.N. 3489)

P.L. 103-414, **3489 *1 COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT

TELECOMMUNICATIONS CARRIER ASSISTANCE TO THE GOVERNMENT

DATES OF CONSIDERATION AND PASSAGE
House: October 4, 5, 1994
Senate: October 7, 1994
Cong. Record Vol. 140 (1994)
House Report (Judiciary Committee) No. 103-827,
Oct. 4, 1994 (To accompany H.R. 4922)
HOUSE REPORT NO. 103-827(I)
October 4, 1994
[To accompany H.R. 4922]

* * *

**3497 *17

* * *

THE LEGISLATION ADDRESSES PRIVACY CONCERNS

Since 1968, the law of this nation has authorized law enforcement agencies to conduct wiretaps pursuant to court order. That authority extends to voice, data, fax, E-mail and any other form of electronic communication. The bill will not expand that authority. However, as the potential intrusiveness of technology increases, it is necessary to ensure that government surveillance authority is clearly defined and appropriately limited.

In the eight years since the enactment of ECPA, society's patterns of using electronic communications technology have changed dramatically. Millions of people now have electronic mail addresses. Business, nonprofit organizations and political groups conduct their work over the Internet. Individuals maintain a wide range of relationships on-line. Transactional records documenting these activities and associations are generated by service providers. For those who increasingly use these services, this transactional data reveals a great deal about their private lives, all of it compiled in one place.

In addition, while the portion of cordless telephone communications occurring between the handset and base unit was excluded from ECPA's privacy protections, the 1991 Privacy and Technology Task Force found that "[t]he cordless phone, far from being a novelty item used only at 'poolside,' has become ubiquitous ... More and more communications are being carried out by people [using cordless phones] in private, in their homes and offices, with an expectation that such calls are just like any other phone call."

Therefore, H.R. 4922 includes provisions, which FBI Director Freeh supported in his testimony, that add protections to the exercise of the government's current surveillance authority. Specifically, the bill:

1. Eliminates the use of subpoenas to obtain E-mail addresses and other similar transactional data from electronic communications service providers. Currently, the government can obtain transactional logs containing a person's entire on-line profile merely upon presentation of an administrative subpoena issued by an investigator without any judicial intervention. Under H.R. 4922, a court order would be required.

2. Expressly provides that the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number. Currently, in

some cellular systems, transactional data that could be obtained by a pen register may include location information. **Further, the bill requires law enforcement to use reasonably available technology to minimize information obtained through pen registers.**

* * *

**3511 *31 SECTIONS 6 AND 7.-RADIO-BASED COMMUNICATIONS

* * *

SECTION 10.-TRANSACTIONAL DATA

Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers, subsection (a) eliminates the use of a subpoena by law enforcement to obtain from a provider of electronic communication services the addresses on electronic messages. In order for law enforcement to obtain such information, a court order is required.

This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the **3512 *32 records are relevant and material to an ongoing criminal investigation.

Law enforcement could still use a subpoena to obtain the name, address, telephone toll billing records, and length of service of a subscriber to or customer of such service and the types of services the subscriber or customer utilized.

Subsection (b) requires government agencies installing and using pen register devices to use, when reasonably available, technology that restricts the information captured by such device to the dialing or signaling information necessary to direct or process a call, excluding any further communication conducted through the use of dialed digits that would otherwise be captured.

EXHIBIT 4

Excerpts from Senator Leahy's 10/25/01 statement introducing USA Patriot Act of 2001

BLUE HIGHLIGHT = Quoted in Houston Decision

PURPLE HIGHLIGHT = Cited in Houston case by government

RED HIGHLIGHT = Not quoted or discussed in Houston Decision

CONGRESSIONAL RECORD -- SENATE

Thursday, October 25, 2001

107th Congress, 1st Session

147 Cong Rec S 10990

REFERENCE: Vol. 147, No. 144

SECTION: Senate

TITLE: USA PATRIOT ACT OF 2001

*S10999 . . .

There is consensus that the existing legal procedures for pen register and trap-and-trace authority are antiquated and need to be updated. I have been proposing ways to update the pen register and trap and trace statutes for several years, but not necessarily in the same ways as the Administration initially proposed. In fact, in 1998, I introduced with then-Senator Ashcroft, the E-PRIVACY Act, S. 2067, which proposed changes in the pen register laws. In 1999, I introduced the E-RIGHTS Act, S. 934, also with proposals to update the pen register laws.

Again, in the last Congress, I introduced the Internet Security Act, S. 2430, on April 13, 2000, that proposed: 1, changing the pen register and trap and trace device law to give nationwide effect to pen register and trap and trace orders obtained by Government attorneys and obviate the need to obtain identical orders in multiple Federal jurisdictions; 2, clarifying that such devices can be used for computer transmissions to obtain electronic addresses, not just on telephone lines; and 3, as a guard against abuse, providing for meaningful judicial review of government attorney applications for pen registers and trap and trace devices.

As the outline of my earlier legislation suggests, I have long supported modernizing the pen register and trap and trace device laws by modifying the statutory language to cover the use of these orders on computer transmissions; to remove the jurisdictional limits on service of these orders; and to update the judicial review procedure, which, unlike any other area in criminal procedure, bars the exercise of judicial discretion in reviewing the justification for the order. The USA Act, in section 216, updates the pen register and trap and trace laws only in two out of three respects I believe are important, and without allowing meaningful judicial review. Yet, we were able to improve the Administration's initial proposal, which suffered from the

same problems as the provision that was hastily taken up and passed by the Senate, by voice vote, on September, 13, 2001, as an amendment to the Commerce Justice State Appropriations Act.

The existing legal procedures for pen register and trap-and-trace authority require service of individual orders for installation of pen register or trap and trace device on the service providers that carried the targeted communications. Deregulation of the telecommunications industry has had the consequence that one communication may be carried by multiple providers. For example, a telephone call may be carried by a competitive local exchange carrier, which passes it at a switch to a local Bell Operating Company, which passes it to a long distance carrier, which hands it to an incumbent local exchange carrier elsewhere in the U.S., which in turn may finally hand it to a cellular carrier. If these carriers do not pass source information with each call, identifying that source may require compelling information from a host of providers located throughout the country.

Under present law, a court may only authorize the installation of a pen register or trap device "within the jurisdiction of the court." As a result, when one provider indicates that the source of a communication is a carrier in another district, a second order may be necessary. The Department of Justice has advised, for example, that in 1996, a hacker (who later turned out to be launching his attacks from a foreign country) extensively penetrated computers belonging to the Department of Defense. This hacker was dialing into a computer at Harvard University and used this computer as an intermediate staging point in an effort to conceal his location and identity. Investigators obtained a trap and trace order instructing the phone company, Nynex, to trace these calls, but Nynex could only report that the communications were coming to it from a long-distance carrier, MCI. Investigators then applied for a court order to obtain the connection information from MCI, but since the hacker was no longer actually using the connection, MCI could not identify its source. Only if the investigators could have served MCI with a trap and trace order while the hacker was actively on-line could they have successfully traced back and located him.

In another example provided by the Department of Justice, investigators encountered similar difficulties in attempting to track Kevin Mitnick, a criminal who continued to hack into computers attached to the Internet despite the fact that he was on supervised release for a prior computer crime conviction. The FBI attempted to trace these electronic communications while they were in progress. In order to evade arrest, however, Mitnick moved around the country and used cloned cellular phones and other evasive techniques. His hacking attacks would often pass through one of two cellular carriers, a local phone company, and then two Internet service providers. In this situation, where investigators and service providers had to act quickly to trace Mitnick in the act of hacking, only many repeated attempts_accompanied by an order to each service provider_finally produced success. Fortunately, Mitnick was such a persistent hacker that he gave law enforcement many chances to complete the trace.

This duplicative process of obtaining a separate order for each link in the communications chain can be quite time-consuming, and it serves no useful purpose since the original court has already authorized the trace. Moreover, a second or third order addressed to a particular carrier that carried part of a prior communication may prove useless during the next attack: in computer intrusion cases, for example, the target may use an entirely different path (i.e., utilize a different set of intermediate providers) for his or her subsequent activity.

The bill would modify the pen register and trap and trace statutes to allow for nationwide service of a single order for installation of these devices,

without the necessity of returning to court for each new carrier. I support this change.

The language of the existing statute is hopelessly out of date and speaks of a pen register or trap and trace "device" being "attached" to a telephone "line." However, the rapid computerization of the telephone system has changed the tracing process. No longer are such functions normally accomplished by physical hardware components attached to telephone lines. Instead, these functions are typically performed by computerized collection and retention of call routing information passing through a communications system.

The statute's definition of a "pen register" as a "device" that is "attached" to a particular "telephone line" is particularly obsolete when applied to the wireless portion of a cellular phone call, which has no line to which anything can be attached. While courts have authorized pen register orders for wireless phones based on the [*S11000] notion of obtaining access to a "virtual line," updating the law to keep pace with current technology is a better course.

Moreover, the statute is ill-equipped to facilitate the tracing of communications that take place over the Internet. For example, the pen register definition refers to telephone "numbers" rather than the broader concept of a user's communications account. Although pen register and trap orders have been obtained for activity on computer networks, Internet service providers have challenged the application of the statute to electronic communications, frustrating legitimate investigations. I have long supported updating the statute by removing words such as "numbers . . . dialed" that do not apply to the way that pen/trap devices are used and to clarify the statute's proper application to tracing communications in an electronic environment, but in a manner that is technology neutral and does not capture the content of communications. That being said, I have been 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.

The Administration's initial pen/trap device proposal added the terms "routing" and "addressing" to the definitions describing the information that was authorized for interception on the low relevance standard under these laws. The Administration and the Department of Justice flatly rejected my suggestion that these terms be defined to respond to concerns that the new terms might encompass matter considered content, which may be captured only upon a showing of probable cause, not the mere relevancy of the pen/trap statute. Instead, 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. 2510(8).

While this is an improvement, the FBI and Justice Department are short-sighted in their refusal to define these terms. We should be clear about the consequence of not providing definitions for these new terms in the pen/trap device statutes. These terms will be defined, if not by the Congress, then by the courts in the context of criminal cases where pen/trap devices have been used and challenged by defendants. If a court determines that a pen register has captured " content, " **which the FBI admits such devices do**, in violation of the Fourth Amendment, suppression may be ordered, not only of the pen register evidence by any other evidence derived from it. We are leaving the courts with little or no guidance of what is covered by "addressing" or "routing."

The USA Act also requires the government to use reasonably available technology that limits the interceptions under the pen/trap device laws "so as

not to include the contents of any wire or electronic communications." This **limitation on the technology used by the government to execute pen/trap orders is important** since, as the FBI advised me in June 2000, pen register devices "do capture all electronic impulses transmitted by the facility on which they are attached, including such impulses transmitted after a phone call is connected to the called party." The impulses made after the call is connected could reflect the electronic banking transactions a caller makes, or the electronic ordering from a catalogue that a customer makes over the telephone, or the electronic ordering of a prescription drug.

This transactional data intercepted after the call is connected is " content. " As the Justice Department explained in a May 1998 letter to then-House Judiciary Committee Chairman Henry Hyde, "the retrieval of the electronic impulses that a caller necessarily generated in attempting to direct the phone call" does not constitute a "search" requiring probable cause since "no part of the substantive information transmitted after the caller had reached the called party" is obtained. But the Justice Department made clear that "all of the information transmitted after a phone call is connected to the called party . . . is substantive in nature. These electronic impulses are the contents' of the call: They are not used to direct or process the call, but instead convey certain messages to the recipient."

When I added the direction on use of reasonably available technology (codified as 18 U.S.C. 3121(c)) to the pen register statute as part of the Communications Assistance for Law Enforcement Act (CALEA) in 1994, I recognized that these devices collected content and that such collection was unconstitutional on the mere relevance standard. Nevertheless, the FBI advised me in June 2000, that pen register devices for telephone services "continue to operate as they have for decades" and that "there has been no change . . . that **would better restrict the recording or decoding** of electronic or other impulses to the dialing and signaling information utilized in call processing." Perhaps, **if there were meaningful judicial review and accountability, the FBI would take the statutory direction more seriously and actually implement it.**

Due in significant part to the fact that pen/trap devices in use today collect " content, " I have sought in legislation introduced over the past few years to update **and modify** the judicial review procedure for pen register and trap and trace devices. Existing law requires an attorney for the government to certify that the information likely to be obtained by the installation of a pen register or trap and trace device will be relevant to an ongoing criminal investigation. The court is required to issue an order upon seeing the prosecutor's certification. The court is not authorized to look behind the certification to evaluate the judgement of the prosecutor.

I have urged that government attorneys be required to include facts about their investigations in their applications for pen/trap orders and allow courts to grant such orders only where the facts support the relevancy of the information likely to be obtained by the orders. This is not a change in the applicable standard, which would remain the very low relevancy standard. Instead, this change would simply allow the court to evaluate the facts presented by a prosecutor, and, if it finds that the facts support the government's assertion that the information to be collected will be relevant, issue the order. Although this change will place an additional burden on law enforcement, it will allow the courts a greater ability to assure that government attorneys are using such orders properly.

Some have called this change a "roll-back" in the statute, as if the concept of allowing meaningful judicial review was an extreme position. To the contrary, this is a change that the Clinton Administration supported in legislation transmitted to the Congress last year. This is a change that the

House Judiciary Committee also supported last year. In the Electronic Communications Privacy Act, H.R. 5018, that Committee proposed that before a pen/trap device "could be ordered installed, the government must first demonstrate to an independent judge that specific and articulable facts reasonably indicate that a crime has been, is being, or will be committed, and information likely to be obtained by such installation and use . . . is relevant to an investigation of that crime." (Report 106-932, 106th Cong. 2d Sess., Oct. 4, 2000, p. 13). Unfortunately, the Bush Administration has taken a contrary position and has rejected this change in the judicial review process.

EXCERPT BREAK

[*S11006]

Sec. 216. Modification of authorities relating to use of pen registers and trap and trace devices. Both the House and Senate bills included this provision to authorize courts to grant pen register and trap and trace orders that are valid anywhere in the nation. It also ensures that the pen register and trap and trace provisions apply to facilities other than telephone lines (e.g., the Internet). It specifically provides, however, that the grant of authority to capture "routing" and [*S11007] "addressing" information for Internet users does not authorize the interception of the content of any such communications. It further requires the government to use the latest available technology to insure that a pen register or trap and trace device does not intercept the content of any communications. Finally, it provides for a report to the court on each use of "Carnivore"-like devices on packet-switched data networks. Makes a number of improvements over Administration proposal, including exclusion of content, exclusion of ISP liability, and Carnivore report.

EXCERPT BREAK

Mr. LEAHY. After that terrible day of September 11, we began looking at our laws, and what we might do. Unfortunately, at first, rhetoric overcame reality. We had a proposal sent up, and we were asked to pass it within a day or so. Fortunately for the country, and actually ironically beneficial to both the President and the Attorney General who asked for such legislation, we took time to look at it, we took time to read it, and we took time to remove those parts that were unconstitutional and those parts that would have actually hurt liberties of all Americans.

I say that because I think of what Benjamin Franklin was quoted as saying at a time when he literally had his neck on the line, where he would have been hanged if our revolution had failed. He said: A people who would give up their liberty for security deserve neither.

What we have tried to do in this legislation is to balance the liberties we enjoy as Americans and those liberties that have made us the greatest democracy in history but at the same time to enhance our security so we can maintain that democracy and maintain the leadership we have given the rest of the world.

We completed our work 6 weeks after the September 11 attacks. I compare this to what happened after the bombing of the Federal Building in Oklahoma City in 1995. It took a year to complete the legislation after that. We have done this in 6 weeks. But there has been a lot of cooperation. There have been a lot of Senators and a lot of House Members in both parties and dedicated staff who have worked around the clock.

I think of my own staff_and this could be said of many others, including the Presiding Officer's staff and the ranking member's staff_who were forced out of their offices because of the recent scares on Capitol Hill, and they continue to work literally in phone booths and in hallways and from their homes and off laptops and cell phones.

I made a joke in my own hide-away office. To those who have ever watched "The X-Files," there is a group called "the lone gunmen," who are sort of these computer nerds who meet in a small house trailer. I am seeing some puzzled looks around the Senate as I say this. But they have all these wires hanging from the ceiling and laptops and all, and they do great things. That is the way our office looked. But they were working around the clock on this legislation to get something better. There was some unfortunate rhetoric along the way, but again, the reality overcame it. We have a good piece of legislation.

As we look back to when we began discussions with the administration about this bill, there were sound and legitimate concerns on both sides of the Capitol, both sides of the aisle, about the legislation's implication for America's rights and freedoms. There was also a sincere and committed belief that we needed to find a way to give law enforcement authority new tools in fighting terrorism.

This is a whole new world. It is not similar to the days of the cold war where we worried about armies marching against us or air forces flying against us or navies sailing against us. This is not that world. Nobody is going to do that because we are far too powerful. Since the end of the cold war, with the strength of our military, nobody is going to do a frontal attack. But as the Presiding Officer and everyone else knows, a small dedicated group of terrorists, with state-supported efforts, can wreak havoc in an open and democratic Nation such as ours.

Anybody who has visited the sites of these tragedies doesn't need to be told the results. We know our Nation by its very nature will always be vulnerable to these types of attacks. None of us serving in the Senate today will, throughout our service, no matter how long it is, see a day where we are totally free of such terrorist attacks. That is the sad truth. Our children and our grandchildren will face the possibilities of such terrorist attacks because that is the only way the United States can be attacked. But that doesn't mean we are defenseless. It doesn't mean we suddenly surrender. [*S11015]

We have the ability, with our intelligence agencies and our law enforcement, to seek out and stop people before this happens. We are in an open session today, so I won't go into the number of times we have done that. But in the last 10 years, we have had, time and time again, during the former Bush administration, during the Clinton administration, and in the present administration, potential terrorist attacks thwarted. People have either been apprehended or eliminated.

Everybody in America knows our life has changed. Whether the security checks and the changes in our airlines are effective or not, we know they are reality. We know travel is not as easy as it once was. We will be concerned about opening mail. We will worry when we hear the sirens in the night. But we are not going to retreat into fortress America. We are going to remain a beacon of democracy to the rest of the world. Americans don't run and hide. Americans face up, as we have, to adversities, whether they be economic or wars or anything else.

We began this process knowing how we had to protect Americans. It was not

that we were intending to see how much we could take out of the administration's proposal, but it was with a determination to find sensible, workable ways to do the same things to protect America the administration wanted but with checks and balances against abuse. We have seen at different times in this Nation's history how good intentions can be abused. We saw it during the McCarthy era.

Following the death of J. Edgar Hoover, we found how much totalitarian control of the FBI hurt so many innocent people without enhancing our security. We saw it during the excesses of the special prosecutor law enacted with good intentions.

We wanted to find checks and balances. We wanted to make sure we could go after terrorism. We wanted to make sure we could go after those who would injure our society, those who would strike at the very democratic principles that ironically make us a target. But we wanted to do it with checks and balances against abuse. That is what we did. In provision after provision, we added those safeguards that were missing from the administration's plan.

By taking the time to read and improve the antiterrorism bill, Congress has done the administration a great favor in correcting the problems that were there. We have used the time wisely. We have produced a far better bill than the administration proposed. Actually, it is a better bill than either this body or the House initially proposed. The total is actually greater than the sum of the parts.

We have done our utmost to protect Americans against abuse of these new law enforcement tools, and there are new law enforcement tools involved. In granting these new powers, the American people but also we, their representatives in Congress, grant the administration our trust that they are not going to be misused. It is a two-way street. We are giving powers to the administration; we will have to extend some trust that they are not going to be misused.

The way we guarantee that is congressional oversight. Congressional oversight is going to be crucial in enforcing this compact. If I might paraphrase former President Reagan: We will entrust but with oversight.

We will do this. The Republican chairman and his ranking member in the House of Representatives intend to have very close oversight. I can assure you that I and our ranking member will have tight oversight in the Senate.

Interestingly enough, the 4-year sunset provision included in this final agreement will be an enforcement mechanism for adequate oversight.

We did not have a sunset provision in the Senate bill. The House included a 5-year provision. The administration wanted even 10 years. We compromised on 4. It makes sense. It makes sense because with everybody knowing there is that sunset provision, everybody knows they are going to have to use these powers carefully and in the best way. If they do that, then they can have extensions. If they don't, they won't. It also enhances our power for oversight.

This is not precisely the bill that Senator Hatch would have written. It is not precisely the bill I would have written, or not precisely the bill the Presiding Officer or others on the floor would have written. But it is a good bill. It is a balanced bill. It is a greatly improved piece of legislation. It is one that sets up the checks and balances necessary in a democratic society that allow us to protect and preserve our security but also protect and preserve our liberties.

I reserve the remainder of my time.

END OF EXCERPTS

EXHIBIT 5

October 11, 2001 Statements of Senators Hatch and Feinstein
(Pertinent portions in **bold**)

CONGRESSIONAL RECORD -- SENATE

Thursday, October 11, 2001

107th Congress, 1st Session

147 Cong Rec S 10547

REFERENCE: Vol. 147, No. 136

SECTION: Senate

TITLE: UNITING AND STRENGTHENING AMERICA ACT

SPEAKER: Mr. LEAHY; Mr. LEAHY. ; Mr. HATCH; Mr. SARBANES; Mr. REID; Mr. GRAHAM; Mr. SPECTER; Mr. FEINGOLD; Ms. CANTWELL; Mr. WELLSTONE; Mr. DURBIN. ; Mr. DASCHLE; Mr. KERRY; Mr. KERRY. ; Mr. LEVIN; Mr. STEVENS; Mr. SMITH of New Hampshire; Mr. SCHUMER; Mr. CORZINE; Mr. EDWARDS; Mr. KYL; Mrs. FEINSTEIN; Mr. ENZI; Mr. KOHL; Ms. SNOWE; Mr. KENNEDY

TEXT: [*S10547]

The PRESIDING OFFICER. The clerk will report the bill by title.

The legislative clerk read as follows:

A bill (S. 1510) to deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.

EXCERPT BREAK

[At *S10561]

The PRESIDING OFFICER. Who yields time?

The Senator from Utah.

Mr. HATCH . Mr. President, I enjoyed the remarks of my distinguished colleague from Vermont. I compliment him for the work he has done on this bill and for the hard work, over the last 3 weeks, that he and his staff have put into this bill, as well as other members of the Judiciary Committee as a whole, and, of course, people on my side as well.

Mr. President, I do not intend to take very long. I know our colleagues are tired, and I know they would like to go home. I also know that we have a distinguished colleague in the Chamber who has some amendments on which we may have to vote.

Four weeks ago we were a relatively tranquil nation, but on September 11, in what amounted to a dastardly attack, an unprovoked attack of war, the World

Trade Center was destroyed, along with almost 6,000 people, or maybe more. Our Pentagon was struck by a volitionary act of terrorism.

As a result of the acts of heroes, one of the planes was downed in Pennsylvania, killing all aboard, including those heroes who made sure that that plane did not strike either the Capitol or the White House. I want to pay special tribute to those people who were so heroic as to give up their own lives to protect the lives of so many others.

There have been so many acts of heroism and self-sacrifice_the firefighters who gave their lives, the firefighters who worked day and night, the volunteers who have gone in there, the mayor of New York City, the Governor, and so many others who deserve mention.

This bill, hopefully, will help to at least rectify and redeem some of the problems, problems that have existed ever since September 11.

We did not seek this war; it was thrust upon us. It was an unprovoked attack by people who claim that they represent a religious point of view when, in fact, what they represent is a complete distortion of the religion of Islam.

Islamic people do not believe in murder, murdering innocent civilians. The Koran does not teach that. They do not believe in suicide. The Koran does not teach that.

This is not a war against Islam; this is a war against terrorism and people who have so little regard for human life that they would do something against innocent civilians that was unthinkable before September 11.

Therefore, we live in a dangerous and difficult world today. It is a different world. And we are going to have to wake up and do the things we have to do to protect our citizenry and, of course, to protect the rest of the world to the extent this great Nation can, with the help of other nations, a number of which have become supportive of our efforts. We are very grateful to them.

But a lot of people do not realize we have terror cells in this country_that has been in the media even_and there are people in this country who are dedicated to the overthrow of America. There are people who are dedicated to terrorism right here within our Nation. And some of these people who have participated in this matter may very well be people who were rightfully in our Nation_or at least we thought were rightfully in our Nation.

The responsibility of redeeming and rectifying this situation is the responsibility of the Congress, the Justice Department, the FBI, the INS, and the Border Patrol. It is our job to provide the tools, and for them to first identify and then eradicate terrorist activity within our borders. And our President has taken the extraordinary step of saying we are going to go after terrorists worldwide and those who harbor them.

I agree with the President. I think it is time to do it. It is time to hit them where it hurts. It is time to let them know we are not going to put up with this type of activity.

A few weeks ago, the Justice Department sent up its legislative proposal. It [*S10560]
was a good legislative proposal. They had a lot of ideas in there that literally we have been trying to get through for years. When we passed the 1996 antiterrorism, effective death penalty act, a number of us tried to get

some of these provisions in at that time, but we were unsuccessful for a variety of reasons, some very sincere.

The fact is, a lot of the provisions we have in the bill are not brand new; a lot of them have been requested for years. And had they been in play, who knows but we might have been able to interdict these terrorists and have stopped what happened and have stopped the loss of civil liberties for approximately 6,000 or more people.

In the past several weeks, after the Justice Department sent up its bill, Senator Leahy and I, Justice Department officials, White House officials, staff members from both of our staffs, and staff members from other members of the committee have worked day and night to come up with this particular bill.

I congratulate my partner and my colleague, Senator Leahy, for his hard work on this bill, and his staffers' for the work they have done on this bill, and, of course, my own staffers, and, of course, those others I have named.

This has been a very difficult bill to put forward because there are all kinds of cross-pressures, all kinds of ideas, all kinds of different thoughts, all kinds of differing philosophies. We believe, with all kinds of deliberation and work, we have been able to put together a bill that really makes sense, that will give the Justice Department the tools it needs to be able to work and stamp out terrorist activity within our country. At least we want to give them the very best tools we possibly can.

We have tried to accommodate the concerns of Senators on both sides of the aisle. We have worked very hard to do so. We cannot accommodate everybody's concerns. As Senator Leahy has said, this is not a perfect bill. Nothing ever seems to be perfect around here. But this is as good a bill as can be put together, in a bipartisan way, in this area in the history of the Senate. I really feel good about it, that we have done this type of a job.

As I say, a lot of these provisions have been requested by the Justice Department and both Democrat and Republican White Houses for years. We took into consideration civil liberties throughout our discussions on this bill. I think we got it just right. We are protective of civil liberties while at the same time giving the tools to the law enforcement agencies to be able to do their jobs in this country.

I might mention that this bill encourages information sharing, that would be absolutely prohibited under current law, among various agencies of Government, information sharing that should have been allowed a long time ago, at least in my view.

It updates the laws with regard to electronic surveillance and brings those laws into the digital age, and brings them into an effective way so that we can, in a modernized way, protect our society, at least to the extent we can, from these types of terrorist activities.

Of course, little things, such as pen registers, trap-and-trace authority_we have been able to resolve these problems after years of problems.

I would like to make a few comments regarding the process for this legislation. Although we have considered this in a more expedited manner than other legislation, my colleagues can be assured that this bill has received thorough consideration. First, the fact is that the bulk of these proposals have been requested by the Department of Justice for years, and have languished in Congress for years because we have been unable to muster the collective political will to enact them into law.

No one can say whether these tools could have prevented the attacks of September 11. But, as the Attorney General has said, it is certain that without these tools, we did not stop the vicious acts of last month. I say to my colleagues, Mr. President, that if these tools could help us now to track down the perpetrators if they will help us in our continued pursuit of terrorist activities within our national borders then we should not hesitate any further to pass these reforms into law. As long as these reforms are consistent with our Constitution and they are it is difficult to see why anyone would oppose their passage.

Furthermore, I would like to clearly dispel the myth that the reforms in this legislation somehow abridge the Constitutional freedoms enjoyed by law-abiding American citizens. Some press reports have portrayed this issue as a choice between individual liberties on the one hand, and on the other hand, enhanced powers for our law enforcement institutions. This is a false dichotomy. We should all take comfort that the reforms in this bill are primarily directed at allowing law enforcement agents to work smarter and more efficiently in no case do they curtail the precious civil liberties protected by our Constitution. I want to assure my colleagues that we worked very hard over the past several weeks to ensure that this legislation upholds all of the constitutional freedoms our citizens cherish. It does.

Mr. President, I will submit for the Record my extended remarks describing this legislation, but I would like to take a minute to explain briefly a few of the most important provisions of this critical legislation.

First, the legislation encourages information-sharing between various arms of the federal government. I believe most of our citizens would be shocked to learn that, even if certain government agents had prior knowledge of the September 11 attacks, under many circumstances they would have been prohibited by law from sharing that information with the appropriate intelligence or national security authorities.

This legislation makes sure that, in the future, such information flows freely within the Federal government, so that it will be received by those responsible for protecting against terrorist attacks.

By making these reforms, we are rejecting the outdated Cold War paradigm that has prevented cooperation between our intelligence community and our law enforcement agents. Current law does not adequately allow for such cooperation, artificially hampering our government's ability to identify and prevent acts of terrorism against our citizens.

In this new war, terrorists are a hybrid between domestic criminals and international agents. We must lower the barriers that discourage our law enforcement and intelligence agencies from working together to stop these terrorists. These hybrid criminals call for new, hybrid tools.

Second, this bill updates the laws relating to electronic surveillance. Electronic surveillance, conducted under the supervision of a federal judge, is one of the most powerful tools at the disposal of our law enforcement community. It is simply a disgrace that we have not acted to modernize the laws currently on the books which govern such surveillance, laws that were enacted before the fax machine came into common usage, and well before the advent of cellular telephones, e-mail, and instant messaging. The Department of Justice has asked us for years to update these laws to reflect the new technologies, but there has always been a call to go slow, to seek more information, to order further studies.

This is no hypothetical problem. We now know that e-mail, cellular telephones, and the Internet have been principal tools used by the terrorists

to coordinate their atrocious activities. We need to pursue all solid investigatory leads that exist right now that our law enforcement agents would be unable to pursue because they must continue to work within these outdated laws. It is high time that we update our laws so that our law enforcement agencies can deal with the world as it is, rather than the world as it existed 20 years ago.

A good example of way we our handicapping our law enforcement agencies relates to devices called "pen registers." Pen registers may be employed by the FBI, after obtaining a court order, to determine what telephone numbers are being dialed from a particular telephone. These devices are essential investigatory tools, which allow law enforcement agents to determine who is speaking to whom, within a criminal conspiracy.

The Supreme Court has held, in Smith v. Maryland, that the information obtained by pen register devices is not information that is subject to any constitutional protection. Unlike the content of your telephone conversation
[*S1056]
once your call is connected, the numbers you dial into your telephone are not private. Because you have no reasonable expectation that such numbers will be kept private, they are not protected under the Constitution. The Smith holding was cited with approval by the Supreme Court just earlier this year.

The legislation under consideration today would make clear what the Federal courts have already ruled that Federal judges may grant pen register authority to the FBI to cover, not just telephones, but other more modern modes of communication such as e-mail or instant messaging. **Let me make clear that the bill does not allow law enforcement to receive the content of the communication, but they can receive the addressing information to identify the computer or computers a suspect is using to further his criminal activity.**

Importantly, reform of the pen register law does not allow as has sometimes been misreported in the press for law enforcement agents to view the content of any e-mail messages not even the subject line of e-mails. In addition, this legislation we are considering today makes it explicit that content can not be collected through such pen register orders.

This legislation also allows judges to enter pen register orders with nationwide scope. Nationwide jurisdiction for pen register orders makes common sense. It helps law enforcement agents efficiently identify communications facilities throughout the country, which greatly enhances the ability of law enforcement to identify quickly other members of a criminal organization, such as a terrorist cell.

Moreover, this legislation provides our intelligence community with the same authority to use pen register devices, under the auspices of the Foreign Intelligence Surveillance Act, that our law enforcement agents have when investigating criminal offenses. It simply makes sense to provide law enforcement with the same tools to catch terrorists that they already possess in connection with other criminal investigations, such as drug crimes or illegal gambling.

In addition to the pen register statute, this legislation updates other aspects of our wiretapping statutes. It is amazing that law enforcement agents do not currently have authority to seek wiretapping authority from a Federal judge when investigating a terrorist offense. This legislation fixes that problem.

Moving on, I note that much has been made of the complex immigration provisions of this bill. I know Senators Specter, Kohl and Kennedy had questions about earlier provisions, particularly the detention provision for

suspected alien terrorists.

I want to assure my colleagues that we have worked hard to address your concerns, and the concerns of the public. As with the other immigration provisions of this bill, we have made painstaking efforts to achieve this workable compromise.

Let me address some of the specific concerns. In response to the concern that the INS might detain a suspected terrorist indefinitely, the Senator Kennedy, Senator Kyl, and I worked out a compromise that limits the provision. It provides that the alien must be charged with an immigration or criminal violation within seven days after the commencement of detention or be released. In addition, contrary to what has been alleged, the certification itself is subject to judicial review. The Attorney General's power to detain a suspected terrorist under this bill is, then, not unfettered.

Moreover, Senator Leahy and I have also worked diligently to craft necessary language that provides for the deportation of those aliens who are representatives of organizations that endorse terrorist activity, those who use a position of prominence to endorse terrorist activity or persuade others to support terrorist activity, or those who provide material support to terrorist organizations. If we are to fight terrorism, we can not allow those who support terrorists to remain in our country. Also, I should note that we have worked hard to provide the State Department and the INS the tools they need to ensure that no applicant for admission who is a terrorist is able to secure entry into the United States through legal channels.

Finally, the bill gives law enforcement agencies powerful tools to attack the financial infrastructure of terrorism giving our Government the ability to choke off the financing that these dangerous terrorist organizations need to survive. It criminalizes the practice of harboring terrorists, and puts teeth in the laws against providing material support to terrorists and terrorist organizations. It gives the President expanded authority to freeze the assets of terrorists and terrorist organizations, and provides for the eventual seizure of such assets. These tools are vital to our ability to effectively wage the war against terrorism, and ultimately to win it.

There have been few, if any, times in our nation's great history where an event has brought home to so many of our citizens, so quickly, and in such a graphic fashion, a sense of our vulnerability to unexpected attack.

I believe we all took some comfort when President Bush promised us that our law enforcement institutions would have the tools necessary to protect us from the danger that we are only just beginning to perceive.

The Attorney General has told us what tools he needs. We have taken the time to review the problems with our current laws, and to reflect on their solutions. The time to act is now. Let us please move forward expeditiously, and give those who are in the business of protecting us the tools that they need to do the job.

Mr. President, I think most people understand this is an important bill. All of us understand it needs to be done. All of us understand that these are tools our law enforcement people deserve and need to have. And, frankly, it is a bill that I think can make a real difference with regard to the interdiction of future acts of terrorism in our society.

Nobody can guarantee, when you have people willing to commit suicide in the perpetration of these awful acts, at all times that we can absolutely protect our Nation. But this bill will provide the tools whereby we might be able_and in most cases should be able_to resolve even those types of problems.

So with that, I am happy to yield the floor.

EXCERPT BREAK

[AT S10691]

Mrs. FEINSTEIN . Mr. President, I rise in strong support of the consensus terrorism bill now on the floor of the U.S. Senate.

The people of the United States awoke on September 12 to a whole new world, one in which we can no longer feel safe within our borders. We awoke to a world in which our very way of life is under attack, and we have since resolved to fight back with every tool at our disposal.

This is an unprecedented state of affairs, and it demands unprecedented action. We must seek out and defeat individuals and groups who would build upon the September 11 attacks with more of their own. We simply must give law enforcement officials the tools they need to track, to hunt down, and to capture terrorists, both in this country, and around the world as well. And that is what this bill would do.

Let me just describe some of the key provisions of this legislation, and how those provisions will make an impact, even in the current investigation into the September 11 attacks.

First, this bill makes it easier to collect foreign intelligence information under the Foreign Intelligence Surveillance Act, FISA. Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence.

But in today's world things are not so simple. In many cases, surveillance will have two key goals_the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary" purpose of the investigation can be difficult, and will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.

Rather than forcing law enforcement to decide which purpose is primary_law enforcement or foreign intelligence gathering, this bill strikes a new balance. It will now require that a "significant" purpose of the investigation must be foreign intelligence gathering to proceed with surveillance under FISA.

The effect of this provision will be to make it easier for law enforcement to obtain a FISA search or surveillance warrant for those cases where the subject of the surveillance is both a potential source of valuable intelligence and the potential target of a criminal prosecution. Many of the individuals involved in supporting the September 11 attacks may well fall into both of these categories.

This language is a negotiated compromise between those who wished the law to stay the same, and those who wished to virtually eliminate the foreign intelligence standard entirely.

The administration originally proposed changing "primary purpose" to "a purpose," but when I questioned Attorney General Ashcroft at our Judiciary Committee hearing, he agreed that "significant purpose" would represent a good compromise.

Second, this legislation will provide multi-point authority, or so-called "roving wiretap authority" in foreign intelligence investigations. This provision is designed to defeat attempts to evade law enforcement by simply switching cell phones or moving locations.

Under current law, law enforcement must get a wiretap order for each individuals phone line. Criminals and terrorists know this, so they often manage to defeat surveillance by simply moving locations or exchanging countless disposable or even stolen cell phones.

This legislation will now allow the surveillance to follow the person, wherever or however that person is communicating. So, no longer will duplicative [*S10592]
wiretap orders be necessary simply to listen to the same, single target of an investigation. This is a powerful change to the law that does not put innocent conversations in danger, but stops the evasion of surveillance now possible under the law.

Third, this legislation allows nationwide service of so-called "pen register" and "trap and trace" orders. Those orders allow law enforcement to track incoming and outgoing phone calls, and now Internet addressing, so that the authorities can make connections between various criminals or terrorists.

The problem with current law is that it has not kept up with technology. Modern communications travel through many jurisdictions before reaching their final destinations, and current law requires court orders from every jurisdiction through which the communication travels.

Under this new legislation, only one court order will be necessary, eliminating the time-consuming and burdensome requirements now placed on law enforcement simply because technology has changed the way communications travel from one place to the other. Law enforcement resources should be spent in the field, not filing unnecessarily burdensome motions in courtroom after courtroom.

I should also mention one important point about this provision. The standard necessary to get a court-ordered pen register or trap and trace is lower than the standard necessary to get a wiretap, so it was very important to make sure that this legislation makes it clear that these orders do not allow law enforcement to eavesdrop on or read the content of communication. Only the origin and destination of the messages will be intercepted.

This legislation also authorizes the seizure of voice-mail messages pursuant to a probable cause warrant, which is an easier standard for law enforcement to meet than the standard required for a wiretap.

Current law treats a voice-mail like an ongoing oral communication, and requires law enforcement to obtain a wiretap order to seize and listen to those saved messages. E-mails, however, receive no similar protection. In my opinion, if law enforcement can access e-mail communications with probable cause, the same should be the case with voice-mails. And so it will be once this legislation passes.

This legislation will also now allow for limited sharing of grand jury and other criminal investigation information with the intelligence community, to assist in the prevention of terrorist acts and the apprehension of the terrorists themselves.

Under current law, law enforcement officials involved in a grand jury investigation cannot share information gathered in the grand jury with the intelligence community, even if that information would prevent a future

terrorist act.

Under this legislation, grand jury and other criminal investigative information can be shared if one, the information can is foreign intelligence and counterintelligence information, as defined by statute; two, the information is given to an official with a need to know in the performance of his or her official duties; and three, limitations on public or other unauthorized disclosure would remain in force.

This balance makes sense, I believe strongly that grand jury information should not be leaked to the public or disclosed haphazardly to anyone. But at the same time, it makes perfect sense to allow our own law enforcement officials to talk to each other about ongoing investigations, and to coordinate their efforts to capture terrorists wherever they may be.

This legislation also contains a heavily negotiated provision regarding the detention of aliens suspected of links to terrorism without charging them. Agreement was reached to one, limit to 7 days the length of time an alien may be held before being charged with criminal or immigration violations, two, allow the Attorney General to delegate the certification power only to the INS Commissioner, and three, specify that the merits of the certification is subject to judicial review.

This legislation also contains several key provisions from a bill I introduced last month with the chairman of the Intelligence Committee, Senator Graham. For instance, the bill: Clarifies the role of the CIA director as the coordinator of strategies and priorities for how the government uses its limited surveillance resources; requires that law enforcement officers who discover foreign intelligence information in the course of a criminal investigation share that information with the intelligence community; includes "international terrorist activities" in the definition of "foreign intelligence" to clarify the authorities of the CIA; includes a sense of Congress that the CIA should make efforts to recruit informants in the fight against terrorism, even if some of those informants may, as is likely the case, not be ideal citizens; requires a report from the CIA on the feasibility of establishing a virtual translation center for use by the intelligence community, so that translators around the country can assist in investigations taking place far, far away. For instance, this center would allow a translator living in Los Angeles to assist law enforcement in New York without even leaving California; and finally, agreement was reached to require the Attorney General, in consultation with the CIA Director, to provide training to federal, state and local government officials to identify foreign intelligence information obtained in the course of their duties.

In addition, this bill also: Triples the number of Border Patrol, Customs Service, and INS inspectors at the northern border; authorizes $50 million to improve INS and Customs technology for monitoring the northern border and to add equipment on the border; lifts the statute of limitations on terrorist acts as defined by law where those crimes resulted in, or created a risk of, death or serious bodily injury. These crimes include bio-terrorism, attacks against airports or airplanes, arson or bombings of U.S. facilities, and other terrorist acts; adds this same list of terrorist crimes certain as predicates for RICO and money laundering; creates two new bio-terrorism crimes, the first prohibits certain restricted persons, including nonresident aliens from countries that support terrorism, from possessing a listed biological agent or toxin; and the second prohibits any person from possessing a biological agent, toxin, or delivery system of a type or in a quantity that, under the circumstances, is not reasonably justified by a peaceful purpose.

The Attorney General and the President of the United States have asked this Congress to give them legislation that will assist in the war against

terrorism, and I am one who believes very strongly that we should do so, and we should do so quickly.

This bill is a product of intense negotiations, and I believe that a good balance has been struck here. Compromises have been reached on the most controversial provisions, roving wiretap authority; trap and trace of computer routing information; sharing of grand jury information; and mandatory detention of aliens suspected of terrorism.

Although I no longer believe it to be necessary now that these compromises have been reached, I would support a five-year sunset on the provisions I just mentioned as a valuable check on the potential abuse of the new powers granted in the bill.

But a two-year sunset, such as the one contained in the House bill, is simply too short to allow law enforcement to accomplish what it needs to do to rout terrorists from this country.

The legislation before us contains provisions that could actually help in the current investigation into Osama bin Laden and his network in the United States and abroad.

I urge this Senate to pass this legislation and get it to the President for his signature. We are in a sustained war against terror, and we have waited long enough.