



U.S. Department of Justice

*United States Attorney
Eastern District of New York*

156 Pierrepont Street

Brooklyn, New York 11201

*Mailing Address: 147 Pierrepont Street
Brooklyn, New York 11201*

May 18, 2007

The Honorable Joan M. Azrack
United States Magistrate Judge
Eastern District of New York
225 Cadman Plaza East
Brooklyn, New York 11215

Re: Applications And Orders For
Pen Registers/Trap and Trace Devices
(Post-cut-through Dialed Digit Litigation)
Docket Nos. 06-MC-547 and 06-MC 561 (JMA)

Dear Magistrate Judge Azrack:

The government respectfully writes in reply to the memorandum ("Amicus Mem.") submitted by amicus curiae Federal Defenders of New York ("amicus"). As further detailed below, amicus' arguments opposing the above applications to record and decode post-cut-through dialed digits ("PCTDD") via pen register¹ are without merit. The applications should accordingly be granted.

A. Preliminary Statement

Since 1994, 18 U.S.C. § 3121(c) has permitted the government to record and decode (but not to use) PCTDD content when there is no "technology reasonably available to" the government to prevent such an occurrence incidental to the

¹ This submission uses and assumes familiarity with the terminology and definitions used in our previous submissions in the above cases.

collection of PCTDD non-content. 18 U.S.C. § 3121(c). In 57 pages of argument, however, amicus make no real attempt to explain how § 3121(c)'s "technology reasonably available" clause can be given effect if, as amicus insists, the definition of a "pen register" under 18 U.S.C. § 3127(3) as amended in 2001 must be construed to impose a blanket proscription on any pen registers collecting content.

This silence, together with amicus' determined refusal to engage the legislative history fatally undermine its arguments. This is so, whether or not 18 U.S.C. § 3127(3) is construed completely to ban a pen register accessing content. If as we maintain, amended § 3127(3) is also susceptible to an interpretation that merely excludes a device from the definition of "pen register" at any moment that it accessing content rather than non-content, the canons of construction require resolving any ambiguity in favor of that construction. For in contrast to an interpretation requiring a flat ban, it gives effect to § 3121(c)'s "technology reasonably available clause" and avoids implying that clause to have been repealed by the 2001 amendment to § 3127(3) when the two are not in irreconcilable conflict.

Moreover, were it true that the text of § 3121(c) and § 3127(3) facially conflict, that would justify the use of legislative history to dispel it that supports the government's position. As demonstrated in our opening brief (at 22-32), the legislative history of § 3121(c) as originally enacted in 1994 and of both § 3121(c) and § 3127(3) as amended in 2001 establish that since 1994, the Pen/Trap Statute has conditioned the government's obligation to avoid incidental access on whether there is technology reasonably available to do so. Amicus contends otherwise only by ignoring what Senator Leahy, a primary drafter of both provisions, actually said in 1994 and as well in 2001.

B. Amicus Misconstrues § 3121(c)

Amicus repeatedly asserts (at 15-20 and again at 32-39) that as they were amended in 2001, (a) 18 U.S.C. § 3127(3) imposes an absolute ban on any "pen register," as that provision defines it, being used to obtain content, and (b) § 3127(3)'s ban is complemented by a clause added to 18 U.S.C. § 3121(c) "exhorting" the Executive Branch to comply with the prohibition allegedly contained in 18 U.S.C. § 3127(3).

These claims are at odds with the plain words of 18 U.S.C. § 3121(c). In its current form, the statute reads:

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

18 U.S.C. § 3121(c)) (emphasis added). The first underlined passage has been part of the statute since 1994; the second was added in 2001 as part of the Patriot Act. As previously explained, the first passage conditions the government's obligation to avoid incidental access to content on whether there exists "technology reasonably available to" the government to filter content from non-content. When the government uses what technology is reasonably available to it to filter content, § 3121(c) permits a pen register incidentally to access the remainder that the technology cannot avoid. See Government Opening Mem. at 13-14. Moreover, the second passage is entirely congruent with the first. The second passage describes § 3121(c)'s tendency when "technology [is] reasonably available" to avoid incidental access to content, i.e., in such circumstances, the statute tends "to [ex]clude . . . contents." See Government Opening Mem. at 12-13.

Thus, neither passage supports amicus' claim that § 3121(c) "exhor[ts]" the government "to comply with the ban on content acquisition" that amicus purports to locate in § 3127(3). Amicus Mem. at 32. Rather, the government's obligation under § 3121(c) to avoid accessing content is conditioned on whether and what technology is "reasonably available," rather than being defined as absolute and without regard to technological capability. Had Congress in 2001 actually intended to conform § 3121(c) to an outright ban on access to content added elsewhere in the Pen/Trap Statute, it would have had no choice but to strike the "technology reasonably available" clause and instead direct the government without exception to limit the information collected by pen register to "recording or decoding . . . dialing, routing, addressing, and signaling information." At the same time, Congress would not have described the object of § 3121(c) as a mere tendency ("so as not to include. . . content"), but rather, as an imperative (e.g., "the government shall restrict any pen register to recording or decoding dialing, routing, addressing, and signaling information.")

Amicus does not discuss the actual effects of § 3121(c)'s "technology reasonably available" clause, however. Instead, amicus falsely accuses the government of construing § 3121(c) in a fashion that would "fre[e]" the government from any statutory restriction on acquisition of content, so long as the technology reasonably available to the government "cannot perfectly distinguish content from non-content." Amicus Mem. at 34 (emphasis added).

Amicus' accusation is an exercise in misdirection. Under § 3121(c), it is obviously irrelevant whether filtering technology can perfectly distinguish content from non-content. The threshold question is instead whether technology exists that is reasonably available to the government and that can in fact separate content from non-content before the government acquires either. To the extent that such technology exists, the government must use it. To the extent that it does not, § 3121(c) permits the government to access the content incidental to acquiring non-content. In this case, we have submitted extensive evidence demonstrating that no "technology reasonably available to the government [exists] that can reliably separate PCTDD content from PCTDD non-content." Gov. Opening Mem. at 5. Thus, with respect to PCTDD, the triggering condition that would otherwise obligate the government to deploy filtering technology has not been satisfied.²

² Amicus makes two, other inaccurate assertions, apparently to bolster the false claim that under the government's interpretation of § 3121(c), the government would only be obligated to deploy content-filtering technology if that technology were "perfect." One is the claim that technology is available to the government that will only extract and produce PCTDD if it is a 10-digit telephone number (e.g., one dialed through a calling card service). See Amicus Br. at 12-13. Amicus erroneously cites the Houston Decision (441 F. Supp.2d 816, at 824), which itself cites to a passage in a Department of Justice instructional manual. As the Houston Decision makes clear, however, the technique at issue does not extract the first 10 digits dialed post-cut-through. Rather, it limits production to the government of the first 10 (or 11) digits dialed by the user. Thus, when applied in any modern telephone system, the technique prevents the government from receiving any digits after a caller enters the standard 10- (or 11-) digit number required to initiate the first leg of a call, i.e., it prevents the government from collecting any additional dialed digits, including any phone numbers or extensions that the caller inputs after connecting to a calling card service or office telephone

C. Amicus Depends On Inapposite Cases

As an implicit acknowledgment of the errors of the Houston and Orlando Decisions issued in 2006, amicus devotes a minimum of discussion to those decisions and far more to prior cases that amicus contends asserts supports its position. See Amicus Mem. 14-29. Amicus contends that these earlier cases stand for the proposition that a pen register order never authorizes the government to obtain "hybrid communications -- i.e., communication containing both . . . content and unprotected content," because doing so "exceeds the essential nature of" a pen register "and because persons have a cognizable Fourth Amendment interests in hybrid communications." Amicus Br. at 21. As demonstrated below, the prior cases on which amicus purports predate § 3121(c) and therefore do not justify amicus' efforts to read the cited provision, and in particular, its "technology reasonably available" clause, out of the Pen/Trap Statute.

Amicus cites two kinds of cases in alleged support of its arguments about the limits on the government's power to obtain. One consists of cases in which courts held that a person has a reasonable expectation of privacy in the contents of digits transmitted to his pager, see, e.g., People v. Pons, 133 Misc.2d 1072, 453 (N.Y. Co. Sup. Ct. 1986), or stored in his pager, e.g., United States v. La Paz, 43 F. Supp.2d 370, 373 (S.D.N.Y. 1999)). There is no dispute here, however, that a person has a reasonable expectation of privacy in the content of telephonic communications that he stores, or that he transmits or that are transmitted to him through a service provider. Nor is there any dispute that if the government acquires such content on a showing of less than probable cause (e.g., a pen register order), that evidence is subject to suppression. Rather, the question is what has

system. In addition, citing nothing -- amicus contends that "it is likely that in this day and age, a large majority of PCTDD is content" (Amicus Mem. at 11-12). This assertion is unsubstantiated, and more importantly, inaccurate. As demonstrated at the hearing, users of the current U.S. telephone system routinely and frequently enter PCTDD non-content every day. Accordingly, to require the government to use what filtering technology is reasonably available to it, which cannot reliably distinguish PCTDD content from non-content would suppress large volumes of PCTDD non-content, even though it is "dialing, addressing, routing and signaling information" of the kind the Pen/Trap Statute expressly authorizes the government to record and to use.

Congress authorized the government to collect by means of a device or process that in the course of recording or decoding non-content may incidentally access content.

The other line of cases on which amicus relies likewise fails to prove its point. These cases address whether the Pen/Trap Statute as originally enacted in 1986 authorized the government to "clone" a pager that displays digits transmitted to it via the pager holder's service provider (a "display pager"). See Brown v. Waddell, 50 F.3d 285, 287 (4th Cir. 1995); State v. Jackson, 650 So.2d 24, 26-29 (Fla. 1995) (construing 1988 Florida Statute incorporating 1986 Pen/Trap Statute). These "cloning" cases are distinguishable because they arose under the 1986 Pen/Trap Statute, rather than the Pen/Trap Statute as amended in 1994 to add 18 U.S.C. § 3121(c) and, in particular, its clause permitting incidental access to content depending on whether technology is reasonably available to avoid it.

A "cloned" pager intercepts the entire digit string that a caller enters after calling the telephone number a service provider assigns to a pager. The string may include "raw" telephone numbers, which as amicus concedes, have no reasonable expectation of privacy (Amicus Mem. at 23-24), but may also include "an unlimited range of number-coded substantive messages." Brown, 50 F.3d at 292. Brown and Jackson held that the original Pen/Trap Statute did not authorize "cloning" of a pager, for several reasons. One was that the cloning technique depended on receiving radio transmissions from the paging service, and not on physically "attach[ing]" a device to a transmission device, as the 1986 definition of "pen register" required. Brown, 50 F.3rd at 291. More importantly, the 1986 legislative history established that Congress had assumed that unlike devices that monitor display pagers, a pen register on a telephone could only record the "mer[e] . . . switching signals that connect telephones'" and not "number-coded substantive messages". Id. at 291-292 (quoting 1986 Senate report); accord Jackson, 650 So.2d at 26-29. Accordingly, the 1986 Act authorized only "investigative technique[s]" that acquire "raw telephone numbers" and did not authorize the acquisition of dialed-digit content. Brown, 50 F.3rd at 291.

By contrast, in the instant case, the Court is called upon to apply the Pen/Trap Statute as substantially amended by, among other things, the addition in 1994 of § 3121(c). On its face, § 3121(c)'s "technology reasonably available" clause demonstrates that as of 1994, Congress knew and understood that technological changes had transformed the capabilities of ordinary telephones with respect to electronic ("touch-tone")

impulses.³ That Congress in 1994 decided to require the government to use "technology reasonably available to it to restrict" pen register output to call-processing information establishes that by then, Congress knew that ordinary telephones were no longer limited to transmitting "switching signals" in the form of "raw" telephone numbers, see Brown above, but rather, were now being used to transmit content in the form of dialed digits to the other telephones that they called. Moreover, the same clause in § 3121(c) demonstrates that in 1994, Congress decided to permit a pen register on an ordinary telephone to access such dialed-digit content, when there exists no technology reasonably available to avoid it. Thus, the cloned pager cases cited by amicus are inapposite.

D. Amicus Ignores § 3127(3)'s Ambiguity

As amended by the Patriot Act in 2001, 18 U.S.C. § 3127 provides in relevant part as follows:

(3) the term "pen register" means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication....

18 U.S.C. § 3127(3) (emphasis added).

As set forth in our opening brief (at 15-16), § 3127(3) is susceptible to two plausible but mutually antagonistic readings. Under the first, a device or process is a "pen register" under § 3127(3) at any moment that it records or decodes PCTDD non-content, but at any other moment that it records or decodes PCTDD content, the same device is not a "pen register" for the purposes of § 3127(3). Under the second interpretation, which amicus obviously prefers, the "shall not" clause added in 2001 imposes a blanket proscription of a device or process regulated by the Pen/Trap Statute from ever accessing content.

Amicus asserts that only the second reading of § 3127(3) is plausible and that the first "reading needs no rebuttal beyond the language of § 3127 itself." Amicus Mem. at 37. The words of § 3127(3) do not permit the first reading to

³ As discussed in Point E below, the legislative history of § 3121(c) confirms that Congress so intended.

be so readily dismissed. Congress had no need to resort to the locution, "such information shall not include" if what it had intended to do was prohibit a device that sometimes would record non-content from recording non-content at any other time. For example, Congress could have instead redefined a "pen register" to mean "a device or process which records or decodes dialing, routing, addressing, or signaling information . . . provided, however, that no such device or process is permitted under this chapter to record or decode content."

But obviously, Congress did no such thing. Accordingly, an interpretation of the "shall not" clause that includes a device within the definition of "pen register" at the times that it records or decodes non-content, but excludes it from that definition at times that the same device records content is at least as plausible as the interpretation preferred by amicus, which would impose an absolute bar on such a device ever accessing content. Moreover, the first interpretation comports with controlling canons of construction. As previously explained, those canons require that § 3127(3) be read, if at all possible, in a manner that gives effect to the "technology reasonably available" clause of § 3121(c) (the "rule against superfluities"), and by the same token, avoids implying that clause's repeal when, there is no clear and manifest evidence to support such an implication ("the rule against implied repeal"). See Gov. Opening Br. at 19-21.

Amicus' brief is conspicuously silent with respect to those canons because at bottom, amicus seeks to read the words "technology reasonable clause" out of § 3121(c) and the Pen/Trap Statute. Again, § 3121(c) specifically predicates the government's obligation to avoid accessing content on whether there exists technology reasonably available to restrict collection to non-content. When that technology does not exist, the condition precedent is unsatisfied. Accordingly, § 3121(c) permits access to content to occur. By contrast, reading § 3127(3) to ban a pen register from ever accessing content, impermissibly requires nullifying the "technology reasonably available" clause.

Thus, the proper resolution of any potential antagonism between § 3121(c)'s "technology reasonably available" clause and the "shall not" clause that Congress added to § 3127(3) is to construe both provisions to permit the government incidentally to access PCTDD content when there is no technology reasonably available to avoid it. Construing the Pen/Trap Statute in this manner gives effect to the safe harbor that Congress created by enacting the "technology reasonably available clause" in 1994.

At the same time, it honors the language that Congress added in 2001 to § 3127(3) establishing that while a device qualifies as a pen register when it records or decodes "dialing, routing, addressing or signaling information" but not when the recorded or decoded information "includ[es] the contents of [a] communication." For the license that the government receives to use evidence obtained from a "pen register" within the meaning of § 3127(3) (provided it also certifies the likely relevance of the non-content pursuant to 18 U.S.C. § 3123(c)) remains limited to non-content.

Amicus points out that no statutory remedy exists were the government to exceed that license by using PCTDD content rather than only PCTDD non-content. As amicus emphasizes (see Amicus Mem. at 40-46), the government's opening brief (at 17-18) incorrectly asserted that 18 U.S.C. § 2515 prohibits the government from offering in any proceeding PCTDD content in violation of Title III (18 U.S.C. § 2510 et seq.), or any evidence derived therefrom. § 2515 in fact vests an aggrieved party with a suppression remedy with respect only to unauthorized use of communications containing the sound of a human voice conveyed by wire, cable or similar device ("wire communications"), see 18 U.S.C. § 2510(1) and (18). On the other hand, § 2515 does not create a statutory remedy with respect to the class of "electronic communications" of which PCTDD is part, see 18 U.S.C. § 2510(12).

The government regrets that our description of § 2515's reach was incorrect. Whether a remedy exists to redress unpermitted use of PCTDD content, however, has no bearing on how the canons of construction require §§ 3121(c) and 3127(3) to be harmonized. The rules against superfluities and implied repeal govern in any event. As explained above, they require that §§ 3121(c) and 3127(3) be construed to permit incidental access to PCTDD content, absent technology reasonably available to the government avoid it. Moreover, even if the existence of a remedy for unpermitted use of PCTDD were material to statutory construction, we submit that on the facts of this case, and in any others that likewise follow this Office's procedures implementing the policies of the United States Department of Justice ("DOJ"), amicus itself would argue that such a remedy is in place.

As Amicus acknowledges, a May 24, 2002 policy memorandum signed by then-Deputy Attorney General Larry D. Thompson (the "DOJ PCTDD Policy Memorandum" attached hereto as Exhibit 1), obligates the department's components not to use PCTDD content obtained under sole authority of the Pen/Trap Statute "for any affirmative investigative purposes except in a

rare case in order to prevent an immediate danger of death, serious physical injury or harm to the national security." DOJ PCTDD Policy Memorandum at 4.

Amicus castigates the above policy memorandum as "[n]othing but a voluntary, unenforceable promise" against affirmative use of PCTDD content. Amicus Mem. at 46. By its express terms (at 5), the DOJ PCTDD Policy Memorandum establishes no remedy. But as amicus was in all probability unaware, it is this Office's standard procedure in any application seeking authorization under the Pen/Trap Statute incidentally to access PCTDD content pen/trap application to make the following representation to the Court:

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

Each of the instant applications (at ¶ 8 thereof) contain the above-quoted representation. We have no doubt that were the government to fail to honor that commitment, amicus would insist that, as to any intercepted party, such a failure would require that any content that the government used and any other evidence obtained as a result be suppressed.⁴ Thus, at minimum, the standard representation in our applications provides colorable grounds for redress.

E. Alternatively, Legislative History
Requires Construing The Pen/Trap Statute
To Permit Incidental Access To PCTDD Content

Were amicus correct that the "shall not" clause of § 3127(3) can only be read to prohibit a device operated under authority of the Pen/Trap Statute from accessing content, that would merely justify the Court's use of legislative history to reconcile the apparent conflict between that clause and

⁴ Because amicus's role in this case is limited to briefing the legal issue of whether incidental access to PCTDD content is permissible under the Pen/Trap Statute, the government has not produced to it the applications in dispute. Amicus' focus on the DOJ PCTDD Policy Memorandum and not how the instant applications implement it, is therefore entirely understandable.

§ 3121(c)'s "technology reasonably available" clause. As demonstrated below, the legislative history of these statutes requires reading both to permit incidental access to content.

§ 3121(c) was originally enacted in October 1994 as part of the Comprehensive Assistance To Law Enforcement Act ("CALEA"). The language of § 3121(c) had originally been introduced by Senator Leahy on August 9, 1994 as part of a precursor bill to CALEA. In his statement introducing that bill, Senator Leahy 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.

Leahy August 1994 Statement, at 11062 (emphasis added).

The above statement establishes that the primary drafter of § 3121(c) as enacted in 1994 intended the government's obligation to use content-filtering technology to occur only when such technology is not reasonably available to the government. By the same token, the Senator's statement shows that in 1994, Congress assented to the "otherwise" scenario, in which a pen register is permitted to access dialed-digit communications, there being no technology reasonably available to prevent it.

Further evidence that Congress in 1994 knew and understood that § 3121(c) would operate in this fashion is found in the Senate and House reports that accompanied CALEA when it was reported out of committee in October 2004. Both reports repeat verbatim Senator Leahy's above remarks on August 9, 1994. See S. Rep. 103-402, at *31 (1994) (excerpted at Ex. 2 to Gov. Opening Mem.); H.R. Rep. 103-827(I) at *32 (1994) (excerpted at Ex. 3 to Gov. Opening Mem.). In addition both reports emphasize that § 3121(c) is intended to "requir[e] law enforcement to use reasonably available technology to minimize information obtained through pen registers" (emphasis added). "Minimiz[ation]" based

on technology reasonably available necessarily entails an understanding that a pen register may exclude some but not necessarily all content.⁵

Amicus has literally nothing to say about Senator Leahy's August 9, 1994 statement or its reiteration in the Senate and House Reports. While amicus' opposition (at 53) quotes the relevant provision, it accords it no other discussion. Instead, amicus bookends the quotation from 1994 with discussion of irrelevant legislative history from before and after it.

It is not in dispute that when it passed the original Pen/Trap Statute in 1986, Congress understood that under the then-current state of technology, a "pen register" regulated by that statute did "'not include the contents of a communication, rather, it records the numbers dialed.'" Amicus Br. at 50-51 (quoting H.R. Rep. No. 99-647, at 78 (1986)). By the time § 3121(c) was enacted in 1994, however, Congress had come to understand that change in technology meant that those categories were not mutually exclusive: by 1994, a pen register on an ordinary telephone could record content in the form of dialed digits. See Part C above.

Nor is amicus any more persuasive when it quotes Senator Leahy (selectively, see below) to the effect that as of 1994, he understood the collection of content under sole authorization of the Pen/Trap Statute to be unconstitutional.

⁵ In our opening brief, we pointed out that the way in which Congress used the verb "to minimize" in CALEA's legislative history parallels Congress's use of the same words in Title III: in much the same way that Title III requires the government to undertake reasonable efforts "to minimize the interception of communications otherwise subject to interception," 18 U.S.C. § 2518 (emphasis added); see also Scott v. United States, 436 U.S. 128, 140 (1978), CALEA's legislative history shows that Congress intended § 3121(c) to permit incidental access to content if technology is not "reasonably available to" the government to avoid it. Accordingly, the 1994 legislative's history's use of the verb "to minimize" is hardly "an isolated passage mined from volumes of legislative history." Amicus Mem. note 13. Rather, the Senate and House reports on CALEA used that verb advisedly to describe the operation of § 3121(c) consistent with the language elsewhere in the same reports stating that the government's obligation under § 3121(c) to avoid incidental collection of content accrues only "when" technology is "reasonably available" to prevent that capture.

Amicus Br. at 52. Senator Leahy made the statement in question in 2001, not 1994. Accordingly, the statement is entitled to no weight in construing what Congress' intended § 3121(c) to mean when it was originally enacted in 1994. See, e.g., United Air Lines, Inc. v. McMann, 434 U.S. 192, 200 n.7 (1977) ("Legislative observations 10 years after passage of the Act are in no sense part of the legislative history.")

Lastly, any fair reading of Senator Leahy's statement in October 2001 with respect to the Patriot Act amendments of the Pen/Trap Statute demonstrate that he well understood that they did not repeal the conditional permission that § 3121(c) as originally enacted had conferred on the government incidentally to access PCTDD content. Rather, his statement on October 25, 2001 (Gov. Opening Mem. Ex. 4) establishes that the Patriot Act amendments made express that the Pen/Trap statute disfavors the collection of content via pen register and permits incidental access only on condition that there is no technology reasonably available to avoid it.

There is no question that Senator Leahy emphasized reservations about this outcome, because he believed that "such collection was unconstitutional on the mere relevance standard," Gov. Opening Br. Ex. 4 at 11000. In the same statement, however, the Senator also conceded that the amendments to the Pen/Trap Statute that he was supporting did not bar the government from incidentally accessing content:

- Senator Leahy acknowledged that the government had reported to Congress in 2000 that pen registers captured all dialed-digit information, because "there has been no change" in technology "that would better restrict the recording or decoding" of information to that needed to process a call. Gov. Opening Br. Ex. 4 at 11000;
- Senator Leahy was supporting the bill, even though Congress had rejected his proposal to increase "meaningful judicial review and accountability" by requiring the government to demonstrate to a Court the relevancy of evidence sought via pen register. Gov. Opening Br. Ex. 4 at 11000, and in particular, of "content" obtained from "pen/trap devices in use today," Id., which in Senator Leahy's view, "may be suppressed" under the Fourth Amendment, Id.; and

- Senator Leahy nonetheless endorsed the Patriot Act as "a good bill," a "balanced bill," and one that established necessary "checks and balances." Gov. Opening Br. Ex. 4 at 11015.

Thus, Senator Leahy's October 2001 remarks demonstrate that however much he would have preferred amending the Pen/Trap Statute to reduce instances in which pen registers access content, the Patriot Act made no provision to change the existing state of affairs in which pen registers capture all dialed digit information, non-content as well as content. His statement therefore falls far short of the "clear and manifest" evidence that the law requires to imply on the part of Congress in 2001 an intent to repeal the exception that it had enacted in 1994 permitting incidental access to content when no technology is reasonably available to avoid it. Radzanower v. Touche, Ross, Co., 426 U.S. 148, 154 (1976).

Amicus denies this reality only by eliding Senator Leahy's above remarks in favor of circular argument. Amicus claims that Senator Leahy's comment that "the Administration agreed that the definition [of a pen register] should expressly exclude the use of pen/trap devices to intercept 'content,'" Gov. Opening Br. Ex. 4 at 11099 (emphasis added), shows the Senator to have intended the Patriot Act to have "prohibited all acquisition of content through pen/trap devices." Amicus Mem. at 54-55 (quoting Senator Leahy and law review articles containing the same quotation).

The passage quoted by amicus does nothing of the kind. Rather, it merely paraphrases the "shall not" clause that the Patriot Act added to the end of § 3127(3). As such, Senator Leahy's comment about § 3127(3), partakes of the same ambiguity as the text of the "shall not" clause itself. As demonstrated in Part D above, the addition of the clause may plausibly be construed either (a) to remove from the definition of "pen register" any device that collects content, even if at other times, the same device collects non-content or (b) to include any such device at the time that it records non-content, but not when it accesses content. Accordingly, Senator Leahy's paraphrase of the "shall not" clause clarifies nothing. By contrast, his other remarks on October 25, 2001 show that he endorsed the Patriot Act, well aware that under it, the Pen/Trap Statute continued to permit the government incidentally to access content when there is no technology reasonably available to avoid it.

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.

Respectfully submitted,

ROSLYNN R. MAUSKOPF
United States Attorney

By:

Jed Davis
Assistant U.S. Attorney
(718) 254-6298

cc: Yuanchung Lee - Federal Defenders

EXHIBIT 1



U.S. Department of Justice

Office of the Deputy Attorney General


The Deputy Attorney General

Washington, D.C. 20530

May 24, 2002

MEMORANDUM

TO: THE ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
THE ASSISTANT ATTORNEY GENERAL, ANTI-TRUST DIVISION
THE ASSISTANT ATTORNEY GENERAL, TAX DIVISION
ALL UNITED STATES ATTORNEYS
THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
THE ADMINISTRATOR OF THE DRUG ENFORCEMENT
ADMINISTRATION
THE COMMISSIONER OF THE IMMIGRATION AND
NATURALIZATION SERVICE
THE DIRECTOR OF THE UNITED STATES MARSHALS SERVICE

FROM: Larry D. Thompson 

SUBJECT: Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices

This Memorandum sets forth the Department's policy regarding avoidance of "overcollection" in the use of pen registers and trap and trace devices that are deployed under the authority of chapter 206 of Title 18, United States Code, 18 U.S.C. § 3121, *et seq.*¹

The privacy that Americans enjoy in the content of their communications – whether by telephone, by facsimile, or by email – is a basic and cherished right. Both the Fourth Amendment and federal statutory law provide important protections that collectively help to ensure that the content of a person's private communications may be obtained by law enforcement only under certain circumstances and only with the proper legal authorization. In updating and revising the statutory law in this area, the recently enacted USA Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) ("the Act"), draws the appropriate balance between the right of individuals to maintain the privacy of their communications and the need for law enforcement to obtain the evidence necessary to prevent and prosecute serious crime.

¹ The authorities granted by the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801, *et seq.*, are outside the scope of this Memorandum.

In particular, Section 216 of the Act revised and clarified existing law governing “pen registers” and “trap and trace” devices – which record limited information concerning the “processing and transmitting” of communications (such as the telephone numbers dialed on a phone) – so that these devices may clearly be used, not just on telephones, but in the context of any number of communications technologies.

At the same time, several provisions of the Act underscore the importance of avoiding unauthorized collection or use, by government agents, of the *content* of wire or electronic communications. In order to accomplish this important goal, this Memorandum briefly describes the relevant law and the changes made by the Act, and then sets forth Departmental policies in this area. Those policies include the following:

- Reasonably available technology must be used to avoid collection of any content.
- If, despite use of reasonably available technology, some collection of a portion of content occurs, *no* affirmative investigative use may be made of that content.
- Any questions about what constitutes “content” must be coordinated with Main Justice.

Prior Law Governing Pen Registers and Trap and Trace Devices. Since 1986, the use of “pen registers” and “trap and trace” devices has been governed by the provisions of chapter 206 of Title 18, United States Code. See 18 U.S.C. § 3121, *et seq.* Prior to the recent enactment of the USA Patriot Act, a “pen register” was defined in chapter 206 as “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.” 18 U.S.C. § 3127(3). Analogously, a “trap and trace” device was defined as “a device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.” *Id.*, § 3127(4). Thus, a pen register could be used to record the numbers of all outgoing calls on a telephone, and a trap and trace device could be used to record the numbers of all incoming calls.

Because the Supreme Court has held that this sort of limited information concerning the source and destination of a communication is not protected by the Fourth Amendment’s warrant requirement, see *Smith v. Maryland*, 442 U.S. 735 (1979), chapter 206 permitted an order authorizing a pen register or trap and trace device to be issued without showing probable cause. Instead, an order shall be issued if the Government “certifie[s] that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3123(a) (2000). By contrast, the *contents* of a telephone conversation are generally protected by the Fourth Amendment, see *Katz v. United States*, 389 U.S. 347 (1967), as well as by the more extensive procedural protections of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968), *codified as amended at* 18 U.S.C. § 2510, *et seq.* (“Title III”).

In enacting the provisions of Chapter 206 governing pen registers and trap and trace devices, Congress also amended Title III to exempt pen registers and trap and trace devices from the requirements of the latter statute. *See* Pub. L. 99-508, § 101(b), 100 Stat. 1848 (1986) (adding 18 U.S.C. § 2511(h)(i)). However, in order to address the possibility that a pen register might, due to technological limitations, obtain some limited measure of “content,” Congress later specifically provided in chapter 206 that an agency authorized to use a pen register must “use technology reasonably available to it” that restricts the information obtained to that used in “call processing.” Pub. L. No. 103-414, § 207(b), 108 Stat. 4279 (1994) (amending 18 U.S.C. § 3121(c)).

Relevant Amendments made by the USA Patriot Act. The Act made several changes to chapter 206 that are of relevance here. In particular, section 3121(c) was amended to make explicit what was already implicit in the prior provision, namely, that an agency deploying a pen register must use “technology reasonably available to it” that restricts the information obtained “so as not to include the contents of any wire or electronic communications.” The amended section 3121(c) now reads, in full, as follows:

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

18 U.S.C. § 3121(c), as amended by Pub. L. No. 107-56, § 216(a), 115 Stat. at 288 (emphasis added).

Similarly, in amending the definitions of “pen register” and “trap and trace device” to make them more technologically neutral, the Act again expressly reiterates what was already implicit in the prior statute, namely, that a pen register or a trap and trace device is not to be viewed as an affirmative authorization for the interception of the content of communications. Thus, the amended definition of a “pen register” now provides, in pertinent part:

[T]he term “pen register” means a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, *provided, however, that such information shall not include the contents of any communication*

18 U.S.C. § 3127(3), as amended by Pub. L. No. 107-56, § 216(c)(2), 115 Stat. at 290 (emphasis added). Likewise, the Act amends the definition of “trap and trace device” so that it now provides:

[T]he term “trap and trace device” means a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, *provided, however, that such information shall not include the contents of any communication . . .*

18 U.S.C. § 3127(4), as amended by Pub. L. No. 107-56, § 216(c)(3), 115 Stat. at 290 (emphasis added).

Department Policy Regarding Avoidance of “Overcollection” in the Use of Pen Registers and Trap and Trace Devices. Although, as noted, the Act’s specific addition of references to “content” in chapter 206 probably does not alter pre-existing law on this point, it is appropriate, in light of Congress’ action, to clearly delineate Department policy regarding the avoidance of “overcollection,” *i.e.*, the collection of “content” in the use of pen registers or trap and trace devices under chapter 206. This policy includes the following basic principles.

1. **Use of reasonably available technology to avoid overcollection.** As mandated by section 3121(c), an agency seeking to deploy a pen register or trap and trace device must ensure that it uses “technology reasonably available to it” that restricts the information obtained “so as not to include the contents of any wire or electronic communications.” 18 U.S.C. § 3121(c) (West Supp. 2002). This provision imposes an affirmative obligation to operate a pen register or trap and trace device in a manner that, to the extent feasible with reasonably available technology, will minimize any possible overcollection while still allowing the device to collect all of the limited information authorized.

Moreover, as a general matter, those responsible for the design, development, or acquisition of pen registers and trap and trace devices should ensure that the devices developed or acquired for use by the Department reflect reasonably available technology that restricts the information obtained “so as not to include the contents of any wire or electronic communications.”

2. **No affirmative investigative use of any overcollection that occurs despite use of reasonably available technology.** To the extent that, despite the use of “technology reasonably available to it,” an agency’s deployment of a pen register does result in the incidental collection of some portion of “content,” it is the policy of this Department that such “content” may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security. For example, if, despite the use of reasonably available technology, a telephone pen register incidentally recorded a bank account number and personal identification number (PIN) entered on an automated bank-by-phone system, those numbers should not be affirmatively used for any investigative purpose.

Accordingly, each agency must take steps to ensure that any incidental collection of a portion

of "content" is not used for any affirmative investigative purpose.² Investigating agencies should take appropriate measures to ensure compliance with this directive, and United States Attorneys should likewise ensure that federal prosecutors do not make any investigative use of such content, whether in court applications or otherwise.

3. Coordination of issues concerning what constitutes "content". In applying the above principles, agencies should be guided by the definition of "content" that is contained in Title III: the term "content" is there defined to include "any information concerning the substance, purport, or meaning of [a] communication." 18 U.S.C. § 2510(8) (West Supp. 2002). Similarly, in describing the sort of information that pen registers and trap and trace devices are designed to capture, the provisions of Chapter 206 make clear that "dialing, routing, addressing or signaling information" that is used in "the processing and transmitting of wire or electronic communications" does not, without more, constitute "content." 18 U.S.C. § 3127(3) (West Supp. 2002); *id.*, § 3121(c).

The Assistant Attorney General for the Criminal Division (AAG) should ensure that the Criminal Division provides appropriate guidance, through amendments to the United States Attorneys' Manual or otherwise, with respect to any significant general issues concerning what constitutes the "content" of a communication.

To the extent that, in applying the above principles, specific issues arise over whether particular types of information constitute "content," such questions should be addressed, as appropriate, to the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).

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

² This is not to say that an agency should not retain a file copy of all of the information it received from a pen register or trap and trace device. An agency may be statutorily *required* to keep a record of all of the information it obtains with a particular pen register or trap and trace device, *see, e.g.*, 18 U.S.C. § 3123(a)(3), *as amended by* Pub. L. No. 107-56, § 216(b)(1), 115 Stat. at 289 (requiring that, in certain limited circumstances, an agency must maintain and file with the issuing court a record of "any information which has been collected by the device"), and, in the event of a subsequent prosecution, the agency may be required to produce to defense counsel a complete record of what was recorded or captured by a pen register or trap and trace device deployed by the agency in a particular case. This Memorandum prohibits *affirmative investigative* uses. Accordingly, nothing in this Memorandum should be construed to preclude an agency from maintaining a record of the full information obtained by the agency from a pen register or trap and trace device.