

Electronic Frontier Foundation discussion of how anti-terrorism bills would change governmental authority to use pen registers and trap-and-trace devices

ATA, CTA, and USAA would each change the regulation of the use of “pen registers” and “trap-and-trace devices” (pen/trap devices). The use of such devices has become increasingly controversial with the advance of telecommunications and the Internet, because it is more and more the case that using such devices obtains information about what people are saying or doing -- information for which law enforcement should use a Title III intercept order. The controversy over the FBI’s “Carnivore” is the most recent installment in this long-running saga.

The following is an analysis of the proposed pen/trap changes by the Electronic Frontier Foundation. Our general conclusion is that USAA is the least dangerous to civil liberties.

Contact: Lee Tien, Senior Staff Attorney, tien@eff.org, (415) 436-9333 x 102

Introduction

Current law does not merely regulate the interception of communications; it also regulates the acquisition of information about the communications via devices known as “pen registers” and “trap-and-trace devices” (pen/trap devices).

Pen/trap devices acquire the “numbers dialed or otherwise transmitted on the telephone line to which such device is attached.” Pen devices capture the numbers dialed from a particular number, while trap devices capture the numbers dialed to a number.

The current pen/trap law permits government to acquire “electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached” and “incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.” 18 U.S.C. §§ 3127(3), (4).

Unlike wiretaps, the use of pen/trap devices is very weakly regulated by federal law: while the government must apply to a court for a pen/trap order, there is no meaningful judicial review or oversight of either the application for or implementation of a pen/trap order. For instance, current law requires only that the government “certify” to the court that installing a pen/trap device is likely to aid an ongoing criminal investigation. Such “certification” is not a factual showing.

Historical background

Why are pen/trap devices so weakly regulated? The main reason is that pen/trap devices, as a historical matter, did not capture very much information. The Supreme Court has twice ruled on the legality of pen/trap devices, but both cases were decided more than 20 years ago.

In 1968, a pen register was understood to be a mechanical device that could be attached to a given telephone line, usually at the central telephone offices. A pulsation of the dial on a line to which the pen register is attached recorded on a paper tape dashes equal to the number dialed. The paper tape then becomes a permanent and complete record of outgoing calls as well as the numbers called on the particular line. Immediately after the number is dialed and before the line called has had an opportunity to answer the pen register mechanically and automatically is disconnected, with neither recording nor monitoring of the conversation. See *United States v. Dote*, 371 F.2d 176 (7th Cir. 1966), cited in Title III Senate Report, S. Rep. No. 1097, 90th Cong., 2d Sess. 66 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2178.

The Dote pen register did not disclose whether the call had been completed or how long it had lasted, the caller's physical location or electronic address, or the numbers dialed after the call had been completed. The pen register was installed by the telephone company, and the record was created on paper.

The Supreme Court then found that Title III did not apply to pen registers (no Fourth Amendment analysis because probable cause was found to exist). *United States v. New York Telephone Co.*, 434 U.S. 159 (1977). In *New York Telephone*, law enforcement agents asked the telephone company to transmit the pen register information over a leased line running from the terminal box to a remote monitoring point. The telephone company refused, and the Court upheld a court order mandating compliance. 434 U.S. at 161-163, 177-78. The Court emphasized that pen registers disclosed neither the purport of the communication, the identities of the parties communicating, nor whether the communication was even completed. 434 U.S. at 166-68.

In its only other pen-register case, the Court described a pen register by incorporating definitions found in prior cases and by repeating the description in *New York Telephone* of the pen register's limited capabilities. *Smith v. Maryland*, 442 U.S. 735, 736 n.1, 741-42 (1979). The pen register in *Smith* was installed by the telephone company at its central offices. *Id.* at 741.

The Court found that pen registers did not even implicate the Fourth Amendment, because no constitutional privacy interest attached to the numbers dialed on a telephone, which was the only information obtained from the installation of the pen register on the defendant's telephone line. The Court held that *Smith* had assumed the risk that the telephone company would reveal the numbers he had dialed: people entertain no actual expectation of privacy in those numbers because they must convey them to the telephone company, and subscribers know that telephone companies can record dialed numbers because they see their toll call numbers listed on their phone bills and because telephone books tell them that the phone company can trace calls to protect them from harassment. 442 U.S. at 742-43.

Smith left non-content privacy in a shambles. On the one hand, the *Smith* Court emphasized the extremely limited scope of the information disclosed by pen register

investigations, echoing its discussion in *New York Telephone*. 442 U.S. at 741 (noting that the device had recorded neither the purport of Smith's communications, nor the identity of the parties, nor even whether calls were completed). But the "assumption of risk" analysis invited lower courts to reject constitutional protection for any aspect of a communication that could be captured as long as it did not constitute the contents of a telephone conversation.

In 1986, Congress enacted the pen/trap statute. Congress omitted the Supreme Court's reference to the "mechanical" nature of the pen register device, and it did not limit the pen register to something that acquired information about a telephone, although it did specify that a telephone line would be involved. The legislative history described pen registers as "devices that record the telephone numbers to which calls have been placed from a particular telephone." ECPA Senate Report, S. Rep. No. 541, 99th Cong., 2d Sess. 14 (1986), at 10, reprinted in 1986 U.S.C.C.A.N. 3555, 3564.

In so doing, Congress approved devices that could capture information beyond that approved by the Supreme Court in both *New York Telephone* and *Smith*. For instance, 18 U.S.C. § 3127 does not exclude information that could determine whether the call has been completed, even though such information was not available in either of the Supreme Court's pen-register cases.

As a result, courts have expanded the definition of a pen register from the device considered in *Smith*. Courts treat as pen registers devices that record the time, date and duration of both incoming and outgoing calls, devices that record, on tape rather than paper, not only the telephone numbers of the calls placed on a telephone, but other digits dialed, such as personal ID numbers and numbers used in maneuvering through voice-mail systems, and even devices that can record the contents of conversations, as long as that capacity is not used. But see *Brown v. Waddell*, 50 F.3d 285, 287-288, 294 (4th Cir. 1995) (finding that, in capturing and displaying up to 25 digits, digital display pager clones, including paging transmission units, may divulge coded messages that constitute content, such as a code for "en route"); *People v. Bialostok*, 610 N.E.2d 374 (N.Y. 1993) (holding that a device's capacity to record communication contents disqualifies it as a pen register under New York law); *United States v. David*, 940 F.2d 722, 727-29 (1st Cir.) (evaluating use of beeper clone under Title III intercept provisions rather than ECPA pen register provisions), cert. denied, 504 U.S. 955 (1992).

The modern context: expanding the scope of the pen/trap statute

The expansion of pen/trap devices is important first because the pen/trap statute hardly constrains law enforcement. Law enforcement agents must get a court order before using the devices, but courts "shall" grant ex parte orders whenever the applicant has certified that the information likely to be obtained is relevant to an ongoing criminal investigation. 18 U.S.C. § 3123(a). See, e.g., *United States v. Hallmark*, 911 F.2d 399, 402 (10th Cir. 1990) (describing the judicial review provision as "intended merely to safeguard against purely random use" of pen registers).

Unlike the wiretap statute, which has a statutory exclusionary rule for wire communications, the pen/trap law has no such provision, and the Fourth Amendment's exclusionary rule does not apply. See *United States v. Fregoso*, 60 F.3d 1314, 1320-21 (8th Cir. 1995); *United States v. Thompson*, 936 F.2d 1249, 1249-50 (11th Cir. 1991). There is no notice provision. There is no provision for judicial supervision of the conduct of pen/trap devices. There is no minimization rule; § 3121(c) only requires the government to use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information used in call processing. If such technology is not reasonably available, it cannot be used.

The second problem is that modern surveillance techniques and communications technology blur the line between contents and non-contents. Courts have found that some new surveillance techniques are completely unregulated and can be conducted without satisfying any procedural safeguards. A California district court granted an application for a cellular telephone digital analyzer that could detect the target cellular phone's electronic serial number, its telephone number and the telephone numbers it called. The court, having refused to consider the device a pen register since it did not attach to a telephone line, found that no court order of any kind was required to use the device. *Order Re Use of Digital Analyzer*, 885 F. Supp.197, 199 (C.D. Cal. 1995). The government had applied for a pen register order "‘out of an abundance of caution,' " and the court evaluated the court order granted according to the requirements set out in the pen register provision of the ECPA. See *id.* at 200-02. The device also had the capability to intercept the contents of cellular telephone conversations.

Moreover, for Internet communications, there is no true equivalent to “numbers dialed on a telephone.” The simplest example is Web browsing, which is clearly a form of electronic communication. If a person goes to the EFF website, <http://www.eff.org>, he or she can continue on to different pages within EFF’s website. Each represents another “address.” And yet each “address” tells you exactly what the person was reading.

ATA

Sec. 101. Modification of authorities relating to use of pen registers and trap and trace devices.

ATA 101 involves two significant expansions of pen/trap authority. First, it expands the nature of information that can be captured under a pen/trap order, but does not define its terms. Second, it expands the geographic reach of a federal pen/trap order. Neither change is directly tied to ATA’s anti-terrorism justification. The first change is especially dangerous because it almost certainly entails the acquisition of communications contents without the protections of Title III, which contains significant constitutional safeguards.

1. In the Internet context, addressing information reveals far more about the contents of a person’s communications as well as his or her First Amendment activities.

ATA 101 would significantly expand law enforcement authority to use trap and trace and pen register devices. It would replace language that refers to telephone numbers with the phrase “dialing, routing, addressing, or signaling information.” It would also replace the current phrase “call processing” with the phrase “the processing and transmitting of wire and electronic communications.” See 18 U.S.C. § 3121(c).

These terms are, however, not defined in ATA. The lack of definition is extremely disturbing given the apparent breadth of the language and the difficulty of defining phrases like “call-identifying information” in the modern telephony context. See generally *U.S. Telecom Ass’n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000) (reversing and remanding to FCC inquiry into whether, inter alia, “signaling information” from custom calling features such as call forwarding and call waiting qualified as “call-identifying information”).

This change would expand pen/trap capacities to the Internet, covering electronic mail, Web surfing, and all other forms of electronic communication. This is especially disturbing in light of the FBI’s controversial use of its Carnivore system.

The problem lies mainly in the false analogy of Internet “addressing” information to “numbers dialed on a telephone.” (If one were seriously to seek an analogy in the Internet context, it might be to DNS (Domain Name System) lookup on port 53.)

One obvious example is subject lines in e-mail headers, which even the Justice Department at present agrees constitutes communications “contents” outside the scope of a pen/trap order. By not defining “dialing, routing, addressing, and signalling information,” ATA is open to the interpretation that subject lines are not contents under Title III.

More generally, e-mail addresses are more personally revealing than phone numbers because e-mail addresses are unique to individual users. A pen register on a phone line only shows the dialed numbers -- it cannot reveal which of the residents answered the phone. In a household, each person online may have a separate e-mail address, and may have different e-mail addresses for different purposes (home vs. work), making it more likely that the government can determine precisely who is contacting whom.

Another example is Web browsing. URLs would clearly qualify as “addressing information.” But URLs are not analogous to telephone numbers in terms of the content/non-content distinction.

When browsing the Web, people enter URLs or click on links; the URL or link would appear to qualify as “routing” or “addressing” information. EFF maintains a website containing much information at <http://www.eff.org>. But this is not the only “address” at EFF’s website. Every document made available to the public resides on a page within the EFF website, and many if not most of these documents have their own individual addresses.

For instance, <http://www.eff.org/Privacy/Surveillance> is a page that contains, among other things, a list of URLs for the present anti-terrorism bills as well as EFF's comments and alerts regarding those bills. Thus, http://www.eff.org/Privacy/Surveillance/fisa_faq.html is a list of "frequently asked questions" about the Foreign Intelligence Surveillance Act.

Obviously, when law enforcement use a pen/trap device to capture these URLs, they learn far more about what one is reading or studying than they would from the telephone numbers one dials or is dialed by. If a journalist calls an EFF staffer about a story, a pen/trap device would only reveal that the two people talked -- nothing about the content of the call would be revealed. If the journalist instead goes to EFF's website, a pen/trap device that captured each URL that the journalist "clicked" to would reveal exactly what the journalist read. To the extent that people use the Internet as a library or entertainment source, capturing the URLs they click on is like getting their library reading or cable TV viewing records.

Even for telephone numbers, modern telephony raises similar issues. For instance, the FBI has sought to compel telephone carriers to acquire the capacity to perform so-called post-cut-through dialed digit extraction under the Communications Assistance to Law Enforcement Act. These are digits dialed after a telephone call has been connected or "cut through."

Post-cut-through dialed digits can represent call content. For example, subjects calling automated banking services enter account numbers. When calling voicemail systems, they enter passwords. When calling pagers, they dial digits that convey actual messages. And when calling pharmacies to renew prescriptions, they enter prescription numbers.

The D.C. Circuit vacated the FCC's order requiring carriers to make available all post-cut-through dialed digits -- those that convey content as well as telephone numbers. *U.S. Telecom Ass'n v. FCC*, 227 F.3d 450 (D.C. Cir. 2000).

2. Jurisdictional expansion of the pen/trap statute

18 USC § 3123(a) currently states that a judge shall authorize the installation and use of a pen register or trap and trace device "within the jurisdiction of the court." This limits the geographic scope of a pen/trap order.

ATA 101 removes this limit for all pen/trap applications by federal officials and expressly provides that pen/trap orders apply to any entity providing wire or electronic communication service in the United States whose assistance "may facilitate the execution of the order."

This means that a single application for a pen/trap order will reach nationwide and to any service provider of any kind, without even naming particular providers. A normal subpoena, even one with nationwide effect, is addressed to a specific custodian of the desired information. Fed. R. Crim. Proc. 17(c). Presumably, the government would obtain a blank order, which it could serve on multiple, unnamed service providers, with no limit

as to time or how often the order could be used. Note also that ATA removes this geographic scope limit for wire communications as well as electronic communications.

CTA Sec. 832

CTA makes essentially the same changes as ATA 101 to pen/trap law, but has two additional features. First, it expands the “emergencies” under which a pen/trap order may be used. Second, it expands the number and type of federal officials who may seek a pen/trap order.

1. Expanding emergency circumstances

Current law permits emergency use of pen/trap devices under only two circumstances, immediate danger of death or serious bodily injury to any person and conspiratorial activities characteristic of organized crime.

CTA adds three new emergency circumstances: immediate threat to U.S. national security interests; immediate threat to public health or safety; or an attack on the integrity or availability of a protected computer which attack would be an offense punishable under 18 U.S.C. § 1030(c)(2)(C) of the Computer Fraud and Abuse Act (establishing punishments for certain second offenses).

Arguably, immediate threats to U.S. national security interests and to public health or safety are already covered by the statute. Such threats are highly likely to involve immediate danger of death or serious bodily injury to some person. As to the CFAA violations, the inclusion of §1030(a)(2)(C) is especially broad. The other CFAA sections that would be included are narrower. §§ 1030(a)(2), (a)(3), (a)(6).

EFF is not aware of any evidence or testimony indicating that these expansions are necessary or that their absence has been problematic.

2. Expanding the officials who may seek an emergency pen/trap order

Under current law, if the federal government seeks an emergency pen/trap order, the applying official must be at least a Deputy Assistant Attorney General; under CTA § 832, any United States Attorney may do so.

As with Title III interceptions, limiting the persons who may seek surveillance orders is a basic procedural safeguard against possible abuse. Such a safeguard ought not be relaxed without good reason, and EFF is not aware of any evidence or testimony on this score.

miscellaneous

The “nationwide scope” provision of CTA is narrower than that of ATA because whereas ATA includes any provider whose assistance “may facilitate” execution of the

pen/trap order, CTA includes only providers whose assistance “is required to effectuate” the order.

USAA Sec. 204

Senator Leahy’s bill does the least harm to civil liberties in the pen/trap arena for two basic reasons. First, although USAA expands the information that may be acquired under pen/trap authority, that expansion is much more limited. Second, USAA requires more than a “certification” by law enforcement; it requires that the government official submit a “statement of facts” to the court.

information reached by pen/trap orders

USAA Sec. 204 expands pen/trap authority in two specific ways. First, it amends the definition of a pen register by reference to “other signaling information that identifies the destination of” communications and the definition of a trap and trace device by reference to “other signaling information which identify the originating instrument or device” from which a communication is transmitted. Second, it provides that a pen/trap order may specify the “attributes of the communication.” See Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. Rev. 949, 953 (1996) (introducing concept of “communication attributes”).

Nevertheless, these changes are more limited than that under either ATA or CTA. USAA expressly refers to destination- or origination-identifying information, which helps address concerns about capturing “contents.” In addition, USAA builds the same sort of limit into 18 U.S.C. § 3121(c), which limits government authority to use pen/trap devices. ATA adds the words “routing, addressing” to the extant “dialing and signaling information,” USAA does not. Moreover, while ATA replaces the phrase “call processing” with “the processing and transmitting of wire and electronic communications,” USAA replaces the phrase “call processing” with “identifying the origination or destination of wire and electronic communications.”

potential increased judicial oversight

Equally important, USAA Sec. 204 creates the potential for somewhat more judicial oversight of pen/trap orders. As explained earlier, courts currently issue pen/trap orders based only on a “certification” by the applying official.

Under USAA, pen/trap applications must contain a “statement of facts showing that” the information obtained is likely to be relevant to an ongoing criminal investigation. Moreover, the court must find this likelihood “based on facts contained in the application.”

While no standard of review is specified, requiring the presentation of facts and tying the order’s issuance to those facts at least creates the possibility of some meaningful review possible.

emergency installation of pen/trap devices without court order

Like CTA, USAA amends the “emergency” provisions of the pen/trap statute; the new “emergency” circumstances are close, but not identical, to those under CTA. Unlike CTA, USAA does not increase the number or type of officials who may make emergency applications.

The overall effect of the emergency provisions of USAA is smaller than for CTA because officials must apply for a pen/trap order under 18 U.S.C. § 3125, subject to the somewhat increased judicial oversight provisions (“statement of facts”).

relaxation of geographic scope limits

Finally, USAA amends the pen/trap statute to permit issuance of nationwide pen/trap orders. Here again, the “statement of facts” requirement may enhance judicial oversight.