

LEXSTAT 18 U.S.C. 3121

UNITED STATES CODE SERVICE
Copyright (c) 2008 Matthew Bender & Company, Inc.
a member of the LexisNexis Group.
All rights reserved.

*** CURRENT THROUGH P.L. 110-239, APPROVED 6/3/2008 ***
*** WITH GAPS OF 110-234 and 110-236 ***

TITLE 18. CRIMES AND CRIMINAL PROCEDURE
PART II. CRIMINAL PROCEDURE
CHAPTER 206. PEN REGISTERS AND TRAP AND TRACE DEVICES

Go to the United States Code Service Archive Directory

18 USCS § 3121

Review expert commentary from The National Institute for Trial Advocacy preceding 18 USCS § 3121 (relating to pen registers and trap and trace devices).

§ 3121. General prohibition on pen register and trap and trace device use; exception

(a) In general. Except as provided in this section, no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title [18 USCS § 3123] or under the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.).

(b) Exception. The prohibition of subsection (a) does not apply with respect to the use of a pen register or a trap and trace device by a provider of electronic or wire communication service--

(1) relating to the operation, maintenance, and testing of a wire or electronic communication service or to the protection of the rights or property of such provider, or to the protection of users of that service from abuse of service or unlawful use of service; or

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect such provider, another provider furnishing service toward the completion of the wire communication, or a user of that service, from fraudulent, unlawful or abusive use of service; or

(3) where the consent of the user of that service has been obtained.

(c) Limitation. A government agency authorized to install and use a pen register or trap and trace device under this chapter [18 USCS §§ 3121 et seq.] 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.

(d) Penalty. Whoever knowingly violates subsection (a) shall be fined under this title or imprisoned not more than one year, or both.

HISTORY:

(Added Oct. 21, 1986, P.L. 99-508, Title III, § 301(a), 100 Stat. 1868.)

(As amended Oct. 25, 1994, P.L. 103-414, Title II, § 207(b), 108 Stat. 4292; Oct. 26, 2001, P.L. 107-56, Title II, §

216(a), 115 Stat. 288.)

HISTORY; ANCILLARY LAWS AND DIRECTIVES

Effective date of section:

This section became effective 90 days after enactment, pursuant to § 302 of Act Oct. 21, 1986, P.L. 99-508, which appears as a note to this section.

Amendments:

1994. Act Oct. 25, 1994 redesignated subsec. (c) as subsec. (d) and added new subsec. (c).

2001. Act Oct. 26, 2001, in subsec. (c), inserted "or trap and trace device", inserted ", routing, addressing,", and substituted "the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications" for "call processing".

Other provisions:

Effective date and application of Act Oct. 21, 1986. Act Oct. 21, 1986, P.L. 99-508, Title III, § 302, 100 Stat. 1872, provides:

"(a) In general. Except as provided in subsection (b), this title and the amendments made by this title [adding 18 USCS §§ 1367 and 3121 et seq.] shall take effect ninety days after the date of the enactment of this Act and shall, in the case of conduct pursuant to a court order or extension, apply only with respect to court orders or extensions made after this title [adding 18 USCS §§ 1367 and 3121 et seq.] takes effect.

"(b) Special rule for State authorizations of interceptions. Any pen register or trap and trace device order or installation which would be valid and lawful without regard to the amendments made by this title [adding 18 USCS §§ 1367 and 3121 et seq.] shall be valid and lawful notwithstanding such amendments if such order or installation occurs during the period beginning on the date such amendments take effect and ending on the earlier of--

"(1) the day before the date of the taking effect of changes in State law required in order to make orders or installations under Federal law as amended by this title [adding 18 USCS §§ 1367 and 3121 et seq.]; or

"(2) the date two years after the date of the enactment of this Act."

NOTES:

Research Guide:

Federal Procedure:

27 Moore's Federal Practice (Matthew Bender 3d ed.), ch 641, Search and Seizure § 641.121.

8A Fed Proc L Ed, Criminal Procedure §§ 22:317, 318.

Am Jur:

29A Am Jur 2d, Evidence § 1229.

68 Am Jur 2d, Searches and Seizures § 343.

Criminal Law and Practice:

1 Criminal Constitutional Law (Matthew Bender), ch 2, Search and Seizure § 2.03.

1 Criminal Defense Techniques (Matthew Bender), ch 5, Electronic Surveillance Under Federal Law §§ 5.10, 5.12.

Annotations:

Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use. 15 ALR Fed 2d 537.

Texts:

Homeland Security Deskbook (Matthew Bender), ch 6, Communications and Cyber Security § 6.02.

Law Review Articles:

Nevin; Scott. The USA Patriot Act: Time To Speak Up [Discussion of T. Derden, One Year Under the Patriot Act]. 46 Advoc (Boise) 19, December 2003.

Brandt; Van Valkenburgh. The USA Patriot Act: The Devil is in the Details [Discussion of T. Derden, One Year Under the Patriot Act]. 46 Advoc (Boise) 24, December 2003.

Chemerinsky. Litigation alerts in the USA Patriot Act. 23 Cal Law 29, April 2003.

Rosenszweig. Civil Liberty and the Response to Terrorism. 42 Duq L Rev 663, Summer 2004.

Sidbury. You've got mail . . . and your boss knows it: rethinking the scope of the Electronic Communications Privacy Act. 5 J Internet L 16, July 2001.

Yonehara. Big Brother: government as service provider and the Electronic Communications Privacy Act's "provider exception". 5 J Internet Law 20, March 2002.

The USA Patriot Act: Privacy Versus Security in a Post-9/11 World. Symposium. 29 NC J Int'l & Com Reg 595, Summer 2004.

Sproule. The Effect of the USA Patriot Act on Workplace Privacy. 49 Prac Law 35, February 2003.

Interpretive Notes and Decisions:

1. Generally 2. Use of evidence obtained

1. Generally

Government's surveillance of defendant's e-mail and Internet activity did not constitute as Fourth Amendment search. Even if government's computer surveillance went beyond scope of former 18 USCS §§ 3121-3127 (amended 2001), he was not entitled to suppression of evidence. *United States v Forrester* (2007, CA9 Cal) 2007 US App LEXIS 16147, amd (2007, CA9 Cal) 495 F3d 1041 and reprinted as amd (2007, CA9 Cal) 2007 US App LEXIS 17626.

Caller ID unit is not trap and trace device; thus, co-worker's installation of caller ID unit on employee's phone was not illegal under 18 USCS § 3121. *Sparshott v Feld Entm't, Inc.* (2002, App DC) 354 US App DC 63, 311 F3d 425, 19 BNA IER Cas 708, 54 FR Serv 3d 659.

Court order was not required to install and use pen register--device which indicates which numbers are dialed from telephone--under 18 USCS §§ 3121 and 3123, in prosecution for violation of gambling, tax, and financial reporting laws, where pen register was installed and used prior to enactment of relevant statutory provisions, because provisions have no retroactive effect. *United States v Mosko* (1987, DC Colo) 654 F Supp 402, *affd* (1989, CA10 Colo) 887 F2d 1009, withdrawn by publisher, reported at (1989, CA10 Colo) 1989 US App LEXIS 9033, *reh gr*, in part, *reh den*, in part, *en banc* (1989, CA10) 1989 US App LEXIS 18893 and *reaffirmed*, in part, *mod*, in part, on *reh* (1989, CA10 Colo) 890 F2d 1461, *cert den* (1990) 494 US 1038, 108 L Ed 2d 632, 110 S Ct 1498 and *cert den* (1990) 495 US 960, 109 L Ed 2d 750, 110 S Ct 2568.

Government may not seek cell site information pursuant to Pen/Trap Statute, 18 USCS § 3121 *et seq.*, because Communications Assistance for Law Enforcement Act, Pub. Law No. 103-313, 108 Stat. 4279, explicitly forbids service providers from disclosing any information that may disclose physical location of subscriber when government proceeds solely pursuant to authority for pen registers and trap and trace devices. In *re Application of United States of America for Order Authorizing Installation and Use of Pen Register* (2005, DC Md) 402 F Supp 2d 597.

Combined authority of Pen/Trap Statute, 18 USCS § 3121 *et seq.*, and Stored Communications Act, 18 USCS § 2701 *et seq.*, did not allow government to obtain real time cell site information (which would reveal physical location of person in possession of cell phone whenever phone was on) upon showing of less than probable cause; court's general authority to issue Fed. R. Crim. P. 41 warrant applied. In *re Application of United States of America for Order Authorizing Installation and Use of Pen Register* (2005, DC Md) 402 F Supp 2d 597.

District court's issuance of court order for cell site information under 18 USCS § 2703 and Pen Register Statute was not unconstitutional in violation of Fourth Amendment's prohibition against unreasonable searches and seizures because Government did not seek to install "tracking device," as individual had chosen to carry device (cell phone) and to permit transmission of its information to third party, carrier and provision of such information to third party carrier did not implicate Fourth Amendment; for purposes of Fourth Amendment, cell site information sought did not provide "virtual map" of user's location and did not pinpoint user's location within building, but only identified nearby cell tower. In *re United States for Order for Disclosure of Telecommunications Records* (2005, SD NY) 405 F Supp 2d 435.

Government was entitled to order that would allow for pen register and trap and trace device on phone number assigned to cellular telephone and was further entitled, pursuant to Pen Register Statute, 18 USCS §§ 3121 *et seq.*, and Stored Communications Act, 18 USCS § 2703, to record cell site information, but only when cell phone was being used for calls and only if location information was used only to give approximate location of phone, based upon cell sites, and was not used to pinpoint exact location of cell phone. In *re United States* (2006, WD La) 411 F Supp 2d 678 (criticized in *re Application of United States for Order for Prospective Cell Site Location Info. on Certain Cellular Telephone* (2006, SD NY) 2006 US Dist LEXIS 11747).

Both statutory text and legislative history of 18 USCS § 3121 *et seq.* authorized use of pen register and trap and trace devices on e-mail accounts during criminal investigations. In *re United States* (2006, DC Dist Col) 416 F Supp 2d 13.

Where government refused to provide sworn affidavit attesting to facts demonstrating probable cause so as to permit court to issue warrant under Fed. R. Crim. P. 41, court denied government's application for pen register to capture and report prospective cell site information in connection with investigation of fugitive; Pen/Trap Statute, 18 USCS §§ 3121 *et seq.*, and 18 USCS § 2703(d), part of Stored Communications Act, did not allow order for capture of prospective cell site information to be issued upon less than probable cause. In *re Order Authorizing Installation and Use of Pen Register* (2006, DC Md) 439 F Supp 2d 456.

Communications content information as defined under 18 USCS § 2510(8), obtained by post-cut-through dialed digits can not be intercepted by law enforcement under Pen/Trap Statute under 18 USCS §§ 3121(c), 3127 and can only be intercepted by law enforcement under 18 USCS § 2518, part of Title III of Omnibus Crime Control and Safe Streets

Act of 1968, and Stored Communications Act, 18 USCS § 2701 et seq. Thus, government was denied authorization for access to such information through pen trap order because call contents would be obtained, which was proscribed by Pen/Trap Statute. *In re United States* (2006, SD Tex) 441 F Supp 2d 816 (criticized in *In re United States for Order for Prospective Cell Site Location Info.* (2006, SD NY) 2006 US Dist LEXIS 76822).

47 USCS § 1002(a)(2) allows cell site information to be disclosed pursuant to Pen Register and Trap and Trace Statute, 18 USCS §§ 3121 to 3127, combined with some other source of authority. *In re Application of United States* (2007, DC Puerto Rico) 497 F Supp 2d 301.

United States District Court for District of Puerto Rico reads phrase "solely pursuant" in 47 USCS § 1002(a)(2) so as to convey meaning that Pen Register and Trap and Trace Statute, 18 USCS §§ 3121 to 3127, may be used in combination with some other authority to obtain location information. *In re Application of United States* (2007, DC Puerto Rico) 497 F Supp 2d 301.

Plaintiff could bring claim against federal prosecutors and law enforcement agents for alleged violations of Pen Register Statute, 18 USCS §§ 3121 et seq., as 18 USCS § 2707(g), part of Stored Communications Act provided civil remedy for violations of Pen Register Statute. *Bansal v Russ* (2007, ED Pa) 513 F Supp 2d 264.

Although no technology existed that would enable Government to separate post-cut-through dialed digits (PCTDDs) containing content from PCTDDs that did not contain content, 18 USCS § 3121(c) did not allow Government to access PCTDDs because (1) 18 USCS § 3127, which defined pen register, unconditionally prohibited collection of content, and (2) allowing Government to access PCTDDs containing information such as bank account numbers, pin numbers, prescription numbers, social security numbers, and credit card numbers would have violated Fourth Amendment prohibition against obtaining contents of communication without probable cause; thus, until Government could separate PCTDDs that did not contain content from those that did, pen register authorization under Pen/Trap Statute, 18 USCS §§ 3121-3127, was insufficient for Government to obtain any PCTDDs. *In re United States* (2007, ED NY) 515 F Supp 2d 325.

2. Use of evidence obtained

Information obtained from pen register placed on telephone can be used as evidence in criminal trial, even if court order authorizing its installation does not comply with requirements of statute regulating pen registers, since violation of statute does not result in unconstitutional search and Congress did not provide for exclusion of evidence for violation of statute, either specifically or by inference. *United States v Thompson* (1991, CA11 Ga) 936 F2d 1249, cert den (1992) 502 US 1075, 117 L Ed 2d 139, 112 S Ct 975.

Cell site information could not be obtained on prospective basis through combination of Pen/Trap Statute and Stored Communications Act (SCA); court could only authorize such disclosure upon showing of probable cause under Fed. R. Crim. P. 41, and information requested did not escape this holding by virtue of less intrusive nature. *In re Application of United States of America for Orders Authorizing Installation and Use of Pen Registers and Caller Identification Devices* (2006, DC Md) 416 F Supp 2d 390.

Government was denied pen/trap order authorizing access to prospective cell site information because 18 USCS § 3121(a) established minimum but not maximum legal process under which pen/trap might be installed or used; elimination of pen/trap orders as legal basis to obtain cell site data under 47 USCS § 1002(a) did not place such information beyond reach of law enforcement based upon flexibility of Fed. R. Crim. P. 41; and Stored Communications Act, specifically 18 USCS § 2702, expressly prohibited disclosure of subscriber information to governmental entities except under certain delineated circumstances, none of which included pen/trap orders. *In re United States* (2006, SD Tex) 441 F Supp 2d 816 (criticized in *In re United States for Order for Prospective Cell Site Location Info.* (2006, SD NY) 2006 US Dist LEXIS 76822).