



U.S. Department of Justice

Executive Office for United States Attorneys
Freedom of Information/Privacy Act Staff
600 E Street, N.W., Room 7300
Washington, D.C. 20530
202-616-6757 Fax 202-616-6478

Requester: Catherine Crump Request Number: 07-4130

Subject of Request: Mobile Phone Tracking (Item 1-4) AUG 12 2008

Dear Requester:

Your request for records under the Freedom of Information Act/Privacy Act has been processed. This letter constitutes an interim reply from the Executive Office for United States Attorneys, the official record-keeper for all records located in this office and the various United States Attorneys' Offices. To provide you the greatest degree of access authorized by the Freedom of Information Act and the Privacy Act, we have considered your request in light of the provisions of both statutes.

The records you seek are located in a Privacy Act system of records that, in accordance with regulations promulgated by the Attorney General, is exempt from the access provisions of the Privacy Act, 28 C.F.R. § 16.81. We have also processed your request under the Freedom of Information Act and are making all records required to be released, or considered appropriate for release as a matter of discretion, available to you. This letter is a [] partial [] full denial.

Enclosed please find:

- 37 page(s) are being released in full (RIF);
- 2 page(s) are being released in part (RIP);
- page(s) are withheld in full (WIF). **The redacted/withheld documents were reviewed to determine if any information could be segregated for release.**

The exemption(s) cited for withholding records or portions of records are marked below. An enclosure to this letter explains the exemptions in more detail.

Section 552

Section 552a

- | | | | |
|---------------------------------|--|---|--|
| <input type="checkbox"/> (b)(1) | <input type="checkbox"/> (b)(4) | <input type="checkbox"/> (b)(7)(B) | <input checked="" type="checkbox"/> (j)(2) |
| <input type="checkbox"/> (b)(2) | <input checked="" type="checkbox"/> (b)(5) | <input type="checkbox"/> (b)(7)(C) | <input type="checkbox"/> (k)(2) |
| <input type="checkbox"/> (b)(3) | <input type="checkbox"/> (b)(6) | <input type="checkbox"/> (b)(7)(D) | <input type="checkbox"/> (k)(5) |
| <u> </u> | <input type="checkbox"/> (b)(7)(A) | <input checked="" type="checkbox"/> (b)(7)(E) | <input type="checkbox"/> <u> </u> |
| <u> </u> | | <input type="checkbox"/> (b)(7)(F) | |


47 additional page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component for review and direct response to you: Department of Justice, Criminal Division.

4 additional page(s) originated with another government component. **These records were found in the U.S. Attorney's Office files and may or may not be responsive to your request.** These records will be referred to the following component for consultation and our office will respond to you after their review: U.S. Marshals Service.

See additional information attached.

Although I am aware that this request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you that if you consider my response to be a denial of your request, you have the right to file an administrative appeal by writing within 60 days from the date of this letter to the **Office of Information and Privacy, United States Department of Justice, 1425 New York Avenue, Suite 11050, Washington, D.C. 20530-0001.** In light of the fact that this is an interim response, I would ask that you wait until the EOUSA has issued its final response in this request before you file an appeal.

Sincerely,


William G. Stewart II
Assistant Director

Enclosure(s)

EXPLANATION OF EXEMPTIONS

FOIA: TITLE 5, UNITED STATES CODE, SECTION 552

- (b)(1) (A) specifically authorized under criteria established by and Executive order to be kept secret in the in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order;
- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual.
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

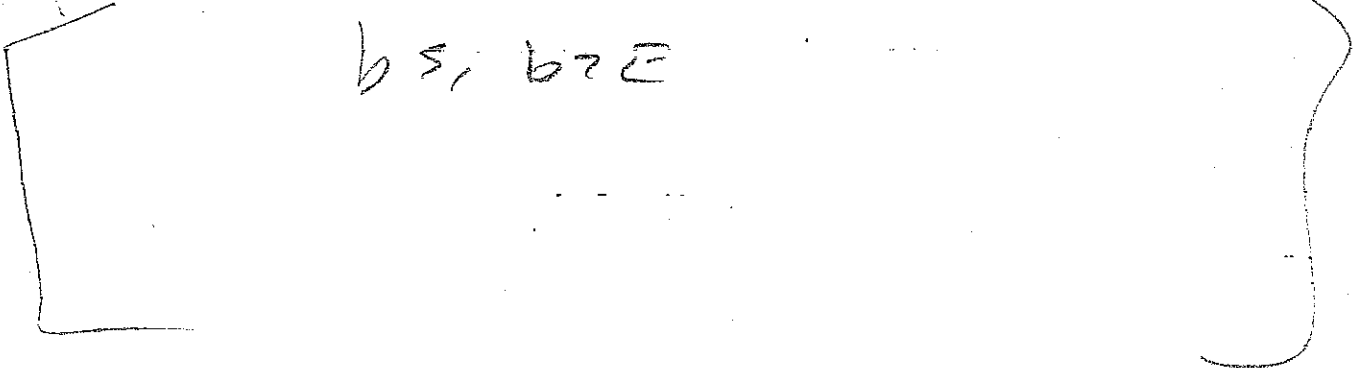
PRIVACY ACT: TITLE 5, UNITED STATES CODE, SECTION 552a

- (d)(5) information compiled in reasonable anticipation of a civil action proceeding;
- (j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;
- (k)(1) information which is currently and properly classified pursuant to Executive Order 12356 in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;
- (k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;
- (k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;
- (k)(4) required by statute to be maintained and used solely as statistical records;
- (k)(5) investigatory material compiled solely for the purpose of determining suitability eligibility, or qualification for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his identity would be held in confidence;
- (k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;
- (k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his identity would be held in confidence.

Bourgeois, Richard

From: Bourgeois, Richard
Sent: Friday, May 28, 2004 4:14 PM
To: USA-LAM-Criminal Attorneys
Subject: 18 U.S.C. 2703

Stan asked me to send out an email regarding the issues were are facing with the magistrate judges in our recent requests for cellular telephone records and subscriber information pursuant to 18 U.S.C. 2703.



If you have any questions about the judges specific concerns, or would like to discuss these issues further, please let me know.

Rich

RIP
b5, b7E

Bourgeois, Richard

From: Bourgeois, Richard
Sent: Friday, May 28, 2004 3:46 PM
To: Salomon, Rene
Subject: 18 USC 2703

Rene,

I know that you are on vacation right now, but when you get back next week let me know when you have some free time. We have some issues that have come up regarding the use of Pen Register / Trap and Trace orders in conjunction with 18 USC 2703 in order to assist in the location of fugitives.

bs

Thanks,
Rich

Richard L. Bourgeois, Jr.
Assistant United States Attorney
Russell B. Long Federal Courthouse
777 Florida Street, Suite 208
Baton Rouge, Louisiana 70801
Tel: 225-389-0443
Fax: 225-389-0561

REP
bs

[USABook Online](#) > [Criminal Procedure](#) > [Electronic Surveillance](#) > [Electronic Surveillance Manual](#) > **XV.**
[prev](#) | [next](#) | [help](#)

XV. The Legal Authorities Required to Locate Cellular Telephones

THIS ISSUE HAS BEEN THE SUBJECT OF EXTENSIVE LITIGATION RECENTLY. THE INFORMATION THAT USED TO APPEAR HERE IS NO LONGER CURRENT. IF YOU HAVE QUESTIONS OR CONCERNS, PLEASE CONTACT MARK ECKENWILER AT OEO (202) 616-0435.

RIF

[USABook Online](#) > [Criminal Procedure](#) > [Electronic Surveillance](#) > [Electronic Surveillance Manual](#) > XV.

[prev](#) | [next](#) | [help](#)

XV. The Legal Authorities Required to Locate Cellular Telephones

[The following analysis was prepared by attorney Richard W. Downing of the Computer Crime and Intellectual Property Section, Criminal Division, U.S. Department of Justice]

- I. [Compelling Providers to Disclose Cell-phone Location Records](#)
 - A. [Obtaining Historical Records from Cellular Providers](#)
 - B. [Compelling Providers to Collect Cell Phone Location Information Prospectively](#)
- II. [Collection of Cell Phone Location Information Directly by Law Enforcement](#)
 - A. [Use of Law Enforcement Cell Phone Tracking Devices Prior to the USA PATRIOT Act of 2001](#)
 - B. [The Pen/Trap Statute, As Amended By The USA PATRIOT Act of 2001](#)
 - C. [The Inapplicability of CALEA's Prohibition on Collection Using Pen/Trap Authority](#)
 - D. [Conclusion](#)

I. Compelling Providers to Disclose Cell-phone Location Records

In order to provide service to cellular telephones, providers have the technical capability to collect information such as the cell tower nearest to a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone. Depending on the number of towers in a particular area and other factors, this information may be used to identify the location of a phone to within a few hundred yards. Some providers routinely update this information at all times that the cell phone is turned on; others update it only when the user places a call. Carriers generally keep detailed historical records of this information for billing and other business purposes. At times, law enforcement authorities seek to compel carriers to preserve that information prospectively for use in a criminal investigation.

A. Obtaining Historical Records from Cellular Providers

Law enforcement investigators may use a search warrant or an order under [section 2703\(d\) of title 18](#) in order to obtain historical records from cellular carriers. Section 2703(c)(1) provides:

A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity

(A) obtains a warrant issued using the procedures described in the Federal Rules of criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

RIF

....

18 U.S.C. 2703(c)(1).

It remains doubtful whether law enforcement authorities may use a subpoena to obtain this same information. The amendments to section 2703(c) enacted in the USA PATRIOT Act of 2001 (the "USA PATRIOT Act") broadened the scope of records that may be obtained using a subpoena. In section 2703 (c), the Act changed "local and long distance telephone toll billing records" to "local and long distance telephone *connection* records, *or records of session times and durations.*" The legislative history does not comment on the intent of this change nor did this topic arise in any of the negotiations surrounding the passage of the Act. There is no evidence, however, that Congress expanded the scope of this definition in order to include cell phone location information. Thus, although there are arguments on both sides, the better practice is to use 2703(d) orders and search warrants -- rather than subpoenas -- to obtain cell phone location information from providers.

B. Compelling Providers to Collect Cell Phone Location Information Prospectively

In order to require a provider to collect cell-phone location information prospectively (e.g., for the following 60 days), law enforcement authorities must obtain a court order. One possibility is an order under section 3123, the Pen Register and Trap and Trace Statute ("Pen/Trap Statute"). The USA PATRIOT Act amended the definitions of "pen register" and "trap and trace device" to include any device or process that collects the "dialing, routing, addressing, and signaling information" associated with a communication. Although no legislative history directly addresses whether "signaling" includes such information as the nearest cell tower, the face used by that cell tower, and the signal strength, a House Judiciary Committee Report on a preceding bill (commenting on language identical to that eventually enacted in the USA PATRIOT Act) suggests that the pen/trap statute governs such information. It states:

This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media.*

H.R. Rept. 107-236, 107th Cong., 1st Sess. 53 (2001) (Rept. to Accompany H.R. 2975) ("House Report") (emphasis supplied). For a more in-depth discussion of this idea, see *infra* Section II.B.

Even if the pen/trap statute's amended definitions include such information, however, it remains doubtful that this non-specific language overrules the previously existing prohibition on carriers providing location information in response to a pen/trap order. In 1994, Congress explicitly prohibited providers from providing cell phone location information in response to a pen/trap order:

(a) ... a telecommunications carrier shall ensure that its equipment, facility or services that provide a customer or subscriber with the ability to originate, terminate, or direct communications are capable of --

...

(2) expeditiously isolating and enabling the government, pursuant to a court order or other lawful authorization, to access call-identifying information that is reasonably available to the carrier--

...

except that, with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices (as defined in section 3127 of title 18, United States Code), such call-identifying information shall not include any information that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number)....

Public Law 103-414, sec. 103(a) (1994) ("CALEA") (emphasis supplied). A court is likely to find that this clear expression of Congressional intent, which makes explicit reference to the definitions of pen registers and trap and trace devices, continues to prohibit providers from supplying cell phone location information in response to a pen/trap order.

Because of the 1994 prohibition, law enforcement authorities have sought other means to compel providers to supply this information prospectively. Most commonly, investigators have used orders under section 2703(d) to obtain this information. Although section 2703(d) generally applies only to stored communications, nothing in that section requires that the provider possess the records at the time the order is executed. Moreover, use of such an order does not improperly evade the intent of the CALEA prohibition. Section 2703(d) court orders provide greater privacy protection and accountability than pen/trap orders by requiring (1) a greater factual showing by law enforcement and (2) an independent review of the facts by a court. Indeed, the very language of the CALEA prohibition -- limiting its application "to information acquired *solely* pursuant to the authority for pen registers and trap and trace devices" -- indicates that Congress intended that the government be able to obtain this information using some other legal process. Public Law 103-414, sec. 103(a) (emphasis supplied). Thus, 2703(d) orders are an appropriate tool to compel a provider to collect cell phone location information prospectively.

Finally, some have suggested that such orders should rely on the Mobile Tracking Devices statute, 18 U.S.C. § 3117. Although making reference to this statute would not be harmful, it does not provide much legal support for such an order. The statute refers to the "installation" of a "mobile tracking device." This language probably would apply to the provider's use of a software program to track the location of a particular cell phone, even though such a program is not literally a physical "device."

More importantly, however, the language of section 3117 assumes that the court has authority from some other source to order the installation of the device. Section 3117 only gives the court authority to authorize the use of such a device outside of the court's jurisdiction. This added benefit will rarely be an issue where a court issues a 2703(d) order for the collection of cell phone location information by a provider, since amendments in the USA PATRIOT Act assure that 2703(d) orders have nationwide effect. Moreover, a provider may well be able to execute such an order at one central point and not require the "use" of the device outside of the court's jurisdiction.

II. Collection of Cell Phone Location Information Directly by Law Enforcement

Law enforcement possesses electronic devices that allow agents to determine the location of certain cellular phones by the electronic signals that they broadcast. This equipment includes an antenna, an electronic device that processes the signals transmitted on cell phone frequencies, and a laptop computer that analyzes the signals and allows the agent to configure the collection of information. Working together, these devices allow the agent to identify the direction (on a 360 degree display) and signal strength of a particular cellular phone while the user is making a call. By shifting the location of the device, the operator can determine the phone's location more precisely using triangulation.

In order to use such a device the investigator generally must know the target phone's telephone number (also known as a Mobile Identification Number or MIN). After the operator enters this information into the tracking device, it scans the surrounding airwaves. When the user of that phone places or receives a call, the phone transmits its unique identifying information to the provider's local cell tower. The provider's system then automatically assigns the phone a particular frequency and transmits other information that will allow the phone properly to transmit the user's voice to the cell tower. By gathering this information, the tracking device determines which call (out of the potentially thousands of nearby users) on which to home in. While the user remains on the phone, the tracking device can then register the direction and signal strength (and therefore the approximate distance) of the target phone.

A. Use of Law Enforcement Cell Phone Tracking Devices Prior to the USA PATRIOT Act of 2001

In 1994, the Office of Enforcement Operations opined that investigators did not need to obtain any legal process in order to use cell phone tracking devices so long as they did not capture the numbers dialed or other information "traditionally" collected using a pen/trap device. This analysis concluded that the "signaling information" automatically transmitted between a cell phone and the provider's tower does not implicate either the Fourth Amendment or the wiretap statute because it does not constitute the "contents" of a communication. Moreover, the analysis reasoned -- prior to the 2001 amendments -- that the pen/trap statute did not apply to the collection of such information because of the narrow definitions of "pen register" and "trap and trace device." Therefore, the guidance concluded, since neither the constitution nor any statute regulated their use, such devices did not require any legal authorization to operate.

B. The Pen/Trap Statute, As Amended By The USA PATRIOT Act of 2001

Although the analysis remains unchanged with respect to the Fourth Amendment and the wiretap statute, substantial amendments to the definitions of "pen register" and "trap and trace device" in the USA PATRIOT Act alter the applicability of the pen/trap statute. The new definitions, on their face, strongly suggest that the statute now governs the use of such devices. Where the old definition of "pen register" applied only to "numbers dialed or otherwise transmitted," "pen register" now means

a device or process which records or decodes dialing, routing, addressing, and signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted....

18 U.S.C. § 3127(3). "Signaling information" is a broader term that encompasses other kinds of non-content information used by a communication system to process communications. This definition appears to encompass all of the non-content information passed between a cell phone and the provider's tower.

Similarly, the USA PATRIOT Act broadened the definition of "trap and trace device." Where before the definition included only "the originating number of an instrument or device," the new definition covers "the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication...." 18 U.S.C. § 3127(4). Like the definition of "pen register," this broader definition appears to include such information as the transmission of a MIN, which identifies the source of a communication.

Moreover, the scant legislative history that accompanied passage of the Act suggests Congress intended that the new definitions apply to all communications media, instead of focusing solely on

traditional telephone calls. Although the House Report cannot definitively state the intent of both houses of Congress when passing the final bill, it does strongly suggest that Congress intended that the statute would apply to all technologies:

This section updates the language of the statute to clarify that the pen/register [sic] authority applies to modern communication technologies. Current statutory references to the target "line," for example, are revised to encompass a "line or other facility." Such a facility includes: *a cellular telephone number; a specific cellular telephone identified by its electronic serial number (ESN); an Internet user account or e-mail address; or an Internet Protocol (IP) address, port number, or similar computer network address or range of addresses.* In addition, because the statute takes into account a wide variety of such facilities, section 3123(b)(1)(C) allows applicants for pen register or trap and trace orders to submit a description of the communications to be traced using any of these or other identifiers.

Moreover, the section clarifies that orders for the installation of pen register and trap and trace devices may obtain *any* non-content information -- "dialing, routing, addressing, and signaling information" -- utilized in the processing and transmitting of wire or electronic communications....

This concept, that the information properly obtained by using a pen register or trap and trace device is non-content information, *applies across the board to all communications media ...* ([and includes] packets that merely request a telnet connection in the Internet context).

H.R. Rept 107-236, at 52-53 (emphasis added). Indeed, this last reference to a packet requesting a telnet session -- a piece of information passing between machines in order to establish a communication session for the human user -- provides a close analogy to the information passing between a cell phone and the nearest tower in the initial stages of a cell phone call.

Finally, the House Report recognizes that pen registers and trap and trace devices could include devices that collect information remotely. The Report states:

Further, because the pen register or trap and trace 'device' is often incapable of being physically 'attached' to the target facility due to the nature of modern communication technology, section 101 makes two other related changes. First, in recognition of the fact that such functions are commonly performed today by software instead of physical mechanisms, the section allows the pen register or trap and trace device to be 'attached or applied' to the target facility [such as an ESN]. Likewise, the definitions of 'pen register' and 'trap and trace device' in section 3127 are revised to include an intangible 'process' (such as a software routine) which collects the same information as a physical device.

H.R. Rept 107-236, at 53 (emphasis added). Thus, the statutory text and legislative history strongly suggest that the pen/trap statute governs the collection of cell phone location information directly by law enforcement authorities.

C. The Inapplicability of CALEA's Prohibition on Collection Using Pen/Trap Authority

In passing CALEA in 1994, Congress required providers to isolate and provide to the government certain information relating to telephone communications. At the same time that it created these obligations, it created an exception: carriers shall not provide law enforcement with "any information

that may disclose the physical location of the subscriber" in response to a pen/trap order. (A fuller quotation of the language appears, above, in Section I.B.). By its very terms, this prohibition applies only to information collected by a provider and not to information collected directly by law enforcement authorities. Thus, CALEA does not bar the use of pen/trap orders to authorize the use of cell phone tracking devices used to locate targeted cell phones.

D. Conclusion

The amended text of the pen/trap statute and the limited legislative history accompanying the 2001 amendments strongly suggest that the non-content information that passes between a cellular phone and the provider's tower falls into the definition of "dialing, routing, addressing, and signaling information" for purposes of the definitions of "pen register" and "trap and trace device." A pen/trap authorization is therefore the safest method of allowing law enforcement to collect such transmissions directly using its own devices.

TITLE II--ENHANCED SURVEILLANCE PROCEDURES

SEC. 216. MODIFICATION OF AUTHORITIES RELATING TO USE OF PEN REGISTERS AND TRAP AND TRACE DEVICES.

1. (a) GENERAL LIMITATIONS- Section 3121(c) of title 18, United States Code, is amended--

- (1) by inserting 'or trap and trace device' after 'pen register';
- (2) by inserting ', routing, addressing,' after 'dialing'; and
- (3) by striking 'call processing' and inserting 'the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications'.

(b) ISSUANCE OF ORDERS-

(1) IN GENERAL- Section 3123(a) of title 18, United States Code, is amended to read as follows:

(a) IN GENERAL-

(1) ATTORNEY FOR THE GOVERNMENT- Upon an application made under section 3122(a)(1), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device anywhere within the United States, if the court finds that the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. The order, upon service of that order, shall apply to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order. Whenever such an order is served on any person or entity not specifically named in the order, upon request of such person or entity, the attorney for the Government or law enforcement or investigative officer that is serving the order shall provide written or electronic certification that the order applies to the person or entity being served.

(2) STATE INVESTIGATIVE OR LAW ENFORCEMENT OFFICER- Upon an application made under section 3122(a)(2), the court shall enter an ex parte order authorizing the installation and use of a pen register or trap and trace device within the jurisdiction of the court, if the court finds that the State law enforcement or investigative officer has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

(3)(A) Where the law enforcement agency implementing an ex parte order under this subsection seeks to do so by installing and using its own pen register or trap and trace device on a packet-switched data network of a provider of electronic communication service to the public, the agency shall ensure that a record will be maintained which will identify--

(i) any officer or officers who installed the device and any officer or officers who accessed the device to obtain information from the network;

(ii) the date and time the device was installed, the date and time the device was uninstalled, and the date, time, and duration of each time the device is accessed to obtain information;

RIF

`(iii) the configuration of the device at the time of its installation and any subsequent modification thereof; and

`(iv) any information which has been collected by the device.

To the extent that the pen register or trap and trace device can be set automatically to record this information electronically, the record shall be maintained electronically throughout the installation and use of such device.

`(B) The record maintained under subparagraph (A) shall be provided ex parte and under seal to the court which entered the ex parte order authorizing the installation and use of the device within 30 days after termination of the order (including any extensions thereof).'

(2) CONTENTS OF ORDER- Section 3123(b)(1) of title 18, United States Code, is amended--

(A) in subparagraph (A)--

(i) by inserting 'or other facility' after 'telephone line'; and

(ii) by inserting before the semicolon at the end 'or applied'; and

(B) by striking subparagraph (C) and inserting the following:

`(C) the attributes of the communications to which the order applies, including the number or other identifier and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied, and, in the case of an order authorizing installation and use of a trap and trace device under subsection (a)(2), the geographic limits of the order; and'.

(3) NONDISCLOSURE REQUIREMENTS- Section 3123(d)(2) of title 18, United States Code, is amended--

(A) by inserting 'or other facility' after 'the line'; and

(B) by striking ', or who has been ordered by the court' and inserting 'or applied, or who is obligated by the order'.

(c) DEFINITIONS-

(1) COURT OF COMPETENT JURISDICTION- Section 3127(2) of title 18, United States Code, is amended by striking subparagraph (A) and inserting the following:

`(A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals having jurisdiction over the offense being investigated; or'.

(2) PEN REGISTER- Section 3127(3) of title 18, United States Code, is amended--

(A) by striking 'electronic or other impulses' and all that follows through 'is attached' and inserting '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'; and

(B) by inserting 'or process' after 'device' each place it appears.

(3) TRAP AND TRACE DEVICE- Section 3127(4) of title 18, United States Code, is amended--

(A) by striking 'of an instrument' and all that follows through the semicolon and inserting '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;'; and

(B) by inserting 'or process' after 'a device'.

(4) CONFORMING AMENDMENT- Section 3127(1) of title 18, United States Code, is amended--

(A) by striking 'and'; and

(B) by inserting ', and 'contents' after 'electronic communication service'.

(5) TECHNICAL AMENDMENT- Section 3124(d) of title 18, United States Code, is amended by striking 'the terms of'.

(6) CONFORMING AMENDMENT- Section 3124(b) of title 18, United States Code, is amended by inserting 'or other facility' after 'the appropriate line'.

A "triggerfish" can also be used to determine the cell site being used by a particular cellular telephone. In addition, the cellular telephone company should be able to provide cell site information. Once a cell site is determined, law enforcement agents can conduct surveillance in a more specific area in an effort to identify the user of the cellular telephone.

Practice note. See pen register forms (305-308) on USABook at <http://10.173.2.12/usao/eousa/ole/usabook/drug/forms>.

[USABook Online](#) > [Criminal Procedure](#) > [Electronic Surveillance](#) > [Electronic Surveillance Manual](#) > **XIV.**

[prev](#) | [next](#) | [help](#)

XIV. Cell Site Simulators/Digital Analyzers/Triggerfish

A cell site simulator, digital analyzer, or a triggerfish can electronically force a cellular telephone to register its mobile identification number ("MIN," *i.e.*, telephone number) and electronic serial number ("ESN," *i.e.*, the number assigned by the manufacturer of the cellular telephone and programmed into the telephone) when the cellular telephone is turned on. Cell site data (the MIN, the ESN, and the channel and cell site codes identifying the cell location and geographical sub-sector from which the telephone is transmitting) are being transmitted continuously as a necessary aspect of cellular telephone call direction and processing. The necessary signaling data (ESN/MIN, channel/cell site codes) are not dialed or otherwise controlled by the cellular telephone user. Rather, the transmission of the cellular telephone's ESN/MIN to the nearest cell site occurs automatically when the cellular telephone is turned on. This automatic registration with the nearest cell site is the means by which the cellular service provider connects with and identifies the account, knows where to send calls, and reports constantly to the customer's telephone a read- out regarding the signal power, status and mode.

If the cellular telephone is used to make or receive a call, the screen of the digital analyzer/cell site simulator/ triggerfish would include the cellular telephone number (MIN), the call's incoming or outgoing status, the telephone number dialed, the cellular telephone's ESN, the date, time, and duration of the call, and the cell site number/sector (location of the cellular telephone when the call was connected).

Digital analyzers/cell site simulators/triggerfish and similar devices may be capable of intercepting the contents of communications and, therefore, such devices must be configured to disable the interception function, unless interceptions have been authorized by a Title III order.

Because [section 3127](#) of Title 18 defines pen registers and trap and trace devices in terms of recording, decoding or capturing dialing, routing, addressing, or signaling information, a pen register/trap and trace order must be obtained by the government before it can use its own device to capture the ESN or MIN of a cellular telephone, even though there will be no involvement by the service provider. See discussion below in [Chapter XV](#).

USABook > Electronic Surveillance > Cell Site Simulators, Triggerfish, Cell Phones

A cell site simulator (sometimes called a digital analyzer, cell site locator, triggerfish, ESN reader, or swamp box) is a mobile device that can electronically force a cell phone to register its telephone number (MIN), electronic serial number (ESN), and information about its location, when the phone is turned on. This can be done without the user knowing about it, and without involving the cell phone provider.

Section 216 of the Patriot Act altered the definition of a pen register in 18 U.S.C. § 3127 (3) so that it includes these devices. Consequently, a pen register/trap and trace order must be obtained by the government before it uses such a device.

The use of a triggerfish to locate cellular telephones is an issue of some controversy. The Office of Enforcement Operations (OEO) encourages AUSAs to contact Mark Eckenwiler at (202) 616-0435 if they have questions or concerns.

Note. It may also be possible to flash the firmware of a cell phone so that you can intercept conversations using a suspect's cell phone as the bug. You don't even have to have possession of the phone to modify it; the "firmware" is modified wirelessly. This law enforcement tool was recently discussed in a Memorandum Opinion from SDNY, and has been getting a bit of news coverage lately. The authority for doing this can be found in 18 U.S. C. § 2518(11), but it sounds like something that you would not want to do without checking with OEO first.

See also:

- *Electronic Surveillance Manual* Chapter XIV
- Electronic Surveillance Issues
- *Federal Narcotics Prosecutions* § 3.16
- 76 ALR4th 536 ("Search and Seizure of Telephone Company Records Pertaining to Subscriber as Violation of Subscriber's Constitutional Rights")
- USABook topic pages: Electronic Surveillance; Pen Registers

updated 02/23/07

ELECTRONIC SURVEILLANCE

9-7.010 Introduction

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders -- Overview and History of Legislation

9-7.110 Format for the Authorization Request

9-7.111 Roving Interception

9-7.112 Emergency Interception

9-7.200 Video Surveillance -- Closed Circuit Television -- Department of Justice Approval Required When There Is A Reasonable Expectation of Privacy

9-7.250 Use and Unsealing of Title III Affidavits

9-7.301 Consensual Monitoring -- General Use

9-7.302 Consensual Monitoring -- "Procedures for Lawful, Warrantless Monitoring of Verbal Communications"

9-7.400 Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings

9-7.500 Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)

9-7.010 Introduction

This chapter contains Department of Justice policy on the use of electronic surveillance. The Federal electronic surveillance statutes (commonly referred to collectively as "Title III") are codified at 18 U.S.C. § 2510, *et seq.* Because of the well-recognized intrusive nature of many types of electronic surveillance, especially wiretaps and "bugs," and the Fourth Amendment implications of the government's use of these devices in the course of its investigations, the relevant statutes (and related Department of Justice guidelines) provide restrictions on the use of most electronic surveillance, including the requirement that a high-level Department official specifically approve the use of many of these types of electronic surveillance prior to an Assistant United States Attorney obtaining a court order authorizing interception.

Chapter 7 contains the specific mechanisms, including applicable approval requirements, for the use of wiretaps, "bugs" (oral interception devices), roving taps, video surveillance, and the consensual monitoring of wire or oral communications, as well as emergency interception procedures and restrictions on the disclosure and evidentiary use of information obtained through electronic surveillance. Additional information concerning use of the various types of electronic surveillance is also set forth in the **Criminal Resource Manual at 27.**

Attorneys in the Electronic Surveillance Unit of the Office of Enforcement Operations, Criminal Division, are available to provide assistance concerning both the interpretation of Title III and the review process necessitated thereunder. Interceptions conducted pursuant to

the Foreign Intelligence Surveillance Act of 1978, which is codified at 50 U.S.C. § 1801, *et seq.*, are specifically excluded from the coverage of Title III. *See* 18 U.S.C. § 2511(2)(a)(ii), (2)(e), and (2)(f).

9-7.100 Authorization of Applications for Wire, Oral, and Electronic Interception Orders -- Overview and History of Legislation

To understand the core concepts of the legislative scheme of Title III, one must appreciate the history of this legislation and the goals of Congress in enacting this comprehensive law. By enacting Title III in 1968, Congress prohibited private citizens from using certain electronic surveillance techniques. Congress exempted law enforcement from this prohibition, but required compliance with explicit directives that controlled the circumstances under which law enforcement's use of electronic surveillance would be permitted. Many of the restrictions upon the use of electronic surveillance by law enforcement agents were enacted in recognition of the strictures against unlawful searches and seizures contained in the Fourth Amendment to the United States Constitution. *See, e.g., Katz v. United States*, 389 U.S. 347 (1967). Still, several of Title III's provisions are more restrictive than what is required by the Fourth Amendment. At the same time, Congress preempted State law in this area, and mandated that States that sought to enact electronic surveillance laws would have to make their laws at least as restrictive as the Federal law.

One of Title III's most restrictive provisions is the requirement that Federal investigative agencies submit requests for the use of certain types of electronic surveillance (primarily the non-consensual interception of wire and oral communications) to the Department of Justice for review and approval before applications for such interception may be submitted to a court of competent jurisdiction for an order authorizing the interception. Specifically, in 18 U.S.C. § 2516(1), Title III explicitly assigns such review and approval powers to the Attorney General, but allows the Attorney General to delegate this review and approval authority to a limited number of high-level Justice Department officials, including Deputy Assistant Attorneys General for the Criminal Division ("DAAGs"). The DAAGs review and approve or deny proposed applications to conduct "wiretaps" (to intercept wire [telephone] communications, 18 U.S.C. § 2510(1)) and to install and monitor "bugs" (the use of microphones to intercept oral [face-to-face] communications, 18 U.S.C. § 2510(2)). It should be noted that only those crimes enumerated in 18 U.S.C. § 2516(1) may be investigated through the interception of wire or oral communications. On those rare occasions when the government seeks to intercept oral or wire communications within premises or over a facility that cannot be identified with any particularity, and a "roving" interception of wire or oral communications is therefore being requested, the Assistant Attorney General or the Acting Assistant Attorney General for the Criminal Division must be the one to review and approve or deny the application. (See the roving interception provision at 18 U.S.C. § 2518(11), discussed at **USAM 9-7.111.**)

In 1986, Congress amended Title III by enacting the Electronic Communications Privacy Act of 1986. Specifically, Congress added a new category of covered communications, i.e., "electronic communications," which would now be protected, and whose interception would be regulated, by Title III. Electronic communications are those types of non-oral or wire

communications that occur, *inter alia*, over computers, digital-display pagers, and facsimile ("fax") machines. *See* 18 U.S.C. § 2510(12).

Although the 1986 amendments permit any government attorney to authorize the making of an application to a Federal court to intercept electronic communications to investigate any Federal felony (18 U.S.C. § 2516(3)), the Department of Justice and Congress agreed informally at the time of ECPA's enactment that, for a three-year period, Department approval would nonetheless be required before applications could be submitted to a court to conduct interceptions of electronic communications. After that period, the Department rescinded the prior approval requirement for the interception of electronic communications over digital-display paging devices, but continued the need for Department approval prior to application to the court for the interception of electronic communications over any other device, such as computers and fax machines. Applications to the court for authorization to intercept electronic communications over digital-display pagers--which are the most commonly targeted type of electronic communications--may be made based solely upon the authorization of a United States Attorney. *See* 18 U.S.C. § 2516(3).

Because there are severe penalties for the improper and/or unlawful use and disclosure of electronic surveillance evidence, including criminal, civil, and administrative sanctions, as well as the suppression of evidence, it is essential that Federal prosecutors and law enforcement agents clearly understand when Departmental review and approval are required, and what such a process entails. *See* 18 U.S.C. §§ 2511, 2515, 2518(10), and 2520.

See the **Criminal Resource Manual at 31** for citations to relevant legislation.

9-7.110 Format for the Authorization Request

When Justice Department review and approval of a proposed application for electronic surveillance is required, the Electronic Surveillance Unit of the Criminal Division's Office of Enforcement Operations will conduct the initial review of the necessary pleadings, which include:

- A. The affidavit of an "investigative or law enforcement officer" of the United States who is empowered by law to conduct investigations of, or to make arrests for, offenses enumerated in 18 U.S.C. § 2516(1) or (3) (which, for any application involving the interception of electronic communications, includes any Federal felony offense), with such affidavit setting forth the facts of the investigation that establish the basis for those probable cause (and other) statements required by Title III to be included in the application;
- B. The application by any United States Attorney or his/her Assistant, or any other attorney authorized by law to prosecute or participate in the prosecution of offenses enumerated in 18 U.S.C. § 2516(1) or (3) that provides the basis for the court's jurisdiction to sign an order authorizing the requested interception of wire, oral, and/or electronic communications; and
- C. A set of orders to be signed by the court authorizing the government to intercept, or approving the interception of, the wire, oral, and/or electronic communications that are the subject of the application, including appropriate redacted orders to be served on any relevant providers of "electronic communication service" (as defined in 18 U.S.C. § 2510(15)).

9-7.111 Roving Interception

Pursuant to 18 U.S.C. § 2518(11)(a) and (b), the government may obtain authorization to intercept wire, oral, and electronic communications of specifically named subjects without specifying with particularity the premises within, or the facilities over which, the communications will be intercepted. (Such authorization is commonly referred to as "roving" authorization.) As to the interception of oral communications, the government may seek authorization without specifying the location(s) of the interception when it can be shown that it is not practical to do so. *See United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993), *cert. denied*, 114 S. Ct. 1644 (1994); *United States v. Orena*, 883 F. Supp. 849 (E.D.N.Y. 1995). An application for the interception of wire and electronic communications of specifically named subjects may be made without specifying the facility or facilities over which the communications will be intercepted when it can be shown that the subject or subjects of the interception have demonstrated a purpose to thwart interception by changing facilities. *See United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992), *cert. denied*, 113 S.Ct. 1859 (1993); *United States v. Villegas*, 1993 WL 535013 (S.D.N.Y. December 22, 1993).

When the government seeks authorization for roving interception, the Department's authorization must be made by the Attorney General, the Deputy Attorney General, the Associate Attorney General, an Assistant Attorney General, or an Acting Assistant Attorney General. *See* 18 U.S.C. § 2518(11)(a)(i) and (b)(I).

9-7.112 Emergency Interception

Title III contains a provision which allows for the warrantless, emergency interception of wire, oral, and/or electronic communications. Specifically, under 18 U.S.C. § 2518(7), the Attorney General (AG), the Deputy Attorney General (DAG), or the Associate Attorney General (AssocAG) may specially designate a law enforcement or investigative officer to determine whether an emergency situation exists that requires the interception of wire, oral, and/or electronic communications before a court order authorizing such interception can, with due diligence, be obtained. As defined by 18 U.S.C. § 2518(7), an emergency situation involves either: (1) immediate danger of death or serious bodily injury to any person; (2) conspiratorial activities threatening the national security interest; or (3) conspiratorial activities characteristic of organized crime. The only situations which will likely constitute an emergency are those involving an imminent threat to life, i.e., a kidnapping or hostage taking. *See United States v. Crouch*, 666 F. Supp. 1414 (N.D. Cal. 1987)(wiretap evidence suppressed because there was no imminent threat of death or serious injury); *Nabozny v. Marshall*, 781 F.2d 83 (6th Cir.)(kidnapping and extortion scenario constituted an emergency situation), *cert. denied*, 476 U.S. 1161 (1986). The emergency provision also requires that grounds must exist under which an order could be entered (*viz.*, probable cause, necessity, specificity of target location/facility) to authorize the interception. Once the AG, the DAG, or the AssocAG authorizes the law enforcement agency to proceed with the emergency Title III, the government then has forty-eight (48) hours, from the time the authorization was granted, to obtain a court order approving the emergency interception. 18 U.S.C. § 2518(7). The affidavit supporting the application for the order must contain only those facts known to the

AG, the DAG, or the AssocAG at the time his or her approval was given, and must be accompanied by a written verification from the requesting agency noting the date and time of the authorization. Failure to obtain the court order within the forty-eight-hour period will render any interceptions obtained during the emergency illegal.

Prior to the agency's contact with the AG, the DAG, or the Associate AG, oral approval to make the request must first be obtained from the Assistant Attorney General (AAG) or a Deputy Assistant Attorney General (DAAG) of the Criminal Division. This approval is facilitated by the Office of Enforcement Operation's Electronic Surveillance Unit, which is the initial contact for the requesting United States Attorney's Office and the requesting agency. Once the Electronic Surveillance Unit attorney briefs and obtains oral approval from the AAG or the DAAG, the attorney notifies the agency representative and the Assistant United States Attorney that the Criminal Division recommends that the emergency authorization proceed. The agency then contacts the AG, the DAG, or the AssocAG and seeks permission to proceed with the emergency Title III.

9-7.200 Video Surveillance -- Closed Circuit Television -- Department of Justice Approval Required When There Is A Reasonable Expectation of Privacy

Pursuant to Department of Justice Order No. 985-82, dated August 6, 1982, certain officials of the Criminal Division have been delegated authority to review requests to use video surveillance for law enforcement purposes when there is a constitutionally protected expectation of privacy requiring judicial authorization. This authority was delegated to the Assistant Attorney General, any Deputy Assistant Attorney General, and the Director and Associate Directors of the Office of Enforcement Operations.

When court authorization for video surveillance is deemed necessary, it should be obtained by way of an application and order predicated on Fed. R. Crim. P. 41(b) and the All Writs Act (28 U.S.C. § 1651). The application and order should be based on an affidavit that establishes probable cause to believe that evidence of a Federal crime will be obtained by the surveillance. In addition, the affidavit should comply with certain provisions of the Federal electronic surveillance statutes. See the **Criminal Resource Manual at 32** for additional discussion of video surveillance warrants.

Department policy requires that the video surveillance application and order be filed separately from, and not incorporated in, an application and order for electronic surveillance pursuant to 18 U.S.C. § 2518. When appropriate, the same affidavit may be submitted in support of both applications/orders.

9-7.250 Use and Unsealing of Title III Affidavits

When the government terminates a Title III electronic surveillance investigation, it must maintain under seal all of the Title III applications and orders (including affidavits and accompanying material) that were filed in support of the electronic surveillance. See 18 U.S.C. § 2518(8)(b); *In re Grand Jury Proceedings*, 841 F.2d 1048, 1053 n.9 (11th Cir. 1988) (although 18 U.S.C. § 2518(8)(b) refers only to "applications" and "orders," "applications" is construed to include affidavits and any other related documentation).

The purpose of this sealing requirement is to ensure the integrity of the Title III materials and to protect the privacy rights of those individuals implicated in the Title III investigation. *See* S.Rep. No. 1097, *reprinted in* 1968 U.S. Code Cong. & Admin. News 2112, 2193-2194. The applications may be unsealed only pursuant to a court order and only upon a showing of good cause under 18 U.S.C. § 2518(8)(b) or in the interest of justice under 18 U.S.C. § 2518(8)(d).

Thus, the government attorney should not attach Title III affidavits or other application material as exhibits to any search warrant affidavit, complaint, indictment, or trial brief. The government attorney may, nevertheless, use information from these materials or the Title III interceptions in documents such as search warrant affidavits, complaints, indictments, and trial briefs. *See* 18 U.S.C. § 2517(8)(a); 18 U.S.C. § 2517(1) and (2); and S.Rep. No. 1097 at 2188. In using this information, however, the government attorney must use care not to disclose publicly information from the Title III affidavits or interceptions that would either abridge the privacy interests of persons not charged with any crime or jeopardize ongoing investigations.

When Title III materials are sought by defense counsel or other persons and the privacy interests of uncharged persons are implicated by the contents of those materials, the government attorney should seek a protective order pursuant to Rule 16(d)(1), Fed. R. Crim. P., that will forbid public disclosure of the contents of the materials. Likewise, a Rule 16 protective order should be sought to deny or defer discovery of those portions of the affidavits and applications that reveal ongoing investigations when disclosure would jeopardize the success of any such investigation.

For discussion about disclosure of intercepted communications in civil litigation see the **Criminal Resource Manual at 33-34.**

9-7.301 Consensual Monitoring -- General Use

Section 2511(2)(c) of Title 18 provides that "It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception...." *See United States v. White*, 401 U.S. 745 (1971). As such, consensual interceptions need not be made under Title III procedures, interception orders under § 2518 are not available, and should not be sought in cases falling within § 2511(2)(c).

The Fourth Amendment to the U.S. Constitution, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communications Privacy Act of 1986 (18 U.S.C. § 2510, *et seq.*), and the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801, *et seq.*) permit government agents, acting with the consent of a party to a communication, to engage in warrantless interceptions of telephone communications, as well as oral and electronic communications. *White, supra*; *United States v. Caceres*, 440 U.S. 741 (1979). Similarly, Title III, by its definition of oral communications, permits Federal agents to engage in warrantless interceptions of oral communications when the communicating parties have no justifiable expectation of privacy. 18 U.S.C. § 2510(2). (No similar exception is contained in the definition of wire communications and, therefore, the nonconsensual

interception of wire communications violates 18 U.S.C. § 2511 regardless of the communicating parties' expectation of privacy, unless the interceptor complies with the court authorization procedures of Title III or with the provisions of the Foreign Intelligence Surveillance Act of 1978.) Since such interception techniques are particularly effective and reliable, the Department of Justice encourages their use by Federal agents for the purpose of gathering evidence of violations of Federal law, protecting the safety of informants and undercover law enforcement agents, or fulfilling other compelling needs. While these techniques are lawful and helpful, their use is frequently sensitive, so they must remain the subject of careful self-regulation by the agencies employing them.

The Department developed guidelines for the investigative use of consensual monitoring, which were promulgated most recently by the Attorney General on May 30, 2002. The guidelines do not apply to consensual monitoring of telephone conversations or radio transmissions. It was left to the enforcement agencies to develop adequate internal guidelines for the use of those aspects of this investigative tool. The following guidelines cover the investigative use of devices which intercept and record certain consensual verbal conversations where a body transmitter or recorder or a fixed location transmitter or recorder is used during a face-to-face conversation. In certain specified sensitive situations, under the regulations, the agencies must obtain advance written authorization from the Department of Justice. The guidelines on consensual monitoring set forth in the Attorney General's Memorandum of May 30, 2002, on that subject are contained in **USAM 9-7.302**.

9-7.302 Consensual Monitoring -- "Procedures for Lawful, Warrantless Monitoring of Verbal Communications"

The following text was taken from a memorandum on "Procedures for Lawful, Warrantless Monitoring of Verbal Communications" issued by the Attorney General on May 30, 2002:

I. DEFINITIONS

As used in this Memorandum, the term "agency" means all of the Executive Branch departments and agencies, and specifically includes United States Attorneys' Offices which utilize their own investigators, and the Offices of the Inspectors General.

As used in this Memorandum, the terms "interception" and "monitoring" mean the aural acquisition of oral communications by use of an electronic, mechanical, or other device. *Cf.* 18 U.S.C. §2510(4).

As used in this Memorandum, the term "public official" means an official of any public entity of government, including special districts, as well as all federal, state, county, and municipal governmental units.

II. NEED FOR WRITTEN AUTHORIZATION

A. Investigations Where Written Department of Justice Approval is Required. A request for authorization to monitor an oral communication without the consent of all parties to the communication must be approved in writing by the Director or Associate Directors of the Office of Enforcement Operations, Criminal Division, U.S. Department of Justice, when it is known that:

- (1) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
- (2) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;
- (3) any party to the communication is a member of the diplomatic corps of a foreign country;
- (4) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;
- (5) the consenting or nonconsenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or
- (6) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

In all other cases, approval of consensual monitoring will be in accordance with the procedures set forth in part V. below.

B. Monitoring Not Within Scope of Memorandum. Even if the interception falls within one of the six categories above, the procedures and rules in this Memorandum do not apply to:

- (1) extraterritorial interceptions;
- (2) foreign intelligence interceptions, including interceptions pursuant to the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. §1801, *et seq.*);
- (3) interceptions pursuant to the court-authorization procedures of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. §2510, *et seq.*);
- (4) routine Bureau of Prisons monitoring of oral communications that are not attended by a justifiable expectation of privacy;
- (5) interceptions of radio communications; and
- (6) interceptions of telephone communications.

III. AUTHORIZATION PROCEDURES AND RULES

A. Required Information. The following information must be set forth in any request to monitor an oral communication pursuant to part II.A.:

- (1) **Reasons for the Monitoring.** The request must contain a reasonably detailed statement of the background and need for the monitoring.
- (2) **Offense.** If the monitoring is for investigative purposes, the request must include a citation to the principal criminal statute involved.
- (3) **Danger.** If the monitoring is intended to provide protection to the consenting party, the request must explain the nature of the danger to the consenting party.
- (4) **Location of Devices.** The request must state where the monitoring device will be hidden: on the person, in personal effects, or in a fixed location.
- (5) **Location of Monitoring.** The request must specify the location and primary judicial district where the monitoring will take place. A monitoring authorization is not restricted to the original district. However, if the location of monitoring changes, notice should be promptly given to the approving official. The record maintained on the request should reflect the location change.
- (6) **Time.** The request must state the length of time needed for the monitoring. Initially, an authorization may be granted for up to 90 days from the day the monitoring is scheduled to begin. If there is the need for continued monitoring, extensions for additional periods of up to 90 days may be granted. In special cases (e.g., "fencing" operations run by law enforcement agents or long-term investigations that are closely supervised by the Department's Criminal Division), authorization for up to 180 days may be granted with similar extensions.
- (7) **Names.** The request must give the names of persons, if known, whose communications the department or agency expects to monitor and the relation of such persons to the matter under investigation or to the need for the monitoring.
- (8) **Attorney Advice.** The request must state that the facts of the surveillance have been discussed with the United States Attorney, an Assistant United States Attorney, or the previously designated Department of Justice attorney responsible for a particular investigation, and that such attorney advises that the use of consensual monitoring is appropriate under this Memorandum (including the date of such advice). The attorney must also advise that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division attorney shall notify the appropriate United States

Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

(9) Renewals. A request for renewal authority to monitor oral communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide an updated statement that the attorney advice required under paragraph (8) has been obtained in connection with the proposed renewal.

B. Oral Requests. Unless a request is of an emergency nature, it must be in written form and contain all of the information set forth above. Emergency requests in cases in which written Department of Justice approval is required may be made by telephone to the Director or an Associate Director of the Criminal Division's Office of Enforcement Operations, or to the Assistant Attorney General, the Acting Assistant Attorney General, or a Deputy Assistant Attorney General for the Criminal Division, and should later be reduced to writing and submitted to the appropriate headquarters official as soon as practicable after authorization has been obtained. An appropriate headquarters filing system is to be maintained for consensual monitoring requests that have been received and approved in this manner. Oral requests must include all the information required for written requests as set forth above.

C. Authorization. Authority to engage in consensual monitoring in situations set forth in part II.A. of this Memorandum may be given by the Attorney General, the Deputy Attorney General, the Associate Attorney General, the Assistant Attorney General or Acting Assistant Attorney General in charge of the Criminal Division, a Deputy Assistant Attorney General in the Criminal Division, or the Director or an Associate Director of the Criminal Division's Office of Enforcement Operations. Requests for authorization will normally be submitted by the headquarters of the department or agency requesting the consensual monitoring to the Office of Enforcement Operations for review.

D. Emergency Monitoring. If an emergency situation requires consensual monitoring at a time when one of the individuals identified in part III.B. above cannot be reached, the authorization may be given by the head of the responsible department or agency, or his or her designee. Such department or agency must then notify the Office of Enforcement Operations as soon as practicable after the emergency monitoring is authorized, but not later than three working days after the emergency authorization.

The notification shall explain the emergency and shall contain all other items required for a nonemergency request for authorization set forth in part III.A. above.

IV. SPECIAL LIMITATIONS

When a communicating party consents to the monitoring of his or her oral communications, the monitoring device may be concealed on his or her person, in personal effects, or in a fixed location. Each department and agency engaging in such consensual monitoring must ensure that the consenting party will be present at all times when the device is operating.

In addition, each department and agency must ensure: (1) that no agent or person cooperating with the department or agency trespasses while installing a device in a fixed location, unless that agent or person is acting pursuant to a court order that authorizes the entry and/or trespass, and (2) that as long as the device is installed in the fixed location, the premises remain under the control of the government or of the consenting party. *See United States v. Yonn*, 702 F.2d 1341, 1347 (11th Cir.), *cert denied*, 464 U.S. 917 (1983) (rejecting the First Circuit's holding in *United States v. Padilla* 520 F.2d 526 (1st Cir. 1975), and approving use of fixed monitoring devices that are activated only when the consenting party is present). *But see United States v. Shabazz*, 883 F.Supp. 422 (D.Minn. 1995).

Outside the scope of this Memorandum are interceptions of oral, nonwire communications when no party to the communication has consented. To be lawful, such interceptions generally may take place only when no party to the communication has a justifiable expectation of privacy -- for example, burglars, while committing a burglary, have no justifiable expectation of privacy. *Cf. United States v. Pui Kan Lam*, 483 F.2d 1202 (2d. Cir. 1973), *cert. denied*, 415 U.S. 984 (1974) -- or when authorization to intercept such communications has been obtained pursuant to Title III or the Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C. § 2510, et seq.) or the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801, et seq. Each department or agency must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted unless proper authorization has been obtained.

V. PROCEDURES FOR CONSENSUAL MONITORING WHERE NO WRITTEN APPROVAL IS REQUIRED

Prior to receiving approval for consensual monitoring from the head of the department or agency or his or her designee, a representative of the department or agency must obtain advice that the consensual monitoring is both legal and appropriate from the United States Attorney, an Assistant United States Attorney, or the Department of Justice attorney responsible for a particular investigation. The advice may be obtained orally from the attorney. If the attorneys described above cannot provide the advice for reasons unrelated to the legality or propriety of the consensual monitoring, the advice must be sought and obtained from an attorney of the Criminal Division of the Department of Justice designated by the Assistant Attorney General in charge of that Division. Before providing such advice, a designated Criminal Division attorney shall notify the appropriate United States Attorney or other attorney who would otherwise be authorized to provide the required advice under this paragraph.

Even in cases in which no written authorization is required because they do not involve the sensitive circumstances discussed above, each agency must continue to maintain internal procedures for supervising, monitoring, and approving all consensual monitoring of oral communications. Approval for consensual monitoring must come from the head of the agency or his or her designee. Any designee should be a high-ranking supervisory official at headquarters level, but in the case of the FBI may be a Special Agent in Charge or Assistant Special Agent in Charge.

Similarly, each department or agency shall establish procedures for emergency authorizations in cases involving non-sensitive circumstances similar to those that apply with regard to cases that involve the sensitive circumstances described in part III.D., including obtaining follow-up advice of an appropriate attorney as set forth above concerning the legality and propriety of the consensual monitoring.

Records are to be maintained by the involved departments or agencies for each consensual monitoring that they have conducted. These records are to include the information set forth in part III.A. above.

VI. GENERAL LIMITATIONS

This Memorandum relates solely to the subject of consensual monitoring of oral communications except where otherwise indicated. This Memorandum does not alter or supersede any current policies or directives relating to the subject of obtaining necessary approval for engaging in nonconsensual electronic surveillance or any other form of nonconsensual interception.

9-7.400 Defendant Motion or Discovery Request for Disclosure of Defendant Overhearings and Attorney Overhearings

See the **Criminal Resource Manual at 35**, for a discussion of the law related to disclosure of defendant overhearings and attorney overhearings.

9-7.500 Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)

In 2001, the USA PATRIOT Act (P.L. 107-56) amended the Pen Register and Trap and Trace Statute (pen/trap statute), 18 U.S.C. § 3121 et seq., to clarify that courts may issue pen/trap orders to collect the non-content information associated with Internet communications. One issue that has been raised in this regard is whether a pen register order may be used to collect (URLs), the terms that a person uses to request information on the World Wide Web (e.g., www.cybercrime.gov/PatriotAct.htm). Because of privacy and other concerns relating to the use of pen register orders in this fashion, use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS. Among the factors that should be considered in deciding whether to apply for such a pen register are (1) the investigative need for the pen register order, (2) the litigation risk in the individual case, (3) how much of any given URL would be obtained, and (4) the impact of the order on the Department's policy goals.

Consultation with CCIPS can help resolve these issues, as well as ensuring that the contemplated use of a pen register would be consistent with the Deputy Attorney General's May 24, 2002 Memorandum on "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."

This policy does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translated into URLs or portions of URLs. Similarly, this policy does not apply to the collection, at a web server, of tracing information indicating the source of requests to view a particular URL using a trap and trace order.

No employee of the Department will use the pen register authority to collect URLs without first consulting with the CCIPS of the Criminal Division. Absent emergency circumstances, such an employee will submit a memorandum to CCIPS that contains (a) the basic facts of the investigation, (b) the proposed application and order, (c) the investigative need for the collection of URLs, (d) an analysis of the litigation risk associated with obtaining the order in the context of the particular case, and (e) any other information relevant to evaluating the propriety of the application. In an emergency, such an employee may telephone CCIPS at (202) 514-1026 or, after hours at (202) 514-5000, and be prepared to describe the above information.

USABook > Criminal Procedure > Electronic Surveillance, Wiretaps, Title III

Department Policy

Manuals and Resource Materials

National Security (FISA)

Forms

Department policy on Electronic Surveillance issues is found in USAM 9-7.000 and Criminal Resource Manual 29-37. Requests made pursuant to Title III to conduct non-consensual, domestic surveillance of wire, oral, and electronic communications for law enforcement purposes are handled by the Electronic Surveillance Unit (ESU) of the Office of Enforcement Operations (OEO), Criminal Division, (202) 514-6809. ESU attorneys will also provide assistance in responding to suppression motions and preparing briefs on Title III issues.

On September 23, 2003, the Attorney General issued Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons and Guidelines Regarding Disclosure to the Director of Central Intelligence and Homeland Security Officials of Foreign Intelligence Acquired in the Course of a Criminal Investigation, specifying procedures that must be followed to disclose foreign intelligence acquired during electronic surveillance to the intelligence community.

On May 30, 2002, the Attorney General issued updated Guidelines on Lawful Warrantless Monitoring of Verbal Communications, Confidential Informants, FBI Undercover Operations, and General Crimes, RICO, and Terrorism Investigations.

In September, 2003, the *United States Attorneys' Manual* was amended to add new USAM 9-7.500, which provides in pertinent part that:

[t]he use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS This policy does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translated into URLs or portions of URLs. Similarly, this policy does not apply to the collection, at a web server, of tracing information indicating the source of requests to view a particular URL using a trap and trace order.

See also the Deputy Attorney General's May 24, 2002 Memorandum on "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."

USAM 9-7.302 (consensual monitoring) was substantially revised in September 2004. Here is a redline copy of the changes.

Manuals and Resource Materials

- The basics are in the Survey of Title III (January 2007 US Attys Bulletin).
- For a more detailed treatment, see the two ESU monographs: the

RIF

Electronic Surveillance Manual, and Electronic Surveillance Issues.

- *Federal Narcotics Prosecutions* (OLE 2004), now in its second edition, has chapters on wiretap and non-wiretap techniques.
- Two manuals devoted to crisis management published in 1999 have extensive guidance and forms regarding electronic surveillance; see the *Crisis Management Coordinators' Manual* ("CMC Manual") at § 5.B and the *Attorney General's Critical Incident Response Group Form Book* ("ACIRG Form Book") at Chapter 1. A condensed version of these materials was published by CTS in 2005. See also the USABook Critical Incident Response page.
- Related USABook topic pages: Cell Site Simulators (triggerfish); Searching and Seizing Computers; Pen Registers/Trap and Trace; FISA; Information Sharing; Narcotics; National Security; Patriot Act; Terrorism
- Chapter 2 of *Prosecuting Computer Crimes* ("Wiretap Act")
- Title III Seminar (February 2003 OLE course materials and forms)
- The Electronic Surveillance Bulletin; articles include Law enforcement access to stored communications; Time computation; Necessity; Use of civilian monitors; DOJ authorization; CALEA decision; Pager applications; and ELSU Staff listing.
- The September 1997 and November 1997 issues of the US Attys' Bulletin were dedicated to electronic surveillance issues. The articles included: Interview With Director Frederick D. Hess, Office of Enforcement Operations; The Office of Enforcement Operations -- Its Role in the Area of Electronic Surveillance; Electronic Surveillance Guide; Don't Forget To . . . ; Defending Wiretaps: "Think in the Beginning What the End Will Bring"; Wiretaps: A DEA Agent's Perspective; Interview with Special Agent Mark Styron; Electronic Surveillance: Does it Bug You?; So You've Always Wanted to do a Wiretap: Practical Tips If You Never Have; Wiretap Checklist; Common (and Uncommon) Problems Encountered During the Course of Title III Investigations Keeping Pace with the Mafia; Operation "Shattered Shield": Investigative and Trial Techniques Used to Jail "Dirty Cops"; The Story of "Operation Zorro II" and Some Practical Suggestions; Was Cellular Telephone Cloning a Crime Before October 1994?; Supervising and Litigating a Foreign Language Electronic Surveillance Interception. See also Recognizing and Meeting Title III Concerns in Computer Investigations, from the March 2001 issue.
- Georgetown Annual Review (2006).
- Search and seizure and intelligence intercepts; see also *War on Terrorism or Global Law Enforcement Operation?*, 78 Notre Dame L. Rev. 307 (January 2003).
- Sixth Circuit Criminal Trial Manual § 1.D. ("Electronic Surveillance");
- 4th Amendment, U.S. Constitution, with annotations, including " Electronic Surveillance

and the Fourth Amendment"

- Prosecuting Online Child Exploitation Cases
- The Electronic Privacy Information Center, Privacy.Org, and the Electronic Frontier Foundation collect unclassified government memoranda and publish material criticizing government electronic surveillance.

National Security (FISA). The ESU does not handle state wiretaps or requests to conduct domestic national security electronic surveillance (i.e. "FISA" requests per 50 U.S.C. §§ 1801-1829). Questions concerning FISA taps should be directed to the Office of Intelligence and Policy Review at (202) 514-5600. See also the FISA topic page.

Forms. Use the forms posted in Chapter 20 of the *Electronic Surveillance Manual*. If they don't cover your situation, look at the forms in the Federal Narcotics Prosecutions (March 2004), and the February 2003 OLE Title III Seminar materials.

updated 10/01/07

Chapter 3

Electronic Surveillance—Non-Wiretap

3.16

Cell site locator/digital analyzer (triggerfish)

A "triggerfish" or "swamp box" is a device that can intercept signals from a cellular telephone. This device has also been referred to as a digital analyzer and ESN reader. FCC regulations require all cellular telephones to contain an Electronic Serial Number, commonly referred to as the ESN. The ESN is electronically programmed in every telephone by chips and/or software. The Mobile Identification Number (MIN) is the actual telephone number for that cellular telephone. When a user turns on (powers up) a cellular telephone, the cellular telephone transmits the identity of the phone to the nearest cell site. The transmitted information is the ESN/MIN. These numbers allow the cellular system to identify the particular telephone and allow the cellular company to bill that particular telephone for the air-time charges. A cellular telephone that is powered up is exchanging this information with cell sites even though no call is in progress.

A "triggerfish" device can perform several functions. A "triggerfish" can intercept this identifying signal and "read" the Electronic Serial Number and Mobile Identification Number of the cellular telephone. From a law enforcement standpoint, if a law enforcement officer has a target that uses a cellular telephone, the officer can use a "triggerfish" to determine the ESN/MIN of the cellular telephone being used by the target. Once a law enforcement officer knows the ESN or MIN, a subpoena can be issued to all the cellular telephone companies in the area requesting the subscriber information and air-time billing records for that particular cellular telephone.

Based on Section 216 of the Patriot Act (pen register definition), it is the opinion of the Electronic Surveillance Unit, Office of Enforcement Operations, that a pen register order is required to intercept the electronic serial number of a cellular telephone. The amended definition includes "signaling information transmitted by an instrument" and includes such information as the ESN signal.

A "triggerfish" can also record the numbers dialed from a particular cellular telephone. If used in this way, the "triggerfish" meets any definition of a pen register and a pen register order must be obtained. With very little additional effort, the "triggerfish" can also intercept the conversations taking place on a particular cellular telephone. If used in this way, the "triggerfish" is intercepting wire communications and a wire intercept order is required; wiretaps are covered in Chapter 4 of this Manual.

RIF

USABook > Criminal Procedure > Electronic Surveillance > Pen Registers, Trap and Trace

- A **pen register**, also called a dialed number recorder (DNR), is a device that records the numbers dialed from a residential, business, or cellular telephone. A **trap and trace** is the reverse; it provides the telephone number calling a particular telephone.
- A traditional trap and trace requires the local telephone company to perform the trace and provide the information to the investigative agency. The more faster and modern practice is for investigative agency to request that Caller ID be activated on a target telephone, so that the the pen register records the originating telephone number.
- The installation and use of a pen register is not a search under the Fourth Amendment, and no warrant is required to install or use one. *Smith v. Maryland*, 442 U.S. 735, 745-46 (1979).
- The installation of a pen register or a trap and trace normally requires a court order pursuant to 18 U.S.C. §§ 3121-3127. General guidance on how to obtain a pen register or a trap and trace can be found in § 3.4 of *Federal Narcotics Prosecutions*. See also Chapter 13 of *Electronic Surveillance Issues*, and Chapter 13 of the *Electronic Surveillance Manual*. See also § 3.12 of *Federal Narcotics Prosecutions* (acting without a court order in emergencies).
- Forms are available in Chapter 20 of the *Electronic Surveillance Manual*.
- Minimization requirements, added to § 3121(c) pursuant to the Patriot Act, are outlined in a May 24, 2002, DAG Memorandum regarding the the Department's policy concerning the avoidance of "overcollection" in the use of pen registers and trap and trace devices.
- A request for a pen register or a trap and trace in a national security case is covered by the Foreign Intelligence Surveillance Act (FISA), and is handled by the Office of Intelligence Policy and Review (OIPR).
- "Post-cut-through digits" are any digits that are dialed from a telephone after the initial call setup is completed. This would include telephone numbers entered when a subject places a calling card, credit card, or collect call by first dialing a long-distance carrier access number and then, after the initial call is "cut through," dialing the telephone number of the destination party. See note 13 of this sample form from the *Electronic Surveillance Manual*.
- Pen registers cannot be used to collect Web Site addresses (URLs) without prior consultation with the Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division. See USAM 9-7.500.
- Section 216 of the Patriot Act altered the definition of a pen register in 18 U.S.C. § 3127 (3) so that it includes triggerfishes.
- For information on how to obtain subscriber information concerning a number recorded in a pen register or trap and trace, see § 3.7 of *Federal Narcotics Prosecutions*.

RIF

- A knowing violation of the pen register and trap and trace statutes can result in criminal liability pursuant to 18 U.S.C. § 3121(d), but suppression of evidence is not available as a remedy. See § 3.11 of *Federal Narcotics Prosecutions*.
- In *United States v. Forrester*, No. 05-50410 (9th Cir. July 6, 2007, amended July 25, 2007), the Ninth Circuit held that surveillance of email and Internet activity is akin to a pen register, and not a Fourth Amendment search:

The surveillance began in May 2001 after the government applied for and received court permission to install a pen register analogue known as a "mirror port" on Alba's account with PacBell Internet. The mirror port was installed at PacBell's connection facility in San Diego, and enabled the government to learn the to/from addresses of Alba's e-mail messages, the IP addresses of the websites that Alba visited and the total volume of information sent to or from his account.

- Related USABook topic pages: Cell Site Simulators; Electronic Surveillance

updated 07/31/07

13. Pen Register/Trap and Trace

Practice

Cell Site Simulator

The Legal Authorities Required to Locate Cellular Telephones

Recent Case re: Cell-site Data

Practice

Use of pen register does not constitute a search for purposes of Fourth Amendment analysis. *Smith v. Maryland*, 442 U.S. 735 (1979).

Both federal and Oregon courts recognize that trap and trace devices do not intercept the substance or content of communications, do not reveal the identity of the parties who might be communicating, and do not indicate whether a communication actually took place. Thus, the defendants (city and police officers) could not have disclosed the content of any communication, as the trap and trace devices did not intercept any communication. *American Agriculture, Inc. v. Shropshire*, 2001 U.S. Dist. LEXIS 13355 (D. Or.).

"Title III makes it clear that devices which satisfy the statutory definition of pen registers or trap and trace devices set forth in 18 U.S.C. § 3127 are exempted from its requirements. See 18 U.S.C. § 2511(2)(h)." *U.S. v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995).

Pen register's mere potential for an invasion of privacy does not implicate the Fourth Amendment. *U.S. v. Shnayderman*, 1993 WL 524782 (E.D. Pa.); *U.S. v. Love*, 859 F. Supp. 725 (S.D.N.Y. 1994).

Title III guards against actual infringements of privacy, not purely hypothetical ones. Section 2516(2)'s reference to compliance with state law for wiretap authorizations was not applicable to the pen registers employed here (New York state) and that section provided no basis for requiring the district court to hold a hearing to determine whether those pen registers, though not capable in the form used of intercepting the contents of wire communications, were capable of being modified to enable such interception. *U.S. v. Miller*, 116 F.3d 641 (2d Cir. 1997); *U.S. v. Veksler*, 62 F.3d 544 (3d Cir. 1995) ("mere suggestion that pen register equipment is now capable of misuse does not give us a basis to depart from the controlling precedent of the *Smith* case").

No suppression where fact of police officer's use of pen register for illegal "audio tests" was omitted from Title III affidavit, because if the information had been included in the affidavit it would not have diminished probable cause. *U.S. v. Lucht*, 18 F.3d 541 (8th Cir. 1994).

RIF

Magistrate judges in the Southern District of New York were authorized under 18 U.S.C. 3123 to issue orders for "the installation and use" of pen registers at DEA headquarters in the Southern District of New York to monitor telephones located in New Jersey. *U.S. v. Rodriguez*, 968 F.2d 130 (2d Cir. 1992); *U.S. v. Burford*, 755 F. Supp. 607 (S.D.N.Y. 1991) (District Court in the Southern District of New York had jurisdiction to issue order authorizing installation and use of pen register device "installed and used" at DEA headquarters in New York, even though the telephones being monitored were located in Maryland).

Information obtained from pen register can be used as evidence in criminal trial even though the court order authorizing its installation does not comply with statutory requirements. Statute (3121-3127) does not provide for exclusion. Suppression not warranted in the absence of a constitutional violation. *U.S. v. Thompson*, 936 F.2d 1249 (11th Cir. 1991); *U.S. v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995).

No suppression where government's inclusion in Title III affidavit of unauthorized pen register information collected during three day period between expiration and renewal of pen register order was not material. *U.S. v. Ishola*, 1996 WL 197461 (N.D. Ill. 4/19/96).

Judicial review in connection with pen register and trap and trace requests is not so narrowly limited and essentially ministerial as to subject the courts to discretion of the Executive in violation of the constitutional separation of powers. *U.S. v. Hallmark*, 911 F.2d 399 (10th Cir. 1990).

"The judicial role in approving use of trap and trace devices is ministerial in nature . . ." *U.S. v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995) (citing *Hallmark*).

The court must issue a pen register order on the mere statutory certification of the applicant that the information sought is relevant to an ongoing criminal investigation. *In re Application of U.S. for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device*, 846 F. Supp. 1555 (M.D. Fla. 1994); *U.S. v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995).

As long as the statutory prerequisites are met, there is no limitation on the number of times a pen register order may be extended. *In re Application of U.S. for Order Authorizing Installation and Use of Pen Register and Trap and Trace Device*, 846 F. Supp. 1555 (M.D. Fla. 1994) (citing and concurring in the opinion of United States District Judge Ralph W. Nimmons, Jr. (M.D. Fla., Nov. 17, 1993) (NO. 93-15-MISC-T-21)).

"We believe that the caller identification service is a "trap and trace device" as that term is defined in 18 U.S.C. s 3127(4)." *U.S. v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995).

The caller ID display unit itself is not a trap and trace device. The trap and trace is performed by the service provider's signaling equipment and software necessary to use the Caller ID display device. *Sparshott v. Feld Entertainment, Inc.*, 311 F.3d 425 (D.C. Cir. 2002).

Defendant argued that the Omaha Police Department did not properly obtain enhanced caller identification services under a pen register/trap and trace order issued by the state court because a

warrant or subpoena was not obtained pursuant to the requirements of 18 U.S.C. 2703 for access to the subscriber names that are supplied with enhanced caller ID services. The federal judge, however, found that the affidavits submitted to the state magistrate (pen register/caller ID application) and to the state court judge (wiretap application) were sufficient to make the showing (relevance and materiality to an ongoing criminal investigation) required by 2703(d) and therefore the judges' orders effectively authorized the use of enhanced caller identification services. *U.S. v. Escarcega*, 2000 U.S. Dist. LEXIS 10643 (D. Neb.).

"[W]e are not persuaded to hold that every device used in a criminal investigation which is not specifically authorized by statute is prohibited" *U.S. v. Fregoso*, 60 F.3d 1314 (8th Cir. 1995).

The Caller ID subscriber is the "user" referred to in section 3121(b)(3). By purchasing the Caller ID service, the subscriber consents to the trap and trace. *Ohio Domestic Violence Network v. Public Utilities Commission of Ohio*, 638 N.E.2d 1012 (Ohio 9/21/94). See also *Wisconsin Professional Police Association v. Public Service Commission of Wisconsin*, 555 N.W.2d 179 (Wis. Ct. App. 1996); *Southern Bell Tel. & Tel. Co. v. Hamm*, 409 S.E.2d 775 (S.C. 1991) (similar South Carolina state law)).

Police Department's use of "clone pagers" to intercept numeric transmissions to suspect's digital display pagers pursuant to state court "pen register" order cannot be considered the use of a "pen register" within the meaning of the ECPA, but was an unauthorized interception of electronic communications under 18 U.S.C. 2511. *Brown v. Waddell*, 50 F.3d 285 (4th Cir. 1995).

Cell Site Simulator

A cell site simulator (CSS) electronically "forces" a cellular telephone to autonomously register its MIN and ESN when the target telephone is turned on but is not being used.

The Legal Authorities Required to Locate Cellular Telephones

THIS ISSUE HAS BEEN THE SUBJECT OF EXTENSIVE LITIGATION RECENTLY. THE INFORMATION THAT USED TO APPEAR HERE IS NO LONGER CURRENT. IF YOU HAVE QUESTIONS OR CONCERNS, PLEASE CONTACT MARK ECKENWILER AT OEO (202) 616-0435.

Recent Case re: Cell-site Data

DEA's capture of defendant's cell-site data did not violate the defendant's Fourth Amendment or Title III rights. Assuming without deciding that cell-site data fits within the definition of "electronic communication," the Court points out that suppression is not a permissible statutory remedy under Title III for the illegal interception of an electronic communication. 18 U.S.C. 2510(1)(c). (The Court finds that a strong argument exists that cell-site data is not a form of communication at all, in that it is not a message and it is not exchanged between individuals, but

is just data sent from a cellular phone tower to the provider's computers.) Under the rationale of *U.S. v. Knotts*, 460 U.S. 276 (1983), the defendant has no legitimate expectation of privacy in the cell-site data because a person has no reasonable expectation of privacy regarding his travel on public thoroughfares, and the surveillance agents could have obtained the same information by following the defendant's car on the public highways. DEA simply used the cell-site data to "augment" sensory faculties, which is permissible under *Knotts*. Defendant's argument that DEA's use of the defendant's cell-site data effectively turned his cell phone into a tracking device within the meaning of 18 U.S.C. 3117, undermines the defendant's contention that suppression is appropriate under Title III. The definition of "electronic communication," 18 U.S.C. 2510(12)(C), excludes "any communication from a tracking device (as defined in section 3117 of this Title)" and thereby removes such tracking device communications from Title III coverage. Assuming, moreover, that the defendant is correct in his assertion that his phone was used as a tracking device, § 3117 does not provide a suppression remedy. *See U.S. v. Gbemisola*, 225 F.3d 753, 758 (D.C. Cir. 2000), where the court observed that, in contrast to other statutes governing electronic surveillance, § 3117 "does not *prohibit* the use of a tracking device in the absence of conformity with the section.... Nor does it bar the use of evidence acquired without a section 3117 order." (Emphasis in original.) The Court finds *Gbemisola* to be persuasive and likewise concludes that § 3117 does not provide a basis for suppressing the cell-site data. Defendant attempted to distinguish his case from *Smith v. Maryland*, 442 U.S. 735 (1979) in that he did not voluntarily convey his cell-site data to anyone, and did not in fact use his cell phone. The agent dialed defendant's cell phone and the dialing caused the phone to send signals to the nearest cell tower. The Court, however, finds that the distinction between the cell-site data and the defendant's location is not legally significant under the particular facts of this case. The cell-site data is simply a proxy for the defendant's visually observable location as to which the defendant has no legitimate expectation of privacy. The Supreme Court's decision in *Knotts* is controlling. The DEA agents did not conduct a search within the meaning of the Fourth Amendment when they obtained the defendant's cell-site data. *U.S. v. Forest*, 355 F.3d 942 (6th Cir. 2004).

Two magistrate judges have recently issued opinions rejecting use of the pen/trap statute and 2703 in applications seeking court orders for prospective acquisition of cell-site information. *See In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 2005 WL 2656621 (S.D. Tex. Oct. 14, 2005); *In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information*, 2005 WL 2739208 (E.D.N.Y. Oct. 24, 2005). The government maintains that the magistrate judges are wrong to assert that cell-site information is not "dialing, routing, addressing, or signaling information" under the Pen/Trap Statute. They are wrong to assert that cell-site information is not "a record or other information pertaining to a subscriber or customer" of an electronic communication service provider under ECPA. They are wrong to assert that the tracking device statute, 18 U.S.C. § 3117, requires a warrant based on probable cause to compel disclosure of cell-site information. They are wrong to assert that cell-phone users have a reasonable expectation of privacy in cell-site information.

From: Jones, Patricia (USALAM)
Sent: Thursday, December 13, 2007 8:47 AM
To: USALAM-Criminal-Attorneys
Cc: Blink, Daryl (USALAM)
Subject: ISP database

I've added an ISP database to the S drive. The folder is creatively named "ISP Database." It has contact information for serving subpoenas and other process on over 100 phone companies and ISPs. It can also generate 2703(f) preservation letters, 2703(d) applications, and subpoenas.

I may have installed something wrong because there is an error message when I pull it up. Hopefully, Daryl can take care of that by the time any of you need it.

Daryl, HELP!

RIF