



U.S. Department of Justice

Office of Information and Privacy

Telephone: (202) 514-3642

Washington, D.C. 20530

AUG 30 2007

Ms. Marcia Hofmann
Electronic Frontier Foundation
1875 Connecticut Avenue, NW
Suite 650
Washington, DC 20009

Re: DAG/07-R0227
CLM:VRB:LAD

Dear Ms. Hofmann:

This is a final response to your Freedom of Information Act request dated September 22, 2006, for records pertaining to pen register and trap and trace orders. This response concerns the two remaining documents that the Executive Office for United States Attorneys (EOUSA) located and forwarded to this Office for processing on behalf of the Office of the Deputy Attorney General. This response is being made on behalf of the Office of the Deputy Attorney General.

By letter dated August 8, 2007, we previously provided a response concerning the documents referred to this Office for processing on behalf of the Office of Attorney General, Legislative Affairs and Public Affairs. In that letter we also advised that we were consulting with another Department component on the remaining two documents which we determined to be responsive to your request. That consultation is now completed. I have determined that the two documents, consisting of seven pages are appropriate for release without excision and copies are enclosed.

Inasmuch as this completes our work on the documents that were referred by EOUSA for processing on behalf of the Office of the Deputy Attorney General, I am closing your file in this Office.

Sincerely,

Carmen L. Mallon
Chief of Staff

Enclosures



U.S. Department of Justice

Office of the Deputy Attorney General


The Deputy Attorney General

Washington, D.C. 20530

May 24, 2002

MEMORANDUM

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

FROM: Larry D. Thompson 

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

.....

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

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

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

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

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

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

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

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

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

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

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

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

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

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



Office of the Deputy Attorney General

Washington, D.C. 20530

February 6, 2003

MEMORANDUM FOR ALL HOLDERS OF THE UNITED STATES ATTORNEYS' MANUAL

FROM: THE DEPUTY ATTORNEY GENERAL 

United States Attorneys' Manual Staff
Executive Office for United States Attorneys

SUBJECT: Criminal Division Approval of Pen Registers and Trap and Trace Applications Involving the Collection of Uniform Resource Locators (URLs)

AFFECTS: All Titles with Criminal Prosecutions
(Titles 3, 4, 5, 6, 7, 8, 9)

The following creates a new section, 9-7.500 (Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division for Applications for Pen Register Orders Capable of Collecting Uniform Resource Locators (URLs)), in Title 9 (Criminal) of the United States Attorneys' Manual, with reference at 9-2.400 (Prior Approvals/Notification table). The new policy similarly has an impact on other titles in regard to their criminal prosecutions and notification/authorization tables. The new section sets forth policy regarding the requirement of prior consultation with the Computer Crime and Intellectual Property Section of the Criminal Division of certain applications for pen register orders.

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.

