United States District Court
District of Massachusetts

IN RE APPLICATION OF
THE UNITED STATES OF
AMERICA FOR AN ORDER
AUTHORIZING THE USE OF
A PEN REGISTER AND TRAP
ON [xxx]INTERNET SERVICE
ACCOUNT/USER NAME
[xxxxxxxx@xxx.com]

MAGISTRATE JUDGE DOCKET
NO. 2005M0499RBC

IN RE APPLICATION OF
THE UNITED STATES OF
AMERICA FOR AN ORDER
AUTHORIZING THE USE OF
A PEN REGISTER AND TRAP
ON [xxx] INTERNET SERVICE
ACCOUNT/USER NAME
[xxxxxxxxxxx@xxx.com]

MAGISTRATE JUDGE DOCKET
NO. 2005M0500RBC

IN RE APPLICATION OF
THE UNITED STATES OF
AMERICA FOR AN ORDER
AUTHORIZING THE USE OF
A PEN REGISTER AND TRAP
ON [xxxxxxx] HIGH SPEED
INTERNET SERVICE ACCOUNT
NO. [xxxxxxxxxxxxxxxx]

MAGISTRATE JUDGE DOCKET
NO. 2005M0501RBC

IN RE APPLICATION OF
THE UNITED STATES OF
AMERICA FOR AN ORDER
AUTHORIZING THE USE OF
A PEN REGISTER AND TRAP
ON [xxxxxxxxxxxx] INTERNET
SERVICE ACCOUNT NO.
[xxxxxxxxxx]

MAGISTRATE JUDGE DOCKET
NO. 2005M0502RBC

MEMORANDUM AND ORDER

COLLINGS, U.S.M.J.

The Department of Justice, through its Trial Attorney, has presented four applications for the use of pen registers and trap and trace devices on four internet service accounts. In the undersigned's view, the use of pen registers and trap and trace devices on such accounts poses problems which do not arise when such devices are installed on telephones. The Memorandum and Order is an attempt, albeit briefly, to identify those problems and hopefully to solve them to the extent possible.[1]

The governing statute is 18 U.S.C. § 3122(a)(1) which permits an attorney for the government to apply for "...an order under section 3123 of this

[1] Since pen registers and trap and trace devices are usually sought in the course of ongoing criminal investigations, time is somewhat of the essence. Hence, the within Memorandum and Order is "brief." The Court has taken the time it needed to deal with the issues but not so much time as it might have taken had it had the luxury of studying the problem thoroughly.

title authorizing or approving the installation and use of a pen register or a trap and trace device under this chapter, in writing under oath or equivalent affirmation, to a court of competent jurisdiction."

Title 18 U.S.C. § 3123(a)(1) provides, in pertinent part, that upon receiving the application,

> ...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 information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.

Title 18 U.S.C. § 3123(a)(1).

The order must limit the use of the pen register and/or trap and trace to a sixty day period, but application may be made to extend the use for additional sixty day periods. Title 18 U.S.C. § 3123(c).

Pen registers and trap and trace devices were installed on telephones so that the pen register could record the telephone numbers dialed out from a particular phone and trap and trace devices could record the telephone numbers dialing into a particular phone. However, in 2001 as part of the Patriot Act, Congress revised the definitions of "pen registers" and "trap and trace devices" so as to broaden the communications media upon which such devices could be

installed.

Thus, pen register is now defined as follows:

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

Title 18 U.S.C. § 3127(3).

Trap and trace device is now defined as follows:

> As used in this chapter, the 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.

Title 18 U.S.C. § 3127(4).

There can be no doubt that the expanded definition of a pen register, especially the use of the term "device or ***process",*** encompasses e-mail communications and communications over the internet. In other words, internet service providers can use a "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." Similarly, internet service providers can use a "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."

The problem in using a "pen register" and/or a "trap and trace device" on computers by which people are communicating over the internet is to insure that the information given to law enforcement "...not include the contents of any communication" as provided in section 3127(3)(4). This prohibition against revealing "content", which is contained in both the definition of a pen register and of a trap and trace device, applies to all pen registers and trap and trace devices. In other words, the government is not entitled to receive "...dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted" (pen register) or "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" (trap and trace device) if the "dialing, routing,

addressing and signaling information" reveals the "contents" of a communication.

In the telephone world, it would seem easy to distinguish numbers dialed out and numbers dialed in from the contents of the communications which occur after the connection has been made. But even then there may be problems. Suppose, for example, a person first dials a telephone number and then, after being connected, is asked to dial a second number such as a personal account number or social security number or any other identifying number in order to receive further information.[2] Would anyone doubt that although this action of dialing the second number creates "...dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted," the government would be prohibited from obtaining this information on a pen register because it contains the "content" of a communication? *See United States Telecom Association v. FCC,* 227 F.3d 450, 462 (D.C. Cir., 2000). But generally speaking, routine pen

---

[2] This is called "post-cut-through dialed digit extraction" which is defined as the "...use of tone-detection equipment to generate a list of all digits dialed after a call has been connected." *United States Telecom Association v. FCC,* 227 F.3d 450, 456 (D.C.Cir., 2000). "Such digits include not only the telephone numbers dialed after connecting to a dial-up long-distance carrier (e.*g.,* 1-800-CALL-ATT) but also, for example, credit card or bank account numbers dialed in order to check balances or transact business using automated telephone services." *Id.*

registers and trap and trace devices installed on telephones record only the numbers dialed out or dialed in and not the contents of any communication.

In the internet world, it seems to me the problem is greater. An obvious problem occurs when one considers e-mail. That portion of the "header" which contains the information placed in the header which reveals the e-mail addresses of the persons to whom the e-mail is sent, from whom the e-mail is sent and the e-mail address(es) of any person(s) "cc'd" on the e-mail would certainly be obtainable using a pen register and/or a trap and trace device. However, the information contained in the "subject" would reveal the contents of the communication and would not be properly disclosed pursuant to a pen register or trap and trace device.[3] After all, "'contents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport or meaning of that communication." Title 18 U.S.C. § 2510(8).

The use of a pen register to obtain the internet addresses accessed by a person presents additional problems. The four applications presently before me

---

[3] In the case of the four applications at issue before me, the Trial Attorney specifically states that he seeks no information from the "subject" line of any e-mails emanating from the internet address or being sent to the internet address. Whether the form of order he proposes be served on the internet provider is sufficient to put the provider on adequate notice that such information is not be disclosed is another question, discussed *infra*.

seek the Internet Protocol (IP) addresses which are defined as a "unique numerical address identifying each computer on the internet." The internet service provider would be required to turn over to the government the incoming and outgoing IP addresses "used to determine web-sites visited" using the particular account which is the subject of the pen register.

If, indeed, the government is seeking only IP addresses of the web sites visited and nothing more, there is no problem. However, because there are a number of internet service providers and their receipt of orders authorizing pen registers and trap and trace devices may be somewhat of a new experience, the Court is concerned that the providers may not be as in tune to the distinction between "dialing, routing, addressing, or signaling information" and "content" as to provide to the government only that to which it is entitled and nothing more.

Some examples serve to make the point. As with the "post-cut through dialed digit extraction" discussed, *supra,* a user could go to an internet site and then type in a bank account number or a credit card number in order to obtain certain information within the site. While this may be said to be "dialing, routing, addressing and signaling information," it also is "contents" of a communication not subject to disclosure to the government under an order

authorizing a pen register or a trap and trace device.

Second, there is the issue of search terms. A user may visit the Google site. Presumably the pen register would capture the IP address for that site. However, if the user then enters a search phrase, that search phrase would appear in the URL after the first forward slash. This would reveal content - - that is, it would reveal, in the words of the statute, "...information concerning the substance, purport or meaning of that communication." Title18 U.S.C. § 2510(8). The "substance" and "meaning" of the communication is that the user is conducting a search for information on a particular topic.

There may be other examples of instances in which "dialing, routing, addressing and signaling information," reveals the "contents" of communications as "contents" is defined. Due to time constraints (as previously noted, *see* n.1*, supra)* and an acknowledged dearth of technological savvy on the part of the undersigned, the Court will not at this time try to identify and discuss them.

In view of the foregoing, it seems that a mere statement in an order authorizing the installation of a pen register and/or a trap and trace device that the internet service provider is to disclose only "dialing, routing, addressing and signaling information" and not to reveal "contents" and, in addition, not to

disclose "dialing, routing, addressing and signaling information" which contains "contents" is insufficient notice to the internet service provider as to what may and may not be disclosed. Accordingly, in my judgment, an order to an internet service provider should contain a listing, to the extent possible, of what may NOT be disclosed pursuant to the order.

In addition, to impose upon the internet service providers the necessity of making sure that they configure their software in such a manner as to disclose only that which has been authorized, the Court will include a provision to the effect that a violation of the order, including the disclosure of prohibited information, may be found to be a contempt of Court and subject the violator to punishment. It is true that the internet service providers would be protected by the provisions of Title 18 U.S.C. § 3124(e) which provides that "[a] good faith reliance on a court order under this chapter…is a complete defense against any civil or criminal action brought under this chapter or any other law." However, to the extent that the order states with a degree of specificity what the internet service provider may disclose as well as what may not be disclosed, the likelihood that good faith errors will occur resulting in unauthorized disclosures will be minimized.

Thus, the Court shall issue the requested order authorizing the installation

of pen registers and trap and trace devices. However, the order shall contain the following language:

CAUTION

It is ORDERED that the pen register and trap and trace device installed in accordance with the within Order be configured to exclude all information constituting or disclosing the "contents" of any communications or accompanying electronic files.

"Contents" is defined by statute as any "...information concerning the substance, purport or meaning of that communication."

The disclosure of the "contents" of communications is prohibited pursuant to this Order even if what is disclosed is also "dialing, routing, addressing and signaling information."

Therefore, the term "contents" of communications includes subject lines, application commands, search queries, requested file names, and file paths. Disclosure of such information is prohibited by the within Order.

Violation of the within Order may subject an internet service provider to contempt of court sanctions.

In implementing the within Order, should any question arise as to whether the pen register and/or trap and trace device should be configured to provide or not to provide any particular category of information over and above those stated, the Trial Attorney and/or the internet service provider are invited to apply to this court for clarification and/or

guidance.

As experience with the use of pen registers and trap and trace devices on internet users increases and technology changes, there is no doubt that more problems will arise as to what constitutes the "contents" of communications. The foregoing represents the Court's best effort to deal with the issue at this point in time.

/s/ Robert B. Collings
ROBERT B. COLLINGS
United States Magistrate Judge

October 21, 2005.

Publisher Information

Note* This page is not part of the opinion as entered by the court. The docket information provided on this page is for the benefit of publishers of these opinions.

John P. McAdams, Trial Attorney
United States Department of Justice
Tax Division
Washington, DC