UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
ORLANDO DIVISION

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER AUTHORIZING THE INSTALLATION AND USE OF AN ELECTRONIC COMPUTERIZED DATA COLLECTION DEVICE EQUIVALENT TO A PEN REGISTER AND TRAP AND TRACE DEVICE

Case No. 6:06-mj-1130

ORDER

This cause comes before the Court for consideration of the United States' appeal of Magistrate Judge Karla R. Spaulding's Order (Doc. 7) partially denying the Government's application for the installation and use of a pen register and trap and trace device directed at a particular telephone number. In her May 23, 2006 Order, Judge Spaulding rejected the Government's request insofar as it sought capture of "post-cut-through" digits.[1] The United States defines "post-cut-through" digits as "any digits dialed by the subject after connecting to another carrier's service[.]" Amended Appeal at 1 n.2. Judge Spaulding reasoned that post-cut-through digits can disclose the content of communications, and 18 U.S.C. § 3127(3) & (4) prohibit the use of pen registers and trap and trace devices to capture such content. The Government frames the issue on appeal as "whether an application pursuant to 18 U.S.C. § 3121 et seq., the pen register/trap trace statutes, authorizes the Court to order the installation and use of a pen register device to register not only the numbers dialed

[1]Judge Spaulding granted the Government's application in other respects.

or pulsed from a mobile telephone, but also, to register post-cut-through digits." Amended Appeal at 2.

The Government concedes that "post cut-through" digits can include content. In that regard, the Government states:

> Some post-cut-through digits occur 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. Other post-cut-through digits can also represent content, such as when numbers are transmitted to an automated banking account, as passwords to voicemail systems, or as actual messages when transmitted to a pager or text message device and those numbers have meaning to the subjects.

Amended Appeal at 2 (citing *U.S. Telecom Ass'n v. F.C.C.*, 227 F.3d 450, 462 (D.C. Cir. 2000)). Additionally, in its legal memorandum supporting its most current application, the United States represents that "[c]urrent technology is unable to separate non-content dialed digits from content laden dialed digits[.]" Memorandum of Law at 52 (footnote omitted). By way of explanation, the Government states: "At the present time the only way to separate non-content from content digits is through contextual analysis; in other words, only when the numbers are received and analyzed will an investigator comprehend the proper category for any series of dialed digits." *Id.* at 52 n.22.

Essentially, the United States' position is that while the Government "cannot **target** contents (i.e., have them as the intended object of the order, with a view to deliberate collection and use)[,] [i]ncidental collection that is an unavoidable adjunct of collecting non-content data is absolutely permitted under the clear meaning of 18 U.S.C. § 3121(c)." Amended Appeal at 3 (emphasis in original). Section 3121(c) provides:

> A government 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.

The Government interprets § 3121(c) as permitting the incidental interception of call content, stating: "[R]ather than subjecting government agencies to the risk of contempt of court when content was inevitably intercepted as part of the execution of a pen register or trap and trace order, Congress established the more elastic requirement in 18 U.S.C. § 3121(c) that the government use 'technology reasonably available to it' to accomplish this end." Amended Appeal at 3.

Apparently, the question presented - whether "post-cut-through" digits may be obtained via an order authorizing a pen register or a trap and trace device - is one that has not yet been addressed in any published decision issued by a federal court. *U.S. Telecom Association* touched on the issue, but did not decide it. That case involved a challenge to an FCC order issued pursuant to the Communications Assistance for Law Enforcement Act of 1994 ("CALEA"), 47 U.S.C. § 1001 *et seq.* There, the Court of Appeals for the D.C. Circuit stated:

> The government contends that a law enforcement agency may receive all post-cut-through digits with a pen register order, subject to CALEA's requirement that the agency uses "technology reasonably available to it" to avoid processing digits that are content. 18 U.S.C. § 3121(c). No court has yet considered that contention, however, and *it may be that a Title III warrant is required to receive all post-cut-through digits.*

227 F.3d at 462 (emphasis added).

In *In re Application of U.S. for an Order Authorizing Use of a Pen Register and Trap*, 396 F. Supp. 2d 45 (D. Mass. 2005), the district court discussed the issue of intercepting dialed digit content, albeit in the context of a case involving the use of pen register/trap and trace devices on internet service accounts:

> 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. *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 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.

396 F. Supp. 2d at 47-48 (footnote omitted; emphasis added).

Turning to the present case, this Court rejects the United States' argument that it can obtain post-cut-through digits on the lesser showing permitted by the pen register and trap-and-trace statutes. Judge Spaulding correctly interpreted 18 U.S.C. § 3127(3) & (4) as flatly prohibiting the interception of communication content by pen registers and trap-and-trace devices. The statute seems plain in that respect, providing that information intercepted by pen registers and trap/trace devices "shall not include the contents of any communication[.]" § 3127(3) & (4). Further, this Court is unpersuaded by the Government's contention that the "technology reasonably available" language contained in § 3121(c) constitutes a blanket authorization for law enforcement agencies to intercept communication content, even incidentally, by means of pen register and trap/trace devices. In the Court's view, § 3121(c) operates as an additional privacy safeguard, rather than an enabling provision.

In any event, the United States' "incidental interception" position suffers from a fundamental flaw: by the Government's own admission, the determination of whether post-cut-through digits represent signaling information or communication content cannot be made until the data is analyzed, post-interception. Hence, it is impossible to ascertain in advance whether any particular post-cut-through digits represent communication content. By the time that analysis is undertaken, the horse is already out of the barn, *i.e.*, the invasion of privacy has already occurred. The Court is convinced that interpreting the statutory framework in the fashion urged by the United States would thwart § 3127's clear prohibition on the interception of content.

Additionally, the Department of Justice's written policy generally prohibiting the use of content intercepted by pen registers and trap/trace devices does not remedy the problem. The statutory

scheme at issue here does not merely proscribe the *use* of content; it prohibits *interception*. The DOJ policy permits interception in some circumstances, which is the point at which the statutory and constitutional violation occurs. Perhaps more fundamentally, this Court cannot cede to the executive branch its responsibility to safeguard the Fourth Amendment.

The Court thus determines that the United States' appeal is without merit. However, the Government is not without a remedy: if it decides that obtaining post-cut-through digits is sufficiently important to its criminal investigation, it may submit a wiretap application. Based on the foregoing, it is ORDERED that the May 23, 2006 Order (Doc. 7) issued by Judge Spaulding is AFFIRMED.

DONE and **ORDERED** in Orlando, Florida this 20th day of June, 2006.

ANNE C. CONWAY
United States District Judge

Copies furnished to:
Counsel of Record
Unrepresented Parties
Magistrate Judge Spaulding
Magistrate Judge Baker