## 18.6.9.10 (U) Post Cut-Through Dialed Digits (PCTDD)

### *18.6.9.10.1 (U) Overview*

(U//FOUO) Telecommunication networks provide users the ability to engage in extended dialing and/or signaling (also known as "post cut-through dialed digits" or PCTDD), which in some circumstances are simply call-routing information and, in others, are call content. For example, non-content PCTDD may be generated when a party 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. In other instances, PCTDD may represent call content, such as when a party calls an automated banking service and enters an account number, calls a pharmacy's automated prescription refill service and enters prescription information, or enters a call-back number when prompted by a voice mail service. See United States Telecom Assn v. Federal Communications Commission, 227 F.3d 450, 462 (D.C. Cir. 2000). After the initial "cut-through," a pen register and the equipment that supports it cannot tell the difference between digits that are dialed to connect a call and those that would otherwise be considered content.

(U//FOUO) The definition of both a pen register device and a trap and trace device provides that the information collected by these devices "shall not include the contents of any communication." See 18 U.S.C. § 3127(3) and (4). In addition, 18 U.S.C. § 3121(c) makes explicit the requirement to "use technology reasonably available" that restricts the collection of information "so as not to include the contents of any wire or electronic communications." "Content" includes any information concerning the substance, purport, or meaning of a communication. See 18 U.S.C. § 2510(8). When the pen register definition is read in conjunction with the limitation provision, however, it suggests that although a PR/TT device may not be used for the express purpose of collecting content, the incidental collection of content may occur despite the use of "reasonably available" technology to minimize, to the extent feasible, any possible over collection of content while still allowing the device to collect all of the dialing and signaling information authorized.

(U//FOUO) ***DOJ Policy:*** In addition to this statutory obligation, DOJ has issued a directive in the form of a DAG Memo (see below paragraph) to all DOJ agencies requiring that no affirmative investigative use may be made of PCTDD incidentally collected that constitutes content, except in cases of emergency—to prevent an immediate danger of death, serious physical injury, or harm to the national security.

(U//FOUO) Although the DAG Memo, dated May 24, 2002 on "Avoiding Collection and Investigative Use of "Content" in the Operation of Pen Registers and Trap and Trace Devices," as written, applies only to the issuance of criminal pen register orders pursuant to 18 U.S.C. § 3121 et seq., the potential collection of PCTDD-content also exists for pen registers authorized under FISA. As such, the principles outlined in the DAG Memo apply to pen registers authorized pursuant to the FISA as well as pen registers authorized pursuant to Title 18 of the United States Code. **In instances in which PCTDD are collected pursuant to FISA, the government may not make any affirmative investigative use of the information, even in cases of emergency, without authorization from the FISC.** Any such emergency use must be recorded in the respective investigative files.

### *18.6.9.10.2 (U) Collection of PCTDD*

(U//FOUO) When requesting pen register collection, the field office case agent must affirmatively decide whether to receive PCTDD during the course of a pen register collection. If no selection is made, the default is set not to collect PCTDD.

A) (U//FOUO) The case agent shall, consistent with DIOG Section 18.6.9.10.1, submit an electronic technical request form that states whether PCTDDs are to be collected—for example, when the order authorizes the "recording or decoding of all dialing, routing, addressing, or signaling information." This selection is accomplished by marking the "Post Cut through Dialed Digits Authorized" check box for each monitored target. If this selection is not made, the PCTDD will not be collected or presented in any collection report.

B) (U//FOUO) The case agent shall advise the technically trained agent (TTA) promptly upon learning that a particular pen register order expressly prohibits the collection or retention of PCTDD. The technical agent shall then take all reasonable steps to ensure compliance with the restrictive order, including coordinating with the service provider and with OTD personnel regarding the use of technology reasonably available to avoid the collection of all PCTDD.

### *18.6.9.10.3 (U) Use of PCTDD*

(U//FOUO) If PCTDD information is collected pursuant to an authorized pen register, the following steps must be taken by all FBI personnel when reviewing pen register derived information to avoid the use of the contents of communications that may be contained within the string of digits:

A) (U//FOUO) Prior to examining any PCTDD, identify—through use of administrative subpoena or other investigative means—the subscriber of the phone number to whom the initial connection was made (i.e., the origination number).

1) (U//FOUO) If the origination number does not appear to be pertinent to the investigation, no examination of any PCTDD associated with that initial phone number shall be made, absent an investigative need to examine the PCTDD.

2) (U//FOUO) If the initial connection is determined to be to a financial institution as defined in the Right to Financial Privacy Act, 12 U.S.C. § 3401(1), PCTDD may not be examined, because there is reason to believe that the PCTDD may contain the contents of a communication, such as a bank account number.

3) (U//FOUO) The fact that the target called the bank, however, can be used for investigative or intelligence purposes, such as to subpoena bank records associated with the target; but any PCTDD cannot be used in the subpoena (such as a bank account number) or later to confirm information received from the bank.

4) (U//FOUO) If the initial connection is determined to be an entity for which it is reasonable to believe that the PCTDD would contain dialing or signaling information, such as a calling card number, a call spoof card service, a company otherwise providing direct access to a telephone service, or a business entity, the PCTDD may be examined to identify the ultimate destination of the call, or any other associated signaling or routing information, such as a calling card PIN or calling card account number. If the initial connection is to a business entity, like a hotel, for example, the PCTDD may be examined to determine if an extension number was dialed.

5) (U//FOUO) If, when examining PCTDD, numbers are encountered that constitute "content" of a communication, except as provided below, those numbers may not be used for any affirmative investigative purpose. In essence, those numbers must be treated as though they did not exist and cannot be used for any purpose. To the extent the information is included in any document for analytic or investigative use, the PCTDD numbers that constitute "content" must be redacted.

B) (U//FOUO) ***Emergency Use:*** In an emergency, PCTDD that constitutes content may be used as necessary in criminal investigations to prevent immediate danger of death, serious physical injury, or harm to the national security. **In instances in which PCTDD are collected pursuant to FISA, the government may not make any affirmative investigative use of the information, even in cases of emergency, without authorization from the FISC.**

1) (U//FOUO) ***Approval:*** In criminal investigations only, an SSA or SIA, who reasonably determines that an emergency situation exists that requires the use of PCTDD content relating to the emergency, may approve the use of such PCTDD without delay.

2) (U//FOUO) ***Notification:*** Within five (5) business days of such emergency use, the use of the particular PCTDD content must be documented in an EC to the appropriate investigative files (i.e., the investigation in which the pen register information was derived and the investigation in which it was used) with notification to the CDC and the FBI General Counsel, OGC (Investigative Law Unit for criminal pen registers and National Security Law Branch for FISA pen registers).

### 18.6.9.10.4 (U) WHAT CONSTITUTES PCTDD CONTENT

(U//FOUO) In applying the above, the term "content" is interpreted to mean "any information concerning the substance, purport, or meaning of a communication" as defined in 18 U.S.C. § 2510. Questions concerning whether specific PCTDD are content as opposed to dialing, routing, addressing, or signaling information should be addressed to the CDC or OGC for coordination with DOJ as necessary.

(U//FOUO) ***Exemption:*** This policy does not pertain to e-mail or Internet account pen register surveillance because such electronic communications do not generate PCTDD. Nor does the policy pertain to PCTDD obtained pursuant to a Title III or FISA electronic surveillance

order, because such orders authorize the interception of contents of communications associated with the targeted phone number.