


Memorandum

Subject: 18 U.S.C. Section 2703(d) orders for cell site information	Date: August 23, 2005
To: Hon. Stephen Wm. Smith United States Magistrate Judge	From: Chuck Rosenberg  United States Attorney

A. Introduction:

To receive service from a cell phone provider, a cell phone owner must transmit a signal to a nearby cell tower to register his presence with the network. Cell phone service providers keep track of such information in a database; they must maintain this information to complete calls to the cell phone. Service providers have the technical capability to collect information including the cell tower currently serving a particular cell phone, the portion of that tower facing the phone, and often the signal strength of the phone. The government often seeks cell-site information in order to locate fugitives or other targets of criminal investigations.

Traditionally, the government has obtained this information by relying in part on 18 U.S.C. §§ 2703(c) & (d), which allow the government to obtain a court order compelling disclosure of non-content records of a subscriber of an electronic communication service after presenting “specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought are relevant and material to an ongoing criminal investigation.” In a memorandum dated June 10, 2005 (“Memorandum”), you raised two primary objections to this process. First, you suggested that a cell phone is a “tracking device”

and that records related to tracking devices fall outside the scope of Title II of the Electronic Communications Privacy Act of 1986, now codified as amended in 18 U.S.C. §§ 2701-2712 (“Stored Communications Act” or “SCA”¹). Memorandum at 6-10. Second, you argued that the SCA’s organizational structure demonstrates that 2703(d) orders are inherently retrospective: for example, the SCA includes no duration period for 2703(d) orders. Memorandum at 10-11. You also argued that legislative history does not support the government’s position that 2703(d) orders may be used for prospective collection of cell-site information. Memorandum at 11-17.

In this memorandum, we set forth our understanding of the legal authorities required to compel disclosure of cell-site information on a prospective basis: such disclosure should be done under the combined authority of both the pen/trap statute and § 2703 of the SCA. Our argument has four primary components. First, respectfully, it is incorrect to state “the government makes no claim that the pen/trap provisions of the ECPA authorize access to cell site data.”

Memorandum at 3. Prospective collection of cell-site information falls squarely within the pen/trap statute, and the provisions of that statute govern such collection. However, the pen/trap statute by itself is insufficient authority for such collection, as Congress has forbidden a provider to disclose cell-site information “solely pursuant” to a pen/trap order. 47 U.S.C. § 1002(a)(2)(B).

¹ Although the provisions now codified at 18 U.S.C. §§ 2701-2712 are often referred to as the “ECPA,” the use of the “ECPA” to refer to those provisions sometimes creates confusion, as the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), also amended the wiretap statute to encompass electronic communications and created the pen/trap statute. To avoid confusion, this memorandum refers to 18 U.S.C. §§ 2701-2712 as the “Stored Communications Act” or “SCA,” 18 U.S.C. §§ 2510-2522 as the “Wiretap Act,” 18 U.S.C. §§ 3121-3127 as the “pen/trap statute,” and the Electronic Communications Privacy Act of 1986 as the “ECPA.”

Second, §§ 2703(c) & (d) of the SCA provide authority for collection of cell-site information. In particular, cell-site information constitutes “record[s] or other information pertaining to a subscriber to or customer of [an electronic communication] service (not including the contents of communications).” 18 U.S.C. § 2703(c)(1). Cell-site information thus falls within the scope of the SCA, and its disclosure may be compelled pursuant to an “articulable facts” order issued under 18 U.S.C. § 2703(d).

Third, the structural argument – that the SCA lacks prospective procedural features and is thus inherently retrospective – fails for two reasons. First, such a structural argument is unavailing because prospective collection of cell-site information is proper under the plain language of the SCA. Although the SCA applies only to stored communications, nothing in the SCA requires that the records be stored at the time the order for their disclosure is issued. Second, there is no reason for the SCA to contain such features. Both the SCA and the pen/trap statute govern prospective collection of cell-site information. Thus, when the SCA is used prospectively to gather cell-site information, the collection will also be governed by the pen/trap statute, which includes prospective procedural features. Thus, the SCA itself need not contain such features, as the pen/trap statute supplies them.

Fourth, cell phones do not fall within a “tracking device exclusion” from the SCA. Cell phones are not “tracking devices” within the meaning of 18 U.S.C. § 3117, and such a conclusion would be contrary to the language, structure, and purpose of ECPA. Moreover, under the plain language of the SCA, cell phone service providers are providers of “electronic communication service” subject to the SCA regardless of whether cell phones are classified as tracking devices.

In addition to these four primary components of the government’s argument, this memorandum addresses the related statutes you discuss: the Communications Assistance for Law Enforcement Act (“CALEA”), the Wireless Communication and Public Safety Act of 1999 (“WCPSA”), and the USA PATRIOT Act of 2001 (“Patriot Act”). See Memorandum at 11-17. Nothing in those statutes or their legislative history suggests that 2703(d) orders for cell-site information are improper.

B. The pen/trap statute governs collection of cell-site information, but it requires the government to rely on additional statutory authority.

The plain text of the pen/trap statute requires the government to obtain a pen/trap order for prospective collection of cell-site information. As explained in this section, the basis for this requirement is straightforward: such collection falls within the definitions of “pen register” and “trap and trace device,” see 18 U.S.C. §§ 3127(3) & (4), and the pen/trap statute thus mandates that the government obtain a pen/trap order for its collection. See 18 U.S.C. § 3121(a). Statutorily, prospective collection of cell-site information differs from other pen/traps in only one respect: cell-site information may not be produced “solely pursuant” to a pen/trap order. 47 U.S.C. § 1002(a)(2)(B).

When the pen/trap statute was first enacted in 1986, pen registers and trap and trace devices were given narrow definitions, which pertained explicitly to the capture of telephone numbers. For example, “pen register” was defined in part to mean “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” ECPA § 301, Pub. L. No. 99-508, 100 Stat. 1848 (1986). However, as communications networks developed, federal law

enforcement began to use pen/trap orders to collect additional categories of non-content information. For example, a pen/trap order was used on an e-mail account to locate fugitive James Kopp, who evaded capture for three years after murdering a doctor. See Fighting Cyber Crime: Hearing Before the Subcommittee on Crime of the Committee on the Judiciary, 107th Cong., 1st Sess. 47-48 (2001) (statement of Michael Chertoff, Assistant Attorney General, Criminal Division, U.S. Dep't of Justice) (at judiciary.house.gov/legacy/chertoff_061201.htm). Nevertheless, under the initial definitions of “pen register” and “trap and trace device,” questions remained about the proper role of pen/trap orders in collecting broad categories of non-content information. See id.

After the enactment of the ECPA in 1986, the enactment of CALEA, Pub. L. No. 103-414, 108 Stat. 4279 (1994), was the next significant change to the pen/trap statute. With CALEA, Congress restricted the use of pen/trap orders to obtain cell-site information. However, it is critical to note the mechanism through which Congress accomplished this restriction. Congress did not simply forbid the use of pen/trap orders to obtain such information. Instead, it prohibited the disclosure of cell-site information “solely pursuant” to a pen/trap order:

(a) ... a telecommunications carrier shall ensure that its equipment, facilities, 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). . . .

CALEA § 103(a), codified at 47 U.S.C. § 1002.² Congress’s use of the “solely pursuant” language suggests two features of the post-CALEA pen/trap statute: that the pen/trap statute could potentially apply to collection of cell-site information, but that additional authority beyond the pen/trap statute should be sought for such collection.

Any remaining ambiguity over whether pen registers and trap and trace devices were narrowly limited to telephone numbers was eliminated by the USA PATRIOT Act of 2001 § 216, Pub. L. No. 107-56, 115 Stat. 272 (2001) (“Patriot Act”). The Patriot Act amended the definitions of “pen register” and “trap and trace device” to make clear that the pen/trap statute applies to a broad variety of communications technologies and allows the collection of a broad range of non-content information. “Pen register” is now defined to mean:

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). Similarly, “trap and trace device” is now defined to mean

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). Prospective collection of cell-site information falls within the scope of these expanded definitions for “pen register” and “trap and trace device,” as cell-site information

² By its terms, this provision applies only to compelled disclosure from telecommunications carriers. The government may rely on pen/trap orders when it independently collects call-identifying information that discloses a subscriber’s location.

constitutes “dialing, routing, addressing, and signaling information.”³ In particular, cell-site information is used by carriers to route calls to and from their proper destination.

Because collection of cell-site information falls within the expanded definition of “pen register” and “trap and trace device,” the government must seek a pen/trap order before collecting it. The pen/trap statute specifies that “no person may install or use a pen register or a trap and trace device without first obtaining a court order under section 3123 of this title” 18 U.S.C. § 3121(a). However, the Patriot Act did not repeal CALEA’s restriction that a provider should not disclose cell-site information solely pursuant to a pen/trap order. As a result, the pen/trap statute governs prospective collection of cell-site information, but the government must also rely on additional authority for such collection.

- C. Collection of cell-site information is authorized by the SCA pursuant to a 2703(d) order.

Section 2703 of the SCA regulates government access to communications stored by network service providers by creating a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications. The structure of the SCA reflects a series of classifications that indicate congressional judgment about what kinds of information implicate greater or lesser privacy interests. Some information may be obtained from providers only with a warrant based on probable cause, while other information

³ The House Report on the bill that became the Patriot Act notes 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 or transmitting of wire and electronic communications.” H.R. Rep. No. 236(I), 107th Cong. 1st Sess. at 53 (2001) (emphasis added). The report further explained the broad scope of pen/trap information: “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.” Id.

may be obtained with a 2703(d) order or even a subpoena. As set forth in this section, cell-site information is properly classified as “record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).” 18 U.S.C. § 2703(c)(1). Thus, the government may obtain a court order under 18 U.S.C. § 2703(d) compelling its disclosure.

As an initial matter, cell-site information is non-content information: it does not concern the “substance, purport, or meaning” of a communication. See 18 U.S.C. § 2510(8). Thus, disclosure of cell-site information is governed by § 2703(c) of the SCA, rather than § 2703(a) or § 2703(b), which both govern compelled disclosure of the contents of communications.

Section 2703(c) sets forth two categories of non-content information: a general category of “record[s] or other information pertaining to a subscriber to or customer of such service” in § 2703(c)(1) and a category of basic subscriber records specifically identified in § 2703(c)(2). Disclosure of either category of records may be made pursuant to a 2703(d) order or a warrant based on probable cause, but disclosure of the basic subscriber records may also be made pursuant to a subpoena. See 18 U.S.C. §§ 2703(c)(1)(A), (c)(1)(B), & (c)(2).

Although you question the relationship between the two categories, see Memorandum at 4, the structure and history of the SCA make clear that the basic subscriber records set forth in § 2703(c)(2) are a subset of the general category of non-content records of § 2703(c)(1). When the SCA was enacted in 1986, it included only the catch-all category for all non-content records now found in § 2703(c)(1), and the government could compel disclosure of all such information pursuant to a subpoena. See ECPA § 201, Pub. L. No. 99-508, 100 Stat. 1848, 1862 (1986). The Senate report on the SCA explained the breadth of the “record or other information” language:

“[t]he information involved is information about the customer’s use of the service not the content of the customer’s communications.” S. Rep. No. 541, 99th Cong., 2d Sess., at 38 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592 (1986).

To protect the privacy of detailed non-content transactional records, CALEA distinguished between basic subscriber records available pursuant to a subpoena and more detailed transactional logs available only pursuant to a 2703(d) order or a warrant. For example, the House Report on CALEA states that CALEA eliminates the use of subpoenas for detailed e-mail address logs. See H.R. Rep. No. 827(I), 103rd Cong., 2d Sess. at 31 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511 (1994).

Cell-site information falls within the scope of § 2703(c)(1) but not § 2703(c)(2). It is non-content information, but it is detailed transactional information not included in any of the § 2703(c)(2) categories of basic subscriber information. Thus, its disclosure may be compelled pursuant to a 2703(d) order. See 18 U.S.C. § 2703(c)(1)(B). To obtain a 2703(d) order, the government must offer “specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought are relevant and material to an ongoing criminal investigation.” 18 U.S.C. § 2703(d).

D. Prospective collection of cell-site information is authorized by the SCA.

You correctly observed that the SCA lacks certain procedural components included in the Wiretap Act and the pen/trap statute. Memorandum at 10-11. For example, the SCA includes no duration requirement and no sealing requirement. However, respectfully, your argument that the SCA is therefore inherently retrospective fails for two reasons. First, prospective collection of cell-site information is proper under the plain language of the SCA. Second, there is no reason

for the SCA to contain such components, as prospective collection of cell-site information is also subject to the pen/trap statute, which itself supplies the procedural guidelines for prospective collection.

As an initial matter, prospective collection of cell-site information falls within the scope of the SCA. As discussed above, cell-site information is “record[s] or other information pertaining to a subscriber or customer” subject to compelled disclosure under § 2703(c) of the SCA, and its disclosure may therefore properly be compelled pursuant to a 2703(d) order. Moreover, nothing within the SCA prevents disclosure of cell-site information on a prospective basis. Although § 2703(c) and (d) apply only to stored communications, nothing in these sections requires a provider to possess the records at the time the order is executed. Courts should not graft such a limitation onto the SCA where Congress has not done so.

In addition, there is no reason for the SCA to contain such procedural features. Both the SCA and the pen/trap statute govern prospective collection of cell-site information. Thus, when the SCA is used prospectively to gather cell-site information, the pen/trap statute also governs the collection, and all procedural features of pen/trap orders apply to the government’s subsequent collection of information. In practice, prospective applications and orders for cell-site information should satisfy the requirements of both the pen/trap statute and the SCA. This dual-authority requirement essentially creates a regime in which pen/trap orders for cell-site information may be issued, but only when the government also satisfies an “articulable facts” evidentiary showing.

Moreover, prospective use of 2703(d) orders for cell-site information is consistent with Congress’s purpose in restricting use of pen/trap orders for such information. Congress was

concerned with issuing such orders based on the pen/trap statute's relatively low evidentiary standard, under which a pen/trap order is issued based on a certification of relevance from an attorney for the government, see 18 U.S.C. § 3122(b)(2), and the SCA provides a higher standard for issuance of such orders. Under the SCA, a prospective order for cell-site information must meet the "articulable facts" standard of 2703(d) orders. Court orders under 2703(d) 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.

E. The SCA contains no "tracking device exclusion."

You suggest that cell-site information is beyond the scope of § 2703 because of the "tracking device exclusion." Memorandum at 6-10. Your argument has three components: that cell phones are tracking devices, that communications from tracking devices are not electronic communications, and that only electronic communications are subject to the SCA. This argument, respectfully, is incorrect for two separate reasons. First, regardless of whether cell phones are tracking devices, it is clear from the language of the SCA that cell phone providers are providers of electronic communication service subject to process under § 2703. Second, the language, structure, and legislative history of the ECPA make clear that cell phones are not tracking devices. Moreover, the "tracking device exclusion" would seriously erode the privacy protections for users of cell phones, text messaging systems, pagers, and other similar devices.

1. Cell phone service providers are providers of electronic communication service subject to the SCA.

Respectfully, your "tracking device exclusion" argument is premised on a possible misreading of the SCA: you focus on the definition of "electronic communication," but the

critical term in § 2703 is “electronic communication service.” You also argue that a cell phone is a “tracking device” within the meaning of 18 U.S.C. § 3117 because it “permits the tracking of the movement of a person or object.” Memorandum at 8-10. You note that the definition of “electronic communication,” which you characterizes as the “most important definition” in the ECPA, excludes “any communication from a tracking device.” Memorandum at 7; 18 U.S.C. § 2510(12). So, one might assume that if communications from a cell phone are not electronic communications, they are not subject to process under § 2703. This is incorrect. As set forth below, voice communications from a cell phone fall squarely within the definition of “wire communications” rather than “electronic communications,” and cell phone service providers therefore fall within the definition of “electronic communication service.” See 18 U.S.C. § 2510(1), (12), & (15). As providers of electronic communication service, cell phone providers are subject to process under § 2703.

Voice communications using a cell phone are wire communications, not electronic communications. “Wire communication” is defined to mean a communication containing the human voice. See §§ 2510(1), (18) (defining “wire communication” to be “any aural transfer” made in part through the aid of wire, and defining “aural transfer” as “a transfer containing the human voice at any point between and including the point of origin and point of reception”). The legislative history of the ECPA also states explicitly that communications over a cell phone are wire communications. See S. Rep. No. 541, 99th Cong., 2d Sess., at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566; H.R. Rep. No. 647, 99th Cong., 2d Sess., at 31 (1986) (noting that “the Committee intends that ‘wire communication’ be construed to include communications made over cellular systems”). Because cell phone communications are wire communications,

they are not “electronic communications,” as the definition of “electronic communication” specifically exempts wire communications. See 18 U.S.C. § 2510(12)(A).

Critically, the definition of “electronic communication service” encompasses services providing wire communications. In particular, “electronic communication service” is defined to mean “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (emphasis added). Thus, cell phone service providers are providers of electronic communication service.

From this straightforward textual analysis, it follows that cell phone providers are subject to compelled disclosure under the SCA. Section 2703(c)(1) allows the government to compel “a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service” pursuant to a 2703(d) order. 18 U.S.C. § 2703(c)(1)(B) (emphasis added). Because cell phone service providers are providers of electronic communication service, their records are subject to compelled disclosure under § 2703(c)(1). There can be no “tracking device exclusion” for cell phones.

2. Cellular telephones are not “tracking devices.”

A “tracking device” is a homing device used to track a person or object. You argue for a much more expansive interpretation of “tracking device,” under which any device used to communicate over the cellular communications network (and perhaps nearly any other communications devices as well) is a tracking device. By definition, a “tracking device” is “an electronic or mechanical device which permits the tracking of the movement of a person or object.” 18 U.S.C. § 3117(b). You also argue that this definition should be interpreted broadly to include devices that “may not have been intended or designed to track movement,” provided

the device “merely ‘permits’ tracking.” Memorandum at 8. Respectfully, such an expansive interpretation is contrary to the language, structure, and legislative history of the ECPA, and it would significantly undermine privacy protections for users of communication networks.

It is true that cell-site data provides information about the location of a cell phone user. However, cell phones do not permit the detailed continuous tracking of movement permitted by a homing device, and thus do not actually “permit the tracking of the movement of a person or object.” If “tracking device” were given the broad interpretation you suggest, nearly all communications devices would be tracking devices. Certainly any device relying on the cellular communication system (including many pagers, text messaging devices such as Blackberries, and cellular Internet systems) would be a tracking device. But your reasoning extends further. It is generally possible to determine the physical location of a user connected to the Internet, and the whereabouts of fugitives and other suspects are frequently monitored based on their use of the Internet (as was done in the previously-mentioned case of James Kopp). Thus, all computers used to communicate over the Internet could be classified as tracking devices based on your interpretation. Similarly, landline phones would also constitute tracking devices, as it is possible to determine a target’s location from his use of a landline phone.

This broad interpretation of “tracking device” would eviscerate privacy protection under the Wiretap Act and the SCA for most communications now deemed electronic communications. If devices sending text messages or other Internet communications were classified as tracking devices, the messages would not be “electronic communications” under 18 U.S.C. § 2510(12)(C) or “wire communications” under 18 U.S.C. § 2510(1). As a result, such communications would fall outside the scope of the Wiretap Act, and it would arguably no longer be a federal crime to

intercept them. See 18 U.S.C. § 2511(1)(a) (criminalizing interception of wire, oral, and electronic communications). Such communications would also lose protections currently offered by the SCA. For example, the government would arguably never need a warrant based on probable cause to compel disclosure of such communications pursuant to § 2703(a), as that section applies only to electronic communications in electronic storage. These results are plainly contrary to Congress’s purposes in passing the ECPA.

Moreover, the legislative history of the ECPA is quite clear that “tracking devices” are homing devices, not cell phones or other communications technologies. Congress enacted the ECPA because the Wiretap Act “had not kept pace with the development of communications and computer technology.” S. Rep. No. 541, 99th Cong., 2d Sess., at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (1986). Cellular phones were one of the new technologies of particular importance to Congress, see id. at 2 & 9, and cellular technology is central to much of the ECPA’s legislative history. See, e.g., id. at 2, 4, 6- 9, 11-12, 21, & 29-30.

Congress made clear that cellular communications were to be protected as wire communications by the Wiretap Act and the SCA. In particular, Congress amended the definition of “wire communication” to ensure that it encompassed cellular communications by inserting the phrase “including the use of such connection in a switching station” into 18 U.S.C. § 2510(1). See ECPA § 101, Pub. L. No. 99-508, 100 Stat. 1848 (1986). As noted by the Senate Report on the ECPA, “[t]his subparagraph makes clear that cellular communications-- whether they are between two cellular telephones or between a cellular telephone and a ‘land line’ telephone--are included in the definition of ‘wire communications’ and are covered by the statute.” S. Rep. No. 541, 99th Cong., 2d Sess., at 11 (1986), *reprinted in* 1986 U.S.C.C.A.N.

3555, 3565 (1986). In addition, Congress made clear that if technical advances led cellular communications to fall outside the definition of wire communications, they would nevertheless be electronic communications: “In the event that the evolution of cellular technology permits the switching or transmission of mobile-to-mobile service (or mobile-to-landline service) without the use of wire, cable, or other like connection, the Committee intends that cellular communications be included within the term ‘electronic communication.’” H.R. Rep. No. 647, 99th Cong., 2d Sess., at 32 (1986).

The tracking device statute was also enacted as part of the ECPA. See ECPA § 108, Pub. L. No. 99-508, 100 Stat. 1848 (1986). Despite the extensive discussion of cell phones throughout the ECPA’s legislative history, there is no evidence in the legislative history that Congress intended cell phones to be classified as tracking devices. Instead, all discussion of tracking devices suggests that Congress understood tracking devices to be homing devices. For example, the Senate Report on the ECPA includes a glossary of technological terms. The glossary, which defines electronic tracking devices separately from cell phones and pagers, defines “electronic tracking devices” as:

These are one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment, and allows the user to trace the geographical location of the transponder. Such “homing” devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item.

S. Rep. No. 541, 99th Cong., 2d Sess., at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564 (1986). There is no reason to supply “tracking devices” with a meaning much broader than that intended by Congress, especially because doing so would deny many communications the

privacy protection Congress intended them to have.

Finally, the structure of 18 U.S.C. § 3117(b) makes clear that a “tracking device” is a homing device intended to permit tracking of a person or object. The substantive component of the tracking device statute, 18 U.S.C. § 3117(a), applies only when a court is authorized to issue an order “for the installation of a mobile tracking device.” It then provides that “such order may authorize the use of that device within the jurisdiction of the court, and outside that jurisdiction if the device is installed in that jurisdiction.” *Id.* Thus, the purpose of the tracking device statute is to provide a court with extra-territorial jurisdiction over use of tracking devices installed within its jurisdiction. Given the limited purpose of the tracking device statute, there is no basis for interpreting “tracking device” broadly to encompass devices that the government would never have any reason to apply to a court to install or use

- F. The related statutes and legislative history you cite do not support limiting the use of 2703(d) orders for prospective collection of cell-site information.

Your Memorandum discusses several statutes related to the SCA and the pen/trap statute, including CALEA, the Wireless Communication and Public Safety Act of 1999 (“WCPSA”), a bill introduced in the House of Representatives called the Electronic Communications Privacy Act of 2000, and the Patriot Act. Memorandum at 11-18. Nothing in these statutes or their legislative history suggests that 2703(d) orders should not be used in conjunction with the pen/trap statute to authorize prospective collection of cell-site information. To the contrary, the 2000 bill and the Patriot Act support the inference that Congress approves of the use of 2703(d) orders for prospective collection of cell-site information.

The government has discussed CALEA and its legislative history above, and little more

needs to be said about it here. We agree with your assessment that under CALEA, a more exacting legal process than pen/trap orders is necessary for prospective collection of cell-site information, but CALEA did not specify what that process is to be. See Memorandum at 13. In your discussion of CALEA, you reject the propriety of 2703(d) orders for cell-site information by again relying on the purported tracking device exclusion, stating that “[r]eal-time subscriber location data is not accessible under any portion of the ECPA – whether Title I (wiretap), Title II (subscriber information), or Title III (pen registers) – for the very same reason: they all share the same definition of ‘electronic communication,’ which explicitly excludes ‘any communication from a tracking device.’” Memorandum at 13. Respectfully, however, this argument is based on a misreading of the SCA.

Similarly, reliance on the WCPSA is misplaced. You assert that the WCPSA demonstrates that “location information is a special class of customer information, which can only be used or disclosed by a carrier in an emergency situation, absent express prior consent by the customer.” Memorandum at 14. This assertion is incorrect. In fact, the WCPSA states that “Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose, or permit access to individually identifiable customer proprietary network information” in certain specified situations. 47 U.S.C. 222(c)(1) (emphasis added). The phrase “except as required by law” encompasses appropriate criminal legal process. See Parastino v. Conestoga Tel & Tel. Co., No. Civ. A 99-679, 1999 WL 636664, at *1-*2 (E.D.Pa, Aug. 18, 1999) (holding that a valid subpoena falls within the “except as required by law” exception of § 222(c)(1)). Such criminal process includes process under the

SCA. You quote § 222(f) of the WCPSA, see Memorandum at 14, but this provision does not limit the “as required by law” exception. Instead, § 222(f) sets rules for determining whether a customer has consented to voluntary disclosure of his call location information. Thus, the WCSPA does not limit the disclosure of cell-site information pursuant to the SCA.

In addition, respectfully, you are incorrect in asserting that “[b]ased on [WCPSA], a cell phone user arguably maintains a reasonable expectation of privacy in his call location information.” Memorandum at 14. To use a cell phone, a user must communicate his presence to the cellular phone company by sending a transmission from his cell phone to a nearby cell site. This transmission enables the cell phone service provider to know where the customer is, so that it is able to route calls to and from the customer. There can be no reasonable expectation of privacy in such information under the principles of Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (finding no reasonable expectation of privacy in phone numbers dialed by owner of a telephone because act of dialing the number effectively tells the number to the phone company) and United States v. Miller, 425 U.S. 435, 440-43 (1976) (holding that bank records are disclosed information and thus not subject to Fourth Amendment protection).⁴ The fact that Congress has provided additional statutory protections for cell-site information does not create a constitutional reasonable expectation of privacy in that information. For example, the pen/trap statute and the SCA create statutory privacy rights in dialed phone numbers, but dialed phone numbers remain constitutionally unprotected under Smith v. Maryland.

⁴ In dicta in United States v. Forest, 355 F.3d 942, 951-52 (6th Cir. 2004), the Sixth Circuit stated that Smith v. Maryland did not apply to cell-site information where the government had dialed the target’s cell phone. The Sixth Circuit failed to understand that cell phones users necessarily communicate their presence to the cell phone service provider and thus have voluntarily disclosed cell-site information to the provider.

Similarly, in your conclusion, you fault cell-site orders under the SCA for “authorizing a mobile tracking device under a lesser threshold (‘specific and articulable facts’) than the probable cause standard of Rule 41.” Memorandum at 17-18. However, a probable cause standard is required for a mobile tracking device only when the government invades a reasonable expectation of privacy. Compare United States v. Knotts, 460 U.S. 276, 285 (1983) (upholding warrantless use of beeper to track vehicle on public roads) with United States v. Karo, 468 U.S. 705, 713-18 (1984) (holding that warrantless use of beeper inside a house violated the Fourth Amendment). Because there is no reasonable expectation of privacy in cell-site information, government collection of cell-site information does not implicate the Fourth Amendment.

Finally, you disparage government reliance on the Electronic Communications Privacy Act of 2000, a bill that would have amended § 2703 to require a warrant based on probable cause for compelled disclosure of cell-site information. Memorandum at 15-17. Although certainly not the strongest form of legislative history, the House report you quote shows that Congress was aware that courts were issuing 2703(d) orders for collection of cell-site information, see Memorandum at 15, and the failure of that bill provides some evidence that Congress did not object to 2703(d) orders for cell-site information. In any case, an additional argument that Congress approves this use of 2703(d) orders can be inferred from the passage of the Patriot Act in 2001. With the Patriot Act, Congress substantially rewrote much of the pen/trap statute and § 2703(c) of the SCA, but it did nothing to restrict use of 2703(d) orders for cell-site information. See Patriot Act §§ 210, 216. Given that Congress acknowledged courts’ issuance of such 2703(d) orders on the record, its refusal to restrict the practice suggests congressional approval. Cf Lorillard v. Pons, 434 U.S. 575, 580-81 (1978) (“Congress is presumed to be aware of an

administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change. . . . So too, where, as here, Congress adopts a new law incorporating sections of a prior law, Congress normally can be presumed to have had knowledge of the interpretation given to the incorporated law, at least insofar as it affects the new statute.”).

G. Summary:

Thank you for giving us an opportunity to respond to your memorandum. Many people worked quite hard on this response, but I take the blame for errors, if any. I hope you will let me know if you have any questions.