

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF TEXAS  
HOUSTON DIVISION

In the Matter of the Application	)	
of the United States of America	)	Magistrate No. H-10-998M
for an Order Authorizing the Use	)	Magistrate No. H-10-990M
Of a Pen Register and Trap and	)	Magistrate No. H-10-981M
Trace Device and Authorizing	)	
Release of Subscriber and Other	)	
Information	)	

Government’s Memorandum Of Law In Support Of  
Request For Historical Cell-site Records

On October 14, 2010, this Court issued an Order noting that it had recently denied several applications by the United States “for orders under 18 U.S.C. § 2703(d) compelling various service providers to disclose records pertaining to a customer’s cell phone use, including historical cell site information.” This Court stated that it “denied those requests in light of recent court decisions and technological developments,” and it “invited the Government, if it disagreed with those rulings, to submit a brief to justify its position with appropriate legal and factual support.”

This brief sets forth the reasons why an order issued pursuant to 18 U.S.C. § 2703(d) (a “2703(d) order”) may be used to compel disclosure of historical cell-site records.<sup>1</sup> It begins with

---

<sup>1</sup>In its October 14 Order, this Court identified only one recent opinion, which addresses the standard for obtaining historical cell-site records: *In re Application of United States*, \_\_\_ F. Supp. 2d \_\_\_, 2010 WL 3463132 (E.D.N.Y. Aug. 27, 2010). In addition, the Third Circuit recently addressed the standard for obtaining historical cell-site records in *In re Application of United States*, \_\_\_ F.3d \_\_\_, 2010 WL 3465170, at \*7 (3d Cir. Sept. 7, 2010). Thus, the United States understands the Court’s October 14 Order as requesting the United States to brief the appropriate standard for obtaining historical cell-site records. If the Court has other questions regarding the United States’s applications, the United States is prepared to address them in

a factual overview of historical cell-site records. It then addresses the statutory language of § 2703 of the Stored Communications Act (“SCA”), 18 U.S.C. § 2703, which authorizes the government to obtain an order compelling disclosure of historical cell-site records using a 2703(d) order. Next, it explains why the Fourth Amendment does not bar the government from using a 2703(d) order to compel disclosure of historical cell-site records. Finally, it addresses this Court’s question regarding judicial notice.

### **I. Factual Overview of Historical Cell-Site Records**

Cellular telephone networks provide service to their customers through tower antennas deployed across the provider’s coverage area. When the user places or receives a call, a signal is transmitted between the telephone and a nearby tower antenna, which relays the call to a local switch for routing. A telephone may move in the course of a single call through the coverage areas of multiple towers, especially where the user is in a moving vehicle. Therefore, the system’s awareness of a wireless telephone’s general whereabouts is essential to providing cellular service.

Spacing between antenna towers varies depending on a number of factors, especially terrain and population density. In heavily populated urban areas, towers may be spaced every few hundred feet; in rural areas, by contrast, towers may be separated by 10 miles or more. *See In re Applications of United States*, 509 F. Supp. 2d 76, 78 n.3 (D. Mass. 2007). A typical tower will have three separate antenna faces (or sectors), each serving a 120-degree portion of the roughly circular coverage area extending out from the antenna mast. *In re Application of United States*, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005). However, a tower may simply have a single

---

additional briefing.

360-degree face.

Cellular telephone companies keep, in the regular course of their business, records of certain information associated with the calls they process. *See In re Applications of United States*, 509 F. Supp. 2d at 78. Whenever a cellular telephone user initiates or receives a communication, the carrier routinely creates a record, including the date, time, cell tower, and sector handling the communication at the start and end of the communication. *See United States v. Garcia-Alvarez*, 2007 WL 996162 at \*1 (D.P.R. 2007) (“The location of the cell site for each call appears as a billing code in each customer’s cell phone records.”).

A redacted sample of historical cell-site information produced by T-Mobile is attached as Exhibit A.<sup>2</sup> It is a sample of the call records produced in response to an order issued October 6, 2010, and it includes calls from September, 2010. T-Mobile produced the following information for each call: (1) date and time of call initiation, answer, and termination (columns J, H, and I); (2) the telephone numbers involved in the call, as well as other identifying numbers (IMEI and IMSI) associated with the target phone (columns B, C, D, E, and F); (3) whether the call originated or terminated with the target phone (column A); (4) the cell tower to which the customer connected at the beginning of the call (columns K and M); (5) the cell tower to which the customer was connected at the end of the call (columns L and N); and (6) the duration of the call (columns G and O).

Cell-site records should not be confused with the more precise mechanisms of Global

---

<sup>2</sup>“Call type” in Exhibit A refers to whether the call originates (“MOC”) or terminates (“MTC”) with the target cell phone. The “translated number” is the same as the called number, though it sometimes has “1” inserted at the beginning of the number. A “LAC” is a “location area code;” a collection of cell towers will share the same LAC.

Positioning System (“GPS”) technology. In applications submitted to this Court, the United States has specified that “‘Cell site information’ as used in this order refers to the antenna tower and sector to which the cell phone sends its signal.”

## **II. A 2703(d) Order May Be Used to Compel Disclosure of Historical Cell-Site Records.**

Although this brief primarily addresses the constitutionality of compelled disclosure of historical cell-site records, it is important to note at the outset that § 2703 of the SCA authorizes compelled disclosure of historical cell-site records pursuant to a 2703(d) order. Congressional authorization is significant because there is a “strong presumption of constitutionality” to federal statutes challenged on Fourth Amendment grounds. *United States v. Watson*, 423 U.S. 411, 416 (1976).

As a statutory matter, a 2703(d) order may be used to compel disclosure of historical cell-site records because cell-site records fall within the scope of 18 U.S.C. § 2703(c)(1). In particular, 18 U.S.C. § 2703(c)(1) requires “a provider of electronic communication service . . . to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)” pursuant to a 2703(d) order. Cell-site records fall within the scope of this provision. First, a cellular telephone company is a provider of electronic communication service because it provides its users with “the ability to send or receive wire or electronic communications,” 18 U.S.C. § 2510(15), as cell phone calls are wire communications. Second, a cell-site record is “a record or other information pertaining to a subscriber or customer of such service (not including the contents of communications).” Therefore, disclosure of cell-site records may be obtained pursuant to 18 U.S.C. §§ 2703(c)(1) and (d). *See In re Application of United States*, \_\_\_ F.3d \_\_\_, 2010 WL 3465170, at \*7 (3d Cir.

Sept. 7, 2010) (holding that cell-site records are “obtainable under a § 2703(d) order”) (hereinafter, “*Third Circuit Opinion*”); *In re Applications of United States*, 509 F. Supp. 2d 76, 79-80 (D. Mass. 2007) (concluding that historical cell-site records fall within the scope of § 2703(c)(1)). This Court previously noted that “historical cell site data more comfortably fits the category of transactional records covered by the SCA.” *In re Application*, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005).

Because historical cell-site records fall within the scope of § 2703(c)(1), the SCA authorizes the United States to obtain a 2703(d) order to compel their disclosure. *See* 18 U.S.C. § 2703(c)(1)(B). Section 2703(d) specifies that a 2703(d) order “may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers 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.” Thus, when the United States satisfies the “specific and articulable facts” standard of § 2703(d), it is entitled to obtain an order to compel disclosure of historical cell-site records.

The Third Circuit recently held that historical cell-site records are available using a 2703(d) order and that “such an order does not require the traditional probable cause determination.” *Third Circuit Opinion*, 2010 WL 3465170 at \* 7. However, the court also held that the statute “as presently written gives the MJ the option to require a warrant showing probable cause,” though it noted that such a requirement was “an option to be used sparingly.” *Id.* at \*13. Essentially, the court found that the “only if” language of § 2703(d) means that the “specific and articulable facts” requirement is a necessary condition for obtaining a 2703(d) order, but not a sufficient one. *See id.* at \*9.

The Third Circuit's interpretation of § 2703(d) should be rejected because it renders the phrase "and shall issue" in § 2703(d) superfluous. The court's "necessary but not sufficient" interpretation of § 2703(d) is equivalent to the following formulation, which omits the critical "and shall issue" language of § 2703(d): a 2703(d) order "may be issued by any court that is a court of competent jurisdiction only if the governmental entity offers specific and articulable facts . . . ." The Third Circuit's interpretation therefore violates the "cardinal principle of statutory construction that a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." *Kaltenbach v. Richards*, 464 F.3d 524, 528 (5th Cir. 2006) (quoting *TRW Inc. v. Andrews*, 534 U.S. 19, 21 (2001) (internal quotation marks omitted)). Furthermore, the word "shall" has critical importance in a statute: as the Supreme Court has stated, "[t]he word 'shall' is ordinarily 'the language of command.'" *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001). Because the Third Circuit's interpretation of § 2703(d) improperly renders "shall" superfluous, it should be rejected.

Moreover, as Judge Tashima stated in his concurrence in the *Third Circuit Opinion*, the Third Circuit's construction of § 2703(d) "provides *no* standards for the approval or disapproval of an application" for a 2703(d) order. *Third Circuit Opinion*, 2010 WL 3465170 at \*14 (Tashima, J., concurring). The Third Circuit's reasoning could permit a magistrate judge to arbitrarily deny an application under 2703(d) without any reasoned basis. As Judge Tashima stated, this interpretation "is contrary to the spirit of the statute." *Id.*

The United States believes that § 2703(d) requires a court to issue a 2703(d) order for information that falls within the scope of the statute when its application satisfies the "specific and articulable facts" standard of § 2703(d). The function of the word "only" in 2703(d) is to

preclude the issuance of a 2703(d) order at the discretion of the issuing court if the government fails to offer specific and articulable facts. Without the word “only,” § 2703(d) would specify that a 2703(d) order “may be issued by any court that is a court of competent jurisdiction and shall issue if” the government offered specific and articulable facts. Thus, omission of the word “only” would leave a court with discretion to issue a 2703(d) order in the absence of specific and articulable facts. Inclusion of “only” in § 2703(d) eliminates this discretion, but it does not eliminate a court’s obligation to issue a 2703(d) order when the government satisfies the “specific and articulable facts” standard.

### **III. The Fourth Amendment Does Not Bar Compelled Disclosure of Historical Cell-Site Records Pursuant to a 2703(d) Order.**

Historical cell-site records are business records generated and stored by cell phone companies when their customers make or receive telephone calls. When they are relevant and material to a criminal investigation, the government thus has a right to compel their disclosure: “For more than three centuries it has now been recognized as a fundamental maxim that the public . . . has a right to every man’s evidence.” 8 J. Wigmore, *Evidence* § 2192 (McNaughton rev. 1961)); *see also United States v. Nixon*, 418 U.S. 683, 709 (1974) (citing cases). The Fourth Amendment does not reverse this rule, and it does not require the United States to demonstrate probable cause when using compulsory process. *See Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946). As explained in section III.A below, an individual’s Fourth Amendment interests are not implicated when the government compels the disclosure of business records, such as historical cell-site records, that are not the individual’s private papers. In addition, as explained in section III.B. below, historical cell-site records would not be protected

by the Fourth Amendment even if they were judged under the standards applicable to tracking devices surreptitiously installed by the government.

- A. The Fourth Amendment does not bar compelled disclosure of business records, including historical cell-site records.

A customer has no privacy interest in business records held by a cell phone provider that are not the customer's private papers. Addressing a Fourth Amendment challenge to a third party subpoena for bank records, the Supreme Court held in *United States v. Miller*, 425 U.S. 435 (1976), that the bank's records "are not respondent's 'private papers'" but are "the business records of the banks" in which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440. The records "pertain to transactions to which the bank was itself a party." *Id.* at 441. As the United States Court of Appeals for the District of Columbia stated, "it has been consistently held by the Supreme Court and the Courts of Appeals that a person has no Fourth Amendment basis for challenging subpoenas directed at the business records of a third party." *Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d 1030, 1044 (D.C. Cir. 1978) (citing cases).

Historical cell-site records are business records kept by the cell phone company of the cell towers it used to process a particular call. *See, e.g., United States v. Garcia-Alvarez*, 2007 WL 996162 at \*1 (D.P.R. 2007) ("The location of the cell site for each call appears as a billing code in each customer's cell phone records."); *In re Application*, 396 F. Supp. 2d 747, 759 n.16 (S.D. Tex. 2005) ("Cell phone companies might legitimately compile such data for customized marketing and billing purposes."). Like the bank records in *Miller*, a customer has neither ownership, possession, or control over historical cell-site records stored by a provider. The

choice to create and store historical cell-site records is made by the provider, not the customer, and the provider controls the format, content, and duration of the records it chooses to create and retain. Indeed, because cell-site records are not in the possession of a customer, a customer could not be expected to produce cell-site records in response to a subpoena for his own cell-site records. Moreover, although a customer is likely to be aware that the cell phone company will assign a cell tower to handle his call, the customer typically does not know which cell tower is assigned to process his calls. Thus, cell-site records cannot be a customer's "private papers." Similarly, the assignment of a cell tower to process a call is certainly a transaction to which the cell phone company is a party: the assignment is made by the cell phone company to facilitate the functioning of its network. Therefore, historical cell-site records are not protected by the Fourth Amendment because they are the phone company's business record rather than a customer's private papers. *See also SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) ("when a person communicates information to a third party even on the understanding that the communication is confidential, he cannot object if the third party conveys that information or records thereof to law enforcement authorities").

The Court's reasoning in *Smith v. Maryland*, 442 U.S. 735 (1979), leads to the same result. In *Smith*, the Court held both that telephone users had no subjective expectation of privacy in dialed telephone numbers and also that any such expectation is not one that society is prepared to recognize as reasonable. *See Smith*, 442 U.S. at 742-44. The Court's reasoning applies equally to cell-site records. First, the Court stated: "we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone

company switching equipment that their calls are completed.” *Id.* at 742. Similarly, cell phone users understand that they must send a radio signal which is received by a cell phone company's antenna if the company is going to route their call to its intended recipient. Indeed, cell phone users routinely experience the frustration associated with dropped calls and recognize they are caused when their phone's radio signal is having difficulty reaching a tower clearly. Cell phones also often display a cell tower icon, along with bars representing the strength of the signal between the phone and tower. Cell phone users also understand that the provider will know the location of its own cell tower, and that the provider will thus have some knowledge of the user's location. Indeed, providers' terms of service and privacy policies make clear that the provider's obtain this information.<sup>3</sup>

---

<sup>3</sup>For example, T-Mobile's privacy policy includes the following provisions:

Our network detects your device's approximate location whenever it is turned on (subject to coverage limitations). This location technology makes the routing of wireless communications possible and is also the basis for providing enhanced emergency 9-1-1 service, which permits us to provide your general location to a public safety answering point, emergency medical service provider, or emergency dispatch provider.

We automatically collect certain information, some of which may be associated with personal information, whenever you use our services or Web sites. For example, our systems capture details about the type and location of wireless device(s) you use, calls and text messages you send and receive, and other data services you use (for example your ringtone purchases).

We use personal information for a variety of business purposes, including for example, to complete transactions and bill for products and services; verify your identity; respond to your requests for service or assistance; anticipate and resolve actual and potential problems with our products and services; create and improve products and services; suggest additional or different products or services; make internal business decisions about current and future offers; provide personalized service and user experiences; and protect our rights and property.

Second, under the reasoning of *Smith*, any subjective expectation of privacy in cell-site records is unreasonable. In *Smith*, the Court explicitly held that “even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not one that society is prepared to recognize as reasonable.” *Id.* at 743 (internal quotation omitted). It noted that “[t]his Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” *Id.* at 743-44. In *Smith*, the user “voluntarily conveyed numerical information to the telephone company” and thereby “assumed the risk that the company would reveal to police the numbers he dialed.” *Id.* at 744. Here, a cell phone user voluntarily transmits a signal to a cell tower for his call to be connected, and the provider thereby observes information regarding which of its cell towers it used to complete the call. The user assumes the risk that the cell phone provider will reveal the cell-site records to law enforcement. Thus, it makes no difference if some users have never thought about how their cell phones work; a cell phone user can have no reasonable expectation of privacy in cell-site records.

In addition, it is important to understand that *Miller* and *Smith v. Maryland* are consistent with a more general constitutional rule that probable cause is not required to compel disclosure of information needed by the government for a criminal investigation. By its terms, the Fourth Amendment protects people against unreasonable searches and seizures, but it imposes a

---

[www.t-mobile.com/company/website/privacypolicy.aspx](http://www.t-mobile.com/company/website/privacypolicy.aspx) (visited October 25, 2010). The first of these paragraphs demonstrates that a cell phone customer will be aware that T-Mobile obtains information regarding the customer’s location. The second paragraph demonstrates that a customer will be aware that T-Mobile collects this information. The third paragraph demonstrates that the customer will be aware that this information becomes a T-Mobile business record.

probable cause requirement only on the issuance of warrants. *See* U.S. Const. Amend IV (“and no Warrants shall issue, but upon probable cause”). For example, in *Oklahoma Press Publishing Co. v. Walling*, 327 U.S. 186, 208 (1946), the Court held that “the Fourth [Amendment], if applicable [to compulsory process], at the most guards against abuse only by way of too much indefiniteness or breadth in the things required to be ‘particularly described,’ if also the inquiry is one the demanding agency is authorized by law to make and the materials specified are relevant. The gist of the protection is in the requirement, expressed in terms, that the disclosure sought shall not be unreasonable.” *See also United States v. Dionisio*, 410 U.S. 1, 11-12 (1973).<sup>4</sup> The Supreme Court has confirmed that the government “has a right to every man's evidence, except for those persons protected by a constitutional, common-law, or statutory privilege.” *Branzburg v. Hayes*, 408 U.S. 665, 688 (1972) (internal quotation marks omitted). Simply put, there is no constitutional, common law, or statutory privilege that prevents compelled disclosure of business records.<sup>5</sup> As the Supreme Court recognized, “exceptions to the demand for every man’s evidence

---

<sup>4</sup>The issue before the Supreme Court in *Miller* was not whether a warrant was required to obtain the defendant’s bank records. Instead, the issue was whether the defendant had a sufficient Fourth Amendment interest to challenge the use of bank records obtained pursuant to a defective subpoena. *See Miller*, 425 U.S. at 438-39. The Court held that he did not. *See Miller*, 425 U.S. at 446. Thus, even if historical cell-site were distinguishable from the business records at issue in *Miller*, nothing in *Miller* suggests that historical cell-site records could not be obtained pursuant to a lawfully authorized 2703(d) order.

<sup>5</sup>To be clear, the government's authority to compel an entity to disclose an item or information via subpoena or 2703(d) order is limited to items or information over which the entity has joint access or control for most purposes. This rule is consistent with the common authority doctrine of *United States v. Matlock*, 415 U.S. 164, 172 n.7 (1974), and also with the rule that “the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities.” *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976) (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). For example, under this rule, the government could not subpoena a landlord to produce documents from a tenant’s apartment to which the landlord had

are not lightly created nor expansively construed, for they are in derogation of the search for truth.” *United States v. Nixon*, 418 U.S. 683, 710 (1974).

Business records do not become privileged merely because they contain location information. Indeed, traditional landline telephone records contain location information far more exact than that of cell phones: they place callers in a particular place (often a home) at a particular time. But it is clear from *Smith v. Maryland* that there is no reasonable expectation of privacy in such information even in the pen register context, where the provider is acting as an agent of the government to collect information in real time. In contrast, with historical cell-site records, the provider has chosen to create and store cell-site records for its own business purposes, not at the direction of the government. With historical call detail records, courts uniformly held that there was no reasonable expectation of privacy in such information. *See Reporters Committee for Freedom of Press v. AT&T*, 593 F.2d at 1046 n.49 (citing cases).

Two recent court decisions have rejected the application of *Miller* and *Smith v. Maryland* to historical cell-site records. *See In re Application of United States*, \_\_\_ F. Supp. 2d \_\_\_, 2010 WL 3463132 (E.D.N.Y. Aug. 27, 2010) (hereinafter, “*Orenstein Opinion*”); *Third Circuit Opinion*, 2010 WL 3465170 at \*11.<sup>6</sup> The *Orenstein Opinion* relies on three arguments in support of its holding. First, it argues that under the reasoning of *United States v. Warshak*, 490 F.3d

---

only a limited right of access. But a cell-phone provider’s authority to access its own historical cell-site records is not limited: no law distinguishes its authority to access its users’ cell-site records from other call detail records stored by the provider.

<sup>6</sup>Other recent cases have rejected Fourth Amendment challenges to acquisition of historical cell-site records without a warrant. *See, e.g., United States v. Benford*, 2010 WL 1266507, at \*3 (N.D. Ind. Mar. 26, 2010) (denying suppression of historical cell-site data); *United States v. Suarez-Blanca*, 2008 WL 4200156, at \*8-\*11 (N.D. Ga. Mar. 26, 2008) (same); *Mitchell v. State*, 25 So.3d 632, 635 (Fla. Dist. Ct. App. 2009) (same).

455 (6th Cir. 2007), “a person may reasonably maintain an expectation of privacy in information about herself that she knows to be held by others.” *Orenstein Opinion*, 2010 WL 3463132 at \*7. Second, it argues that a cell phone user has not “voluntarily conveyed” cell-site records to the provider. *Id.* at \*8 (quoting *In re Application*, 396 F. Supp. 2d at 756). Third, it argues that “a recognizable privacy interest in caller location information is provided by the Wireless Communication and Public Safety Act of 1999.” *Id.* at \*8 (quoting *In re Application*, 396 F. Supp. 2d at 757). The *Third Circuit Opinion* relies only on the second of these arguments. *See Third Circuit Opinion*, 2010 WL 3465170 at \*11. As explained below, each of these arguments is mistaken. In addition, it is significant that the *Orenstein Opinion* concedes that the recent tracking device case *United States v. Maynard*, 615 F.3d 544, (D.C. Cir. 2010) does not undermine the reasoning of *Miller* and *Smith v. Maryland*. *See Orenstein Opinion*, 2010 WL 3463132 at \*7 (stating that “*Maynard* provides no answer” to the reasoning of *Miller*).

First, the *Orenstein Opinion* relies on *United States v. Warshak*, 490 F.3d 455 (6th Cir. 1990), which is no longer even good law: it was vacated in the en banc decision *United States v. Warshak*, 532 F.3d 521 (6th Cir. 2008) (en banc). But even the vacated *Warshak* decision held only that the government could not compel disclosure of the content of stored email without a warrant or prior notice to the subscriber. Critically, the court based its decision on a determination that an email provider had access to the content of email “only in limited circumstances, rather than wholesale inspection, auditing, or monitoring of e-mails.” *Warshak*, 490 F.3d at 474. The reasoning of the vacated *Warshak* panel opinion could apply to historical cell-site records only if providers had authority to access their historical cell-site records “only in limited circumstances.” But there is no such restriction on a cell phone provider’s access to its

own records. The provider is entitled to access its cell-site records to the same extent it is entitled to access its other historical call detail records, which courts have agreed are unprotected by the Fourth Amendment.

In addition, if the reasoning of the vacated *Warshak* panel opinion could be applied to historical cell-site records, there is no clear reason why it could not also be applied to dialed telephone numbers or any other business records. This reasoning would then reverse the Supreme Court's decisions in *Smith v. Maryland* and *United States v. Miller*, which only the Supreme Court may do.

Second, the *Orenstein Opinion* and the *Third Circuit Opinion* assert that *Miller* and *Smith v. Maryland* do not apply to historical cell-site records because such records are not "voluntarily" conveyed to the cell phone company. As discussed at pages 10-11 above, information regarding a user's location is voluntarily conveyed by the user under the Supreme Court's analysis in *Smith v. Maryland*. Use of a cell phone is entirely voluntary, and a user will know from his experience with his cell phone and from a provider's privacy policy/terms of service that he will communicate with a provider's cell tower and that this communication will convey information to the provider about his location. *Cf. United States v. Gallo*, 123 F.2d 229, 231 (2d Cir. 1941) (L. Hand, Swan, A. Hand, JJ.) ("When a person takes up a telephone he knows that the company will make, or may make, some kind of a record of the event, and he must be deemed to consent to whatever record the business convenience of the company requires."). In addition, voluntariness is not essential to *Miller*'s reasoning. Although *Miller* does note that the bank statements "contain only information voluntarily conveyed to the banks," this statement comes three paragraphs after the core paragraph of the decision, in which the Court reasons that "the

documents subpoenaed here are not respondent's 'private papers'" but are instead "the business records of the banks," over which a customer "can assert neither ownership nor possession." *Miller*, 425 U.S. at 440. See *Wilson v. First Gibraltar Bank*, 1994 WL 199108, at \*3 (5th Cir. May 12, 1994) (noting that the bank records of *Miller* were not protected by the Fourth Amendment because they were the "bank's business records rather than depositor's private papers"). Thus, because historical cell-site records are business records of the provider, the government may use a 2703(d) order to compel their disclosure.

Third, the *Orenstein Opinion* states that "a recognizable privacy interest in caller location information is provided by the Wireless Communication and Public Safety Act of 1999" ("WCPSA"). *Orenstein Opinion*, 2010 WL 3463132 at \*8 (quoting *In re Application*, 396 F. Supp. 2d at 757). However, any argument that the WCPSA creates a Fourth Amendment privacy interest has now been foreclosed by the Supreme Court's recent rejection of the proposition that statutes can create a constitutional reasonable expectation of privacy. In *City of Ontario v. Quon*, 130 S. Ct. 2619 (2010), Quon argued that a violation of § 2702 of the SCA rendered a search of his text messages unreasonable under the Fourth Amendment. The Supreme Court rejected the notion that the SCA created Fourth Amendment rights: "Respondents point to no authority for the proposition that the existence of statutory protection renders a search per se unreasonable under the Fourth Amendment. And the precedents counsel otherwise." *Id.* at 2632 (citing *Virginia v. Moore*, 553 U.S. 164, 168 (2008) and *California v. Greenwood*, 486 U.S. 35, 43 (1988)).

In any case, the WCPSA by its terms allows compelled disclosure pursuant to the SCA. In particular, it provides 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.*, 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)). Because the WCPSA allows compelled disclosure pursuant to 2703(d) order, it does not render 2703(d) orders unconstitutional.

- B. Even under the standards applicable to surreptitiously installed tracking devices, the Fourth Amendment does not bar compelled disclosure of historical cell-site records.

As a business record in the possession of a third party, cell-site records should not be judged under Fourth Amendment standards applicable to tracking devices surreptitiously installed by the government. For example, a pen register or historical call detail records may provide law enforcement with information regarding the activity inside a private home at a particular time, which would violate the Fourth Amendment if judged under the standards of *United States v. Karo*, 468 U.S. 705 (1984). But as discussed in section III.A, a customer has no Fourth Amendment interest in this information.

Nevertheless, even measured against the constitutional standards articulated by the Supreme Court regarding surreptitiously installed tracking devices, there is no reasonable expectation of privacy in historical cell-site records. The mere use of a tracking device, even when surreptitiously placed by the government, does not implicate Fourth Amendment privacy

concerns. *See United States v. Knotts*, 460 U.S. 276, 282 (1983) (police monitoring of beeper signals along public roads did not invade any legitimate expectation of privacy). To be of constitutional concern, a surreptitiously installed tracking device must reveal facts about the interior of a constitutionally protected space. *See United States v. Karo*, 468 U.S. at 715 (distinguishing *Knotts* and holding that police monitoring of a beeper that disclosed information about the interior of a private residence, not open to visual surveillance, required a warrant).

At issue in *Karo* was not whether persons or objects in private spaces enjoy generalized and undifferentiated Fourth Amendment protection. Rather, as the Court explains at the outset, the exact question is “whether monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals information that could not have been obtained through visual surveillance.” *Id.* at 707. In that case, agents had installed a radio transmitter in a can of ether expected to be used in processing cocaine. Without first obtaining a warrant, the agents monitored the signal from the beeper as it moved through a series of residences and multi-unit storage facilities. *See id.* at 708-09. Where the tracking system enabled the government to locate the can of ether in particular residences, the Supreme Court found that the Fourth Amendment had been infringed. *See id.* at 715. (“The beeper tells the agent that a particular article is actually located at a particular time in the private residence . . . . [L]ater monitoring . . . establishes that the article remains on the premises.”)

Conversely, the Court found no Fourth Amendment violation where the beeper disclosed only the general location of the ether. In particular, “the beeper equipment was not sensitive enough to allow agents to learn precisely which locker [in the first storage facility] the ether was in.” *Id.* at 708. Instead, the agents learned the can’s precise location inside a specific locker only

after subpoenaing the storage company for rental records; tracking the beeper to a specific row of lockers; and then using their sense of smell to detect the ether. *See id.* When one of the targets moved the ether, a similar scenario played out again: agents traced the beeper to another self-storage facility, and then – using their noses – located the smell of ether coming from a given locker. *See id.* at 709.

As to these two episodes, the Supreme Court held emphatically that no Fourth Amendment violation occurred:

[T]he beeper informed the agents only that the ether was somewhere in the warehouse; it did not identify the specific locker in which the ether was located. Monitoring the beeper revealed nothing about the contents of the locker that Horton and Harley had rented and hence was not a search of that locker.

*Id.* at 720. In sum, the test under *Karo* is not simply whether a tracked object is inside a private, constitutionally protected pocket, purse, or home. (The can of ether was at the relevant times unquestionably in each of the two lockers, both of which enjoyed a reasonable expectation of privacy. *See id.* at 720 n.6.) Rather, *Karo* holds that government use of a tracking device violates the Fourth Amendment only where the monitoring actually reveals the particular private location in which the tracked object may be found.

Based on this standard from *Karo*, cell-site records are not precise enough to implicate the Fourth Amendment. Cell-site records can only reveal a telephone's general location to within several hundred feet, at best. As a result, such information cannot reveal whether a telephone is within a constitutionally protected private space (such as a residence) and therefore does not implicate any Fourth Amendment-protected privacy interests. *See United States v. Ortega-Estrada*, 2008 WL 4716949, at \*13 (N.D. Ga. Oct. 22, 2008) (finding that even GPS information

accurate to within 32 meters “revealed only a general area where the suspect was at a particular time, and thus, did not invade a place where he might have an expectation of privacy”).

In holding that a warrant is required to compel disclosure of historical cell-site information, the *Orenstein Opinion* relies heavily on *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), a recent case holding that agents violated the Fourth Amendment after they covertly installed a GPS device on a car when they tracked the car’s movements for 28 days. *Maynard* promulgated a new “intimate picture” or “mosaic” theory of the Fourth Amendment, under which “[t]he whole of one’s movements over the course of a month is not constructively exposed to the public,” even though one’s individual movements are exposed to the public. *Id.* at 561-62. *Maynard*’s holding is inconsistent with the basic rule that “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.” *Katz v. United States*, 389 U.S. 347, 351 (1967). *Maynard* asserts that the exposure rule from *Katz* is based not on what is actually exposed to the public, what instead on what “a reasonable person expects another might actually do.” *Maynard*, 615 F.3d at 559. But this assertion is inconsistent not only with the language of *Katz*, but also with the Court’s holding in *Smith v. Maryland*: a reasonable person would not expect the phone company to closely monitor the network of people he calls in an attempt to draw inferences about the scope of his conduct and connections.

Furthermore, *Maynard* is vague and unworkable: it allows law enforcement to conduct some tracking without a warrant, but it provides no standards for when that tracking must cease. *Maynard* is also inconsistent with Fourth Amendment doctrine because under the “mosaic” rule of *Maynard*, future law enforcement conduct can cause past law enforcement conduct to become unconstitutional: tracking without a warrant may comply with the Fourth Amendment at the time

it is done, but if the tracking continues, all of the tracking apparently violates the Fourth Amendment. This “retroactive unconstitutionality” is not a feature of any other Fourth Amendment doctrine. The *Maynard* decision conflicts with the opinions of three other courts of appeals on the use of tracking devices, and it should be rejected. See *United States v. Marquez*, 605 F.3d 604, 609-10 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212, 1216-17 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994, 997-98 (7th Cir. 2007).

Any reliance on *Maynard* is mistaken, but the *Orenstein Opinion* extends the mosaic theory of *Maynard* far beyond even *Maynard*’s reasoning. First, *Maynard*’s mosaic rationale is inconsistent with business records cases from the bank records and telephone cases of *Miller* and *Smith v. Maryland* to more recent cases applying these principles to the Internet, such as *United States v. Forrester*, 512 F.3d 500, 510-11 (9th Cir. 2008) (holding that pen register/trap and trace device for email and IP addresses did not violate Fourth Amendment). Such business records often supply an “intimate picture” of a user’s life, but as discussed in section III.A, they are unprotected by the Fourth Amendment. Indeed, the *Orenstein Opinion* concedes that “*Maynard* provides no answer” to the reasoning of *Miller*. See *Orenstein Opinion*, 2010 WL 3463132 at \*7.

Second, *Maynard* involves a tracking device covertly installed by the government, but historical cell-site records involve only records of a user’s location at the beginning and end of phone calls. Even if a person would not reasonably expect his driving over the course of a month to be observed, he could not reasonably expect his cell phone provider to be unaware of his location when he made actual phone calls. Indeed, with historical cell-site records, the government seeks access to records that the provider has already created, collected, and

maintained in the ordinary course of its business, not at the direction of the government.

Third, historical cell-site records are much less precise than the GPS information of *Maynard*. As discussed at pages 18-19 above, *Karo* holds that government use of a tracking device violates the Fourth Amendment only where the monitoring actually reveals the particular private location in which the tracked object may be found. Historical cell-site records lack this precision.

Fourth, *Maynard* was decided on a motion to suppress, so the court could base its decision on the actual facts regarding the information collected by the government using a tracking device. In contrast, the *Orenstein Opinion* was based on the court's speculation about information the government might obtain from historical cell-site records. The *Maynard* approach does not preclude all warrantless tracking; instead, warrantless tracking by the government is evaluated after the fact via a motion to suppress or other appropriate litigation. In contrast, the *Orenstein Opinion* precludes the government from obtaining any historical cell-site information using a 2703(d) order. The *Orenstein Opinion*'s approach violates the usual Fourth Amendment rule that courts in Fourth Amendment cases make "case-by-case determinations that turn on the concrete, not the general, and offering incremental, not sweeping, pronouncements of law." *United States v. Warshak*, 532 F.3d 521, 528 (6th Cir. 2008) (en banc); see also *Sibron v. New York*, 392 U.S. 40, 59-62 (1968) (reasonableness under the Fourth Amendment is properly addressed on the facts of the particular case).

#### **IV. Judicial Notice**

In this Court's October 14 Order, the Court stated that it intended to take judicial notice of certain facts, including "(1) congressional testimony at recent hearings before House and

Senate committees on ECPA reform; (2) published surveys and studies by telecommunications industry groups such as CTIA regarding cell sites and cell phone usage; (3) published reports and product specifications concerning current microcell technology; and (4) published privacy policies of providers regarding call location information.” This Court invited the government to make objections or proposed additions “to these categories of judicially noticed facts.”

Under Rule 201 of the Federal Rules of Evidence, “[a] judicially noticed fact must be one not subject to reasonable dispute in that it is either (1) generally known within the territorial jurisdiction of the trial court or (2) capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned.” The United States cannot determine from the broad categories cited by the Court whether it is appropriate to take judicial notice of any particular facts that might fall within those categories. Some facts that fall within these categories may appropriately be the subject of judicial notice, while others may not. For example, congressional testimony is typically a form of advocacy not subject to rigorous cross-examination, and someone speaking before Congress is not necessarily a source “whose accuracy cannot reasonably be questioned.” Similarly, published surveys, studies, or reports by industry groups may reflect various industry biases.

On the other hand, the United States believes that it is appropriate to take judicial notice of providers’ terms of service and privacy policies for the purpose of establishing the contractual relationship between customers and providers. In addition, the United States notes that it may be appropriate to take judicial notice of FCC reports concerning cell-site records. For example, in one proceeding, the FCC found that a certain location-finding technique accurate to within 500-1000 meters “would be significantly more precise” than “the location of the cell site or sector

receiving the call.” *In re Revision of the Commission’s Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems*, 15 FCC Rcd. 17442, 17462 (Sept. 8, 2000).

**V. Conclusion**

For these reasons, the government respectfully submits that a 2703(d) order may be used to compel disclosure of historical cell-site records.

Respectfully submitted,

JOSE ANGEL MORENO  
UNITED STATES ATTORNEY

By: Eric D. Smith /s/  
Eric D. Smith  
Assistant U. S. Attorney

Nathan Judish  
Senior Counsel, Computer Crime and  
Intellectual Property Section  
U.S. Department of Justice