

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-----X

IN RE APPLICATION OF

THE UNITED STATES OF AMERICA FOR AN :

ORDER FOR DISCLOSURE OF

TELECOMMUNICATIONS RECORDS :

AND AUTHORIZING THE USE OF A PEN

REGISTER AND TRAP AND TRACE :

OPINION AND ORDER

05 Mag. 1763

-----X

Attorney Appearances:

Thomas G.A. Brown, Lauren M. Ouziel, Assistant United States Attorneys, U.S.
Attorney's Office, Southern District of New York, New York, NY

Yuanchung Lee, Assistant Federal Defender, Federal Defenders of New York, Inc., New
York, NY, as amicus curiae.

GABRIEL W. GORENSTEIN, United States Magistrate Judge

On October 19, 2005, the Court granted an ex parte application from the Government seeking an order requiring a provider of cellular telephone service to produce, inter alia, information pertaining to the location of cell site towers receiving a signal from a particular cellular telephone for a period of 60 days. The Court's Order expired on December 18, 2005. Because at least three other district courts have concluded that the Government lacks statutory authority for applications relating to certain types of cell site data, the Court is setting forth the reasons it granted the application in this case. Subsequent to the issuance of the Order, the Court sought additional information and briefing from the Government regarding the application. In addition, the Court asked the Federal Defenders of New York, Inc. to appear as amicus curiae. The Court has greatly benefitted from the briefing provided by both sides.

I. BACKGROUND

Cellular telephones communicate by means of signals to cellular telephone towers, which are operated by the various commercial carriers that provide cellular telephone service. As a cell phone user moves from place to place, the cell phone automatically switches to the tower that provides the best reception. In this case, the Government's application sought information on a prospective basis regarding cell towers being signaled by a specifically identified cellular telephone. The application, which remains under seal, furnishes detailed information indicating that the user of the target cellular telephone is engaged in ongoing criminal activity involving the illegal sale of contraband and that a warrant for the arrest of this person is outstanding. An order was previously granted by another Magistrate Judge in this District for cell site information with respect to the same target telephone.

The relevant portions of the application seek, for a period of 60 days, "cell site activations" for the telephone. The application also seeks a directive that the provider of the service furnish a map showing cellular tower "locations/addresses, sectors and orientations" as well as "the physical address/location of all cellular towers in the specified market." In a portion of the application not relevant to the instant opinion, the application seeks numbers dialed, incoming numbers, call durations, and other information relating to the subscriber of the target cellular telephone. The application contains additional provisions requiring that the provider furnish certain assistance to the federal law enforcement agents necessary to comply with the requested court order.

While the application uses the term "cell-site activations," the Government has specified that it seeks "cell-site information concerning the physical location of the antenna towers

associated with the beginning and termination of calls to and from a particular cellphone.” See Letter to the Court from Thomas A. G. Brown, dated November 22, 2005 (“Gov’t Letter”), at 10. This phrasing corresponds roughly to the information that in fact has been obtained by the Government in this District in the past with respect to cell site information. Under prior orders issued in this District, the Government has been able to obtain a list of each call made by the subject cell phone, along with a date, start time and end time. With respect to the beginning or end of the call (and possibly sometimes in between), there is a listing of a three-digit number assigned to a cellphone tower or base station. At least one cellular provider will give, in addition to the number of the tower, a digit (“1,” “2” or “3”) indicating a 120 degree “face” of the tower towards which the cell phone is signaling.

In suburban or rural areas, towers can be many miles apart. The Court has examined a map of cellular towers of a provider in lower Manhattan, which is one of the areas more densely populated by towers. In this area, the towers may be anywhere from several hundred feet to as many as 2000 feet or more apart.

The Court is aware of three cases that have considered the availability of cell site data: In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority, 396 F. Supp. 2d 747 (S.D. Tex. 2005) (“Texas Decision”); In the Matter of an Application of the United States for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing Release of Subscriber Information and/or Cell Site Information, 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (“EDNY Decision”); and In re Application of the United States for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers (Sealed) and Production of Real Time Cell Site Information, 2005 WL

3160860 (D. Md. Nov. 29, 2005) (“Maryland Decision”). These cases appear to involve requests for cell site information that go beyond both what has been sought in this case and what has actually been received by the Government pursuant to any cell site application in this District. First, the cell site information provided in this District is tied only to telephone calls actually made or received by the telephone user. Thus, no data is provided as to the location of the cell phone when no call is in progress. Second, at any given moment, data is provided only as to a single cell tower with which the cell phone is communicating. Thus, no data is provided that could be “triangulated” to permit the precise location of the cell phone user. Third, the data is not obtained by the Government directly but is instead transmitted from the provider digitally to a computer maintained by the Government. That is, the provider transmits to the Government the cell site data that is stored in the provider’s system. The Government then uses a software program to translate that data into a usable spreadsheet.

II. DISCUSSION

The Government’s application cites to two enactments: the statutes governing the installation of pen registers and trap and trace devices, 18 U.S.C. §§ 3121-27 (“the Pen Register Statute”), and a provision of the Stored Wire and Electronic Communications and Transactional Records Access Act codified at 18 U.S.C. § 2703. We begin our discussion with the text of these statutes inasmuch as “[e]very exercise in statutory construction must begin with the words of the text.” Saks v. Franklin Covey Co., 316 F.3d 337, 345 (2d Cir. 2003). “The plainness or ambiguity of statutory language is determined by reference to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.” Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997) (citations omitted). In general, if the

statutory language is not ambiguous, the statute is construed according to the plain meaning of the words. See, e.g., Greenery Rehab. Group, Inc. v. Hammon, 150 F.3d 226, 231 (2d Cir. 1998) (citing Rubin v. United States, 449 U.S. 424, 430 (1981)). We look to the legislative history and other tools of statutory construction only if the statutory terms are ambiguous. Id. (citing Aslanidis v. United States Lines, Inc., 7 F.3d 1067, 1073 (2d Cir. 1993)).

A. Pen Register Statute

The Pen Register Statute is the statute used to obtain information on an ongoing or prospective basis regarding outgoing calls from a particular telephone (captured by a “pen register”) and incoming calls (captured by a “trap and trace” device). These devices are more fully defined in 18 U.S.C. § 3127(3), (4).¹ A “pen register” is defined as a device that provides not merely the telephone number of a telephone call dialed from the subject telephone – the most common use of the term “pen register” – but also “signaling information” transmitted by the subject telephone itself or the “facility from which a wire or electronic communication is transmitted,” 18 U.S.C. § 3127(3). The term “signaling information” was added by the USA PATRIOT Act in 2001. See Pub. L. No. 107-56, § 216(c)(2), 115 Stat. 272, 290 (2001). Prior to the enactment of the USA PATRIOT act, the District of Columbia Circuit had held in connection with its interpretation of a related statute, 47 U.S.C. § 1001(2), that because a cell phone sends “signals” to cellphone towers in order to operate, the term “signaling information” includes

¹At one time, a “pen register” referred perforce to a physical device that recorded information regarding outgoing telephone calls. In this District at least, law enforcement agencies do not in all instances need to install a physical device on a telephone line to obtain information regarding these calls. Instead, information that was heretofore captured by a pen register can now be transmitted digitally by the telephone service provider. The Government has properly assumed that, despite this change in technology, it is bound to follow the Pen Register Statute to obtain information otherwise covered by the statute.

information on the location of cell site towers used by a cellular telephone. See United States Telecom. Ass’n v. FCC, 227 F.3d 450, 458, 463-64 (D.C. Cir. 2000).² While one cell site decision notes an absence of legislative history indicating that Congress intended cell site data to be included in this term when it enacted the USA PATRIOT Act, see Texas Decision, 396 F. Supp. 2d at 761, the language enacted is not so limited. Indeed, the legislative history reflects that the language regarding “signaling information” would apply “across the board to all communications media.” H. R. Rep. No. 107-236(I), 107th Cong., 1st Sess., available at 2001 WL 1205861, at *53 (Oct. 11, 2001). Accordingly, we will interpret this provision in accordance with its most obvious meaning and the one that naturally would have been available to Congress, through the United States Telecom case, when the statutory language was enacted in 2001. See Lorillard v. Pons, 434 U.S. 575, 581 (1978) (“Where . . . 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.”).

In addition, construing the pen register definition as covering the capture of cell site data is the only way to make sense of a separate statute: 47 U.S.C. § 1002. As described in the next

²Because the location information is “transmitted” by the cell phone, a pen register (not a trap and trace device) identifies location information for both incoming and outgoing calls. See 18 U.S.C. § 3127(3).

On a separate point, amicus contends that the “signaling information” available under the Pen Register Statute is only the “signaling information” that is transmitted during a particular telephone call. See Letter to the Court from Yuanchung Lee, dated October 27, 2005 (“Amicus Letter”) at 16. The statute is ambiguous on this point, however. It says only that a pen register records the “signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted.” 18 U.S.C. § 3127(3). The term “is transmitted” is susceptible of two meanings: it could refer either to a particular communication or to an ongoing transmission. It is not necessary to reach this issue, however, because here the Government has sought only cell-site information tied to telephone calls.

section, that statute specifically assumes that cell site data is available under the Pen Register Statute.

Notably, the showing required to install a pen register is a low one: the Government need only identify the law enforcement agency conducting the investigation and certify that the information likely to be obtained is “relevant to an ongoing criminal investigation” being conducted by the agency. 18 U.S.C. § 3122(b)(1), (2). Orders requiring the installation of a pen register may not exceed 60 days, though they may be extended for additional 60-day periods if the required showing is made. 18 U.S.C. § 3123(c). In certain emergency situations, a pen register may be installed even in the absence of a court order. 18 U.S.C. § 3125. The Pen Register Statute explicitly excludes from its definition “the contents of any communication” – an exclusion not relevant to the instant application as there is no effort to obtain the contents of any telephone calls. See 18 U.S.C. § 3127(3).

The Government has certified that the cell site information it seeks here is “relevant and material to an ongoing investigation.” Thus, the Pen Register Statute would by itself provide authority for the order being sought by the Government were it not for a provision codified elsewhere in the United States Code. That provision occurs in an “exception” clause within 47 U.S.C. § 1002, which is entitled “Assistance capability requirements.”

B. 47 U.S.C. § 1002

Section 1002 was enacted as part of the Communications Assistance for Law Enforcement Act of 1994. It requires telecommunications carriers to ensure that their equipment is capable of providing a law enforcement agency with information to which it may be entitled under statutes relating to electronic surveillance. Section 1002 provides, in pertinent part, as follows:

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 –

(A) before, during, or immediately after the transmission of a wire or electronic communication (or at such later time as may be acceptable to the government); and

(B) in a manner that allows it to be associated with the communication to which it pertains,

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), 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);

47 U.S.C. § 1002(a)(2) (emphasis added).

The phrase “information that may disclose the physical location of the subscriber” in the exception clause can reasonably be interpreted to encompass the prospective cell site information being sought by the Government here, although, as already discussed, the information the Government obtains in this District “disclose[s] the physical location” of the subscriber in only the roughest manner.³

³A literal reading of this exception clause might lead one to question whether it is of any relevance at all to the Government’s application inasmuch as the clause is framed only as an exception to the sort of “capab[ilities]” a carrier is obligated to “ensure” that it possesses. Under this reading, the exception clause merely states that a carrier is not obligated to ensure that it possesses the capability to disclose physical location information. The clause says nothing about whether the carrier should or should not disclose such information. Nor does it say anything about whether the Government may obtain an order for such information. As is described below, however, the legislative history relevant to this provision reflects that a literal reading of this kind would be at odds with the intention of Congress.

The effect of the exception clause is not obvious at first glance. But the clause plainly reflects an underlying assumption that physical location data would have been obtainable under the Pen Register Statute in the absence of the exception clause. Otherwise, it would have been unnecessary to add the exception clause at all. Indeed, the legislative history of section 1002 states as much. See H. Rep. 103-827(I), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 1994 WL 557197, at *17 (Oct. 4, 1994) (“Currently, in some cellular systems, transactional data that could be obtained by a pen register may include location information.”); S. Rep. 103-402, available at 1994 WL 562252, at *18 (Oct. 6, 1994) (same).⁴

But if the exception clause of 47 U.S.C. § 1002(a)(2) is read to mean that a pen register may not be used at all to deliver cell site information to the Government, then the Government may not acquire cell site information by any mechanism. This is because the Pen Register Statute is clear that the device that captures cell site information – that is, a “pen register” – may be installed only pursuant to the Pen Register Statute itself. As noted, the Pen Register Statute defines a pen register as a device that provides “signaling information” (e.g., cell site information). See 18 U.S.C. § 3127(3). At the same time, the Pen Register Statute states unequivocally (with exceptions not relevant here) that “no person may install or use a pen register . . . without first obtaining a court order under section 3123” – that is, pursuant to a court order issued under the Pen Register Statute itself. See 18 U.S.C. § 3121(a). Taken together, the two

⁴In fact, the definition of a “pen register” in effect at the time of the exception clause’s passage did not seem to include cell site or location information, inasmuch as the term “pen register,” prior to the USA PATRIOT Act amendment in 2001, had been defined as a device that identified “the number dialed or otherwise transmitted.” See Pub. L. No. 99-508, §301, 100 Stat 1848 (Oct. 21, 1986). Nonetheless, Congress obviously thought such information was available under the Pen Register Statute when the exception clause was enacted in 1994.

sections require that prospective cell site information may be obtained only pursuant to the Pen Register Statute. If the exception clause in 47 U.S.C. § 1002(a)(2) is read to mean that the Pen Register Statute may not be used in any form to obtain cell site information, as is urged by amicus and the other cell site cases, the exception clause in combination with section 3121(a) would constitute a directive that cell site information was not obtainable by any mechanism at all.

Amicus and the other cell site cases do not address this question and simply assume that 47 U.S.C. § 1002(a)(2) means that some mechanism other than the Pen Register Statute may be used to obtain cell site information as long as this mechanism stands on its own – that is, as an independent ground authorizing the collection of cell site data. The cell site cases believe a search warrant under Fed. R. Crim. P. 41 is the appropriate mechanism, see, e.g., Texas Decision, 396 F. Supp. 2d at 757, and amicus asserts that it is the Title III wiretap statute, see Letter to the Court dated December 6, 2005 from Yuanchung Lee, at 5-6. But, again, this reading fails to give effect to the explicit directives contained in the Pen Register Statute that a pen register – which is defined to include a device providing cell site information – can be installed only pursuant to “a court order under section 3123 of [Title 18].” 18 U.S.C. § 3121(a). In other words, Fed. R. Crim. P. 41 or Title III cannot by themselves provide authority for the Government’s application because any warrant or order issued pursuant to those mechanisms must necessarily authorize the installation of a “pen register.”

If the cell site cases and amicus were correct in their interpretation of the exception clause – that is, that it constitutes a simple direction that no cell site information may be obtained pursuant to the Pen Register Statute – this Court might conclude that Congress intended that the Government could not obtain cell site information by any means. However, the exception clause

in fact does not contain a direction that no cell site information may be obtained “pursuant” to the Pen Register Statute. Instead, it states that cell site information may not be obtained “solely pursuant” to the Pen Register Statute. 47 U.S.C. § 1002(a)(2). The phrase “solely pursuant” is an unusual one – so unusual that the only time it appears in the United States Code is in 47 U.S.C. § 1002(a)(2).⁵

The use of the word “solely” is significant. “Solely” means “without another” or “to the exclusion of all else.” See Merriam-Webster’s Collegiate Dictionary (10th ed. 2000), at 1114. If we are told that an act is not done “solely” pursuant to some authority, it can only mean that the act is done pursuant to that authority “with[] another” authority. Id. As a result, the use of the word “solely” in section 1002 necessarily implies that “another” mechanism may be combined – albeit in some unspecified way – with the Pen Register Statute to authorize disclosure of cell site information.

As just noted, amicus and the other cell-site cases read the exception clause as a direction to the Government to rely exclusively on some other mechanism to obtain the cell-site information and to rely on that other mechanism alone. We have already pointed out one problem with this reading – that it results in a contradiction in the terms of the Pen Register Statute and 47 U.S.C. § 1002. But there is a second problem, which is reflected in section 1002 itself. If section 1002 means that the Pen Register Statute cannot be relied on whatsoever to obtain cell site

⁵The phrase “only pursuant” appears several dozen times in the United States Code. But in each instance the phrase is used to direct affirmatively how an act is to be done – for example, to direct that judicial review of an order may be obtained “only pursuant” to a particular statutory provision. 49 U.S.C. § 46301(d)(7)(D)(iii). Here, however, the exception clause authorizes something to be done as long as it is not done “solely pursuant” to a particular statutory provision. Thus, the statutes using “only pursuant” provide no assistance in our interpretation.

information, it would have been sufficient for the statute's drafters to use the word "pursuant" rather than the phrase "solely pursuant." In other words, the use of the word "pursuant" would have been enough by itself to give a clear direction that cell-site information cannot be obtained under the Pen Register Statute. Given the doctrine that "we must, if possible, construe a statute to give every word some operative effect," Cooper Industries, Inc. v. Aviall Services, Inc., 125 S. Ct. 577, 584 (2004), the word "solely" must be given semantic content if it is possible to do so. The most reasonable reading of the word "solely" is that if cell-site information is not being obtained "solely" pursuant to the statute, it is being obtained pursuant to the opposite of "solely": that is, not "alone" but in combination with some other mechanism.

While we have extracted some semantic content out of the word "solely," it has hardly been a satisfying exercise inasmuch as we are left with the conclusion that Congress has given a direction that cell site information may be obtained through some unexplained combination of the Pen Register Statute with some other unspecified mechanism. As unsatisfying as this result is, the only alternative is either (1) to ignore the plain dictate of 18 U.S.C. § 3121(a) by assuming that 47 U.S.C. § 1002 means that some other mechanism may be used to intercept "physical location" information if it can do so on an independent basis, or (2) to ignore Congress's inclusion of the otherwise unnecessary word "solely" and conclude that ongoing cell site data is not obtainable at all.

We reject the first choice as it requires us to ignore a clear statutory command. Nor can we accept the second choice because it requires us to conclude that Congress intended that ongoing cell site location information could not be obtained by any means at all. Congress, however, plainly manifested its intention to the contrary. First, as noted, any such interpretation

necessarily reads the word “solely” out of the exception clause. If Congress had intended that no prospective cell site data be obtainable, it would have simply said in the exception clause that physical location information could not be obtained “pursuant” to the Pen Register Statute.

Second, the only legislative history that directly bears on the meaning of the exception clause – consisting of a prepared statement of former Federal Bureau of Investigation (“FBI”) director Louis Freeh – reflects that the §1002 exception was put in at the suggestion of the FBI itself, as a way of assuring Congress that the FBI would rely on mechanisms – referred to as “court orders and subpoenas” – other than the Pen Register Statute to obtain physical location information, including cell site data. See Police Access to Advanced Communication Systems: Before the Subcommittee on Technology and the Law of the Committee on the Judiciary United States Senate and the Subcommittee on Civil and Constitutional Rights of the Committee on the Judiciary House of Representatives (1994) (statement of FBI Director Louis J. Freeh) (“Freeh Statement”), available at 1994 WL 223962 (“Even when such generalized location information, or any other type of ‘transactional’ information, is obtained from communications service providers, court orders or subpoenas are required and are obtained.”). Thus, it would not make sense for Congress to have taken Director Freeh up on his proposal by barring law enforcement agencies from obtaining cell site information entirely.

Third, the District of Columbia Circuit, in considering the “solely pursuant” exception in the context of a Federal Communications Commission’s rule-making proceeding, approved of the FCC’s decision that section 1002 “simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices.” United States Telecom Ass’n, 227 F.3d at 463 (citing In the Matter of Communications

Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, 16815, ¶ 44 (1999)). The plain import of this statement is that law enforcement agencies would be able to get authorizations to obtain cell site information from some mechanism, although the Government would have to meet an authorization requirement different from the minimal standard provided in the Pen Register Statute.

Having rejected the two alternatives – that is, that cell site data can be obtained without reliance on the Pen Register Statute or that it is not obtainable at all – we are back at the originally discussed reading of the word “solely.” We thus conclude that Congress expected physical location information – including cell site information – would be obtainable by the Government by using some mechanism in combination with the Pen Register Statute. The idea of combining some mechanism with as yet undetermined features of the Pen Register Statute is certainly an unattractive choice. After all, no guidance is provided as to how this “combination” is to be achieved. But, again, in light of the language used in section 1002, the Court believes that it is the only choice possible.

The next question is (1) whether the other mechanism relied on by the Government – 18 U.S.C. § 2703 – is an appropriate mechanism to “combine” with the Pen Register Statute, and (2) if so, how section 2703 should be “combined” with the Pen Register Statute. To answer these questions, we turn to an examination of section 2703.

C. Section 2703

Section 2703 contains three main sections that authorize the Government to obtain records. Two are not relevant here: section 2703(a) authorizes disclosure of the contents of wire or electronic communications held by a “provider of electronic communication service” and

section 2703(b) authorizes disclosure of the contents of wire or electronic communications in a “remote computing service.”

Section 2703(c)(1) – the section relied upon by the Government – provides that a “governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications),” provided the Government “offers specific and articulable facts showing . . . reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation” under 18 U.S.C. § 2703(d). A separate portion of section 2703 provides that basic subscriber information – such as name, address and duration of calls – need not even meet this threshold showing but is obtainable merely by subpoena. See 18 U.S.C. § 2703(c)(2). The Government may obtain additional information about a subscriber under 18 U.S.C. § 2703(c)(1)(B) as long as the “specific and articulable facts” standard is met.

The first question that arises is whether prospective cell site data is encompassed in the phrase “record or other information pertaining to a subscriber to or customer of [an electronic communication] service.”

Certainly, prospective cell site data is “information,” and it may also be said – in this District at least – to be in the form of a “record” inasmuch as cell site information is transmitted to the Government only after it has been in the possession of the cell phone company. Cell site data also “pertain[s]” to a subscriber to or customer of cellular telephone service. The remaining question is whether cellular telephone service constitutes an “electronic communication service.” According to 18 U.S.C. § 2711(1), we must turn to 18 U.S.C. § 2510 for the definition of this

term. Section 2510 defines an “electronic communication service” 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).

The phrase “electronic communication” is itself defined. Section 2510(12) provides that “electronic communication” means “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce.” With the definition taken thus far, it would be plain that a user of a cellular telephone is a “customer of an electronic communication service” under section 2703(d) since the cellular telephone makes transmissions to a tower through an electromagnetic system. See generally <http://www.fda.gov/cellphones/qa.html#1> (wireless phones rely on radio-frequency energy, which is a form of electromagnetic energy).

Amicus argues, however, that an exception contained in the definition of “electronic communication” in section 2510(12) is of importance here. Amicus Letter at 8. The exception states that an “electronic communication . . . does not include . . . any communication from a tracking device (as defined in section 3117 of this title).” 18 U.S.C. § 2510(12)(C). Section 3117 in turn defines a tracking device as “an electronic or mechanical device which permits the tracking of the movement of a person or thing.” 18 U.S.C. § 3117(b).

Because a cellular telephone arguably has the capability of being a “device which permits . . . tracking” – in addition to its normal voice and data transmission uses – we must determine if the tracking device exception to the definition of “electronic communication” means that a

cellular telephone service subscriber is not in fact a “customer of an electronic communication service” under section 2703(c).

To understand the import of this exception, it is necessary to examine what “service” is being provided to the customer of a cellular telephone. This is because the term “electronic communication” is used in section 2703 to describe the sort of “service” that an individual subscribes to or is a customer of, and the Government may only obtain “records or other information” pertaining to such a person. Section 2510(15) says that the relevant service is a service that provides to users thereof the ability to “send or receive . . . electronic communications.” The exception in section 2510(12)(C) tells us only that “tracking” information is not considered to be an electronic communication. But this exception does not alter the fact that the cellular telephone service that the customer uses and to which the subscriber subscribes is nonetheless an “electronic communication service” under section 2510(15).

We next turn back to section 2703, which governs “information” pertaining to “customers and users” of electronic communications service. It is certainly the case that cell site or tracking information constitutes “information” pertaining to customers or users of electronic communications services. Thus, such cell site or tracking information comes within section 2703(c) and consequently is the sort of “information” that the Government may seek pursuant to an order under section 2703(d).

The objection to this reading, see Amicus Letter at 8-9, appears to be as follows: section 2703(c) governs information pertaining to electronic communication services. The definition of “electronic communication” in section 2510(12)(C) excludes tracking information. Therefore, the Government cannot get under section 2703 the tracking information a cell phone provides.

The problem with this syllogism is that it assumes that the term “information” in section 2703(c) is limited by the definition contained in section 2510. In fact, section 2510 does not speak to the scope of the term “information” in section 2703. Rather, section 2510 speaks only to the meaning of the term “electronic communication service,” which it defines broadly as a service that “provides to users thereof the ability to send or receive . . . electronic communications.” Thus, the term “electronic communications service” in section 2703(c) refers broadly to the “service” of providing users with the “ability to send or receive . . . electronic communications.” It does not refer to any one particular piece of information, such as cell site information, that might be obtainable from the device carried by the user of the service. While tracking information is not to be considered part of “electronic communications” pursuant to the exception contained in 2510(12)(C), this does not alter the fact that the cellular telephone service to which a cellphone customer subscribes necessarily comes within the definition of section 2510(15). After all, the service a cellular telephone company “provides to users” is the ability to make cellular telephone calls, not exclusively tracking information. Inasmuch as a service that provides cellular telephone capabilities is within section 2510(15), information pertaining to a subscriber to or customer of that “service” is obtainable under section 2703(c).

In other words, information on the location of cell towers is not the “service” to which a cellular customer subscribes. Instead, the user subscribes to the voice – and perhaps data – transmission capabilities provided by the cellular carrier. Although tower location information may be a necessary ingredient for the operation of that service, the “service” to which the user subscribes is still the “electronic communication” capabilities of the cellular telephone. Section 2703(c) tells us broadly that the Government may obtain “information” pertaining to users of this

sort of service. Cell site information is just one of many possible categories of “information” that pertains to users of this service. The exception in section 2510(12)(C) does not purport to limit the meaning of the term “information.”⁶

It may seem anomalous that the Government may obtain under section 2703 a particular category of information pertaining to a user of electronic communications that is excepted from the term electronic communications itself. But this is not surprising given the multiple purposes that the section 2510(12)(C) exception serves. The definitions in section 2510 apply across the board to (1) wiretaps; (2) section 2703 applications; and (3) Pen Register Statute applications. See 18 U.S.C. §§ 2510 (introductory clause); 2711(1); and 3127(1). There is no suggestion in the structure of the statutes that the section 2510(12)(C) exception was meant to limit in any way the “information” that the Government was entitled to get under section 2703(c).

In light of the analysis so far, section 2703(c)’s use of the term “information” would cover the prospective cell site data being sought here. At least some of the cell site cases recognize that the term “information” includes historical cell site information. See Texas Decision, 396 F. Supp. 2d at 759 n.16; EDNY Decision, 396 F. Supp. 2d at 313; Maryland Decision, 2005 WL 3160860, at *4; see also Amicus Letter at 12. They question, however, whether cell site information not yet in existence at the time of the order – that is, prospective or what is colloquially referred to as “real time” data – may be included in the term “information.”

⁶There is potentially an independent reason why the exception clause in section 2510(12)(C) does not limit the Government’s ability to obtain cell site information under section 2703. The exception clause points to section 3117 for the definition of a tracking device. Section 3117, however, is a statute that refers to a tracking device that has been “install[ed]” at the behest of the Government. 18 U.S.C. § 3117(a). Here, however, no tracking device has been “installed.”

The text of the statute itself contains no limitation of this kind. Some courts have pointed to the title of the chapter in which the statute appears – the “Stored Wire and Electronic Communications and Transactional Records Access” – as harboring some importance in this regard. See Texas Decision, 396 F. Supp. 2d at 760. But this title is of limited significance for two reasons. First, it refers to types of data – “communications” and “records” – that are narrower than one of the actual terms in section 2703(c): “information.” Second, and more significantly, even the data being obtained regarding the location of the cell phone is in fact “stored” by the carrier – at least in this District. Cell site information is not obtained directly by the Government. Instead, it is transmitted to the Government only after it has come into the possession of the cellular telephone provider in the form of a record.

The question of “historical” versus “real time” data is still of some significance, however. While the data the Government seeks can appropriately be characterized as “stored” or “historical” records by the time the Government gets possession of them, the Government wants that information on an ongoing basis. That is, it wants a continuing order for the cell phone company to provide the stored records in the future.

Amicus and the cell site cases have properly pointed to aspects of 2703 that make it unsuited to requiring the carrier to provide cell site data on an ongoing basis. Amicus Letter at 12. The two related statutes that plainly permit transmission of information to the Government on an ongoing basis – the Pen Register Statute and Title III – both contain limitations, 60 days and 30 days respectively, that cap the duration of any prospective orders. See 18 U.S.C. § 3123(c)(1); 18 U.S.C. § 2518(5). Section 2703, by contrast, contains no such time limitation. In a similar vein, the Pen Register Statute and Title III contain automatic sealing provisions, see 18 U.S.C.

§ 2518(8)(b) and 3123(d)(1) – provisions that are obviously important to the Government when obtaining ongoing information – whereas section 2703 does not.

These omissions, however, are understandable when considered in the context of the discussion presented thus far. Amicus and the cell site cases have conducted their analysis of section 2703 as an effort to determine whether Congress “intended” section 2703 to cover prospective cell site data. See, e.g., Texas Decision, 396 F. Supp. 2d at 760; Amicus Letter at 11-12. But there is no reason to believe that section 2703 was specifically enacted as the mechanism to cover such cell site data inasmuch as the Pen Register Statute professes to be the only statute that authorizes the installation of the device used to capture this sort of data, i.e. “signaling information.” See 18 U.S.C. § 3121(a).

Section 2703, however, remains an appropriate candidate as a legal mechanism that could properly be “combined,” as contemplated by 47 U.S.C. §1002(a)(2), with the Pen Register Statute to obtain cell site locations. This is because the text of section 2703(c) covers the data the Government seeks here. The heart of the statute – granting authority to obtain “information” about cell phone customers – does not on its face contain any limitation regarding when such information may come into being. It is thus susceptible to an interpretation that the “information” sought might come into being in the future. Moreover, because cell site data in this District exists as a record before it is transmitted to the Government, the text of the statute does not prevent the Government from presenting daily or hourly (or even more frequent) applications to the Court to obtain historical cell site data. Thus, as a theoretical matter, the statute permits the Government to obtain cell site data on a continuing or ongoing basis even under a narrow reading of section 2703.

The principal reason why the statute does not serve easily as a fully independent source of authority for providing such data is a structural one: the statute does not contain certain procedural features, such as a time limitation, that Congress has typically included in statutes that permit the gathering of ongoing information. But this is an understandable omission given that Congress envisioned a pen register as the mechanism that would be used to capture cell site data, and the Pen Register Statute contains the procedural features missing from section 2703. In other words, the Pen Register Statute contains the time limitation (and sealing) provisions that are tied to the very “device” – that is, the pen register – that Congress deemed necessary to obtain prospective cell site information. It is thus logical to conclude that these two statutes in combination contain the necessary authority contemplated by Congress in 47 U.S.C. § 1002.

Section 2703 is an appropriate mechanism to “combine” with the Pen Register Statute for yet another reason. As the District of Columbia Circuit recognized, and as is implicit from the statement presented by Director Freeh, the objection to using the Pen Register Statute alone for the purpose of obtaining cell site data was that it contained a “minimal[]” authorization requirement. United States Telecom Ass’n, 227 F.3d at 463 (citing In the Matter of Communications Assistance for Law Enforcement Act, 14 F.C.C.R. 16794, 16815, ¶ 44 (1999)). Thus, the District of Columbia Circuit concluded that the section 1002 exception “simply imposes upon law enforcement an authorization requirement different from that minimally necessary for use of pen registers and trap and trace devices.” Id. Section 2703, by contrast, contains a higher authorization requirement than that required for a pen register. While the Pen Register Statute permits disclosure of information upon the mere showing that the information likely to be obtained is “relevant to an ongoing criminal investigation” being conducted by the agency, 18

U.S.C. § 3122(b)(2), section 2703 requires the Government to offer “specific and articulable facts showing . . . reasonable grounds to believe that . . . the records or other information sought, are relevant and material to an ongoing criminal investigation.” See 18 U.S.C. § 2703(d). Using section 2703 thus fulfills the apparent purpose of the section 1002 exception: to require something different from than the “minimal[]” authorization requirement imposed by the Pen Register Statute.

Of course, amicus and the cell site cases suggest that Fed. R. Crim. P. 41 or Title III are better mechanisms than section 2703 to obtain the cell site information. They rely on them, however, based in part on their belief that the non-pen-register mechanism for obtaining cell-site data must operate independently of the Pen Register Statute.⁷ But once this proposition is rejected, section 2703 is a far more obvious source of authority since it covers the very sort of information that is being sought under the warrant. Its only failing is that it does not explicitly allow for the continuous release of such information. Certainly, Title III does not represent an appropriate fit for cell site information inasmuch as its purpose is to govern the interception of the “contents” of communications. See, e.g., 18 U.S.C. §§ 2510(4), 2511(1); United States v. New York Tel. Co., 434 U.S. 159, 167 (1977) (pen registers not within Title III because they do not acquire the “contents” of communications).

In sum, section 2703 is the most obvious candidate to be used in combination with the Pen Register Statute to authorize the ongoing collection of cell site information because it covers cell site information generally. Section 2703’s absence of procedural provisions that typically attach

⁷Their reliance is also based on the belief that a cell phone is transformed into a “tracking device” when prospective cell site data is sought. For reasons discussed further in the next section, the requirements that attach to tracking devices are not relevant here.

to the transmission of ongoing information is explained by the fact that the pen register is the proper “device” to obtain cell-site information. Thus the Pen Register Statute’s procedural provisions that are tied to such a device are appropriately combined with an application under section 2703 to obtain such information.

D. Effect of the Fourth Amendment

The only remaining question is whether the issuance of a court order for cell site information under section 2703 and the Pen Register Statute is unconstitutional because it violates the Fourth Amendment’s prohibition against unreasonable searches and seizures. Amicus (and some of the cell site cases) discusses the issue in terms of whether the cell phone is a “tracking device” and whether a warrant grounded in probable cause is necessary for the installation of such a device. But the data being sought by the Government in this District is not what amicus believes it to be. The information does not provide a “virtual map” of the user’s location. Amicus Letter at 24. The information does not pinpoint a user’s location within a building. Instead, it only identifies a nearby cell tower and, for some carriers, a 120-degree face of that tower. These towers can be up to 10 or more miles apart in rural areas and may be up to a half-mile or more apart even in urban areas. Moreover, the data is provided only in the event the user happens to make or receive a telephone call. Thus, amicus’s reference to tracking devices and the cases considering this technology is not on point.⁸

⁸The tracking device statute, 18 U.S.C. § 3117, is of no relevance at all because it provides no guidance on what showing must be made to install a tracking device. It states only that “If a court is empowered to issue a warrant or other order for the installation of a mobile tracking device, 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.” 18 U.S.C. § 3117(a) (emphasis added); see also United States v. Gbemisola, 225 F.3d 753, 758 (D.C. Cir. 2000) (“section 3117 does not prohibit the use of a tracking device in the absence of conformity

In any event, the case most strongly relied on by amicus, United States v. Karo, 468 U.S. 705 (1984), held only that the installation of a true tracking device without the knowledge of the person it was tracking must be the subject of a warrant if the device discloses its location inside someone’s home and that information could not have been obtained by observation. 468 U.S. at 714; cf. United States v. Knotts, 460 U.S. 276, 282 (1983) (no warrant required where the installed tracking device reveals information observable from a public highway). Here, however, the Government does not seek to install the “tracking device”: the individual has chosen to carry a device and to permit transmission of its information to a third party, the carrier. As the Supreme Court has held in the context of telephone numbers captured by a pen register, the provision of information to a third party does not implicate the Fourth Amendment. See Smith v. Maryland, 442 U.S. 735, 744 (1979); see also United States Telecom. Ass’n v. FCC, 227 F.3d at 459 (“Smith’s reason for finding no legitimate expectation of privacy in dialed telephone numbers – that callers voluntarily convey this information to the phone company in order to complete calls – applies as well to much of the information provided by the challenged capabilities.”) (referring to information that included “antenna tower location”). Amicus argues that the information is not voluntarily conveyed because, unlike telephone numbers, location information is being transmitted even in the absence of a telephone call. Amicus Letter at 23 (citing Texas Decision,

with the section”). Not only is the statute prefaced by a conditional clause, the statute itself contemplates that a tracking device may be installed merely pursuant to an “order” – that is, without a warrant and thus without a probable cause showing. And, of course, it contemplates the “installation” of a tracking device, which has not been sought here.

396 F. Supp. 2d at 756-57). The Court need not reach this question because the only information being sought by the Government here is information tied to an actual telephone call.⁹

Conclusion

The above analysis applies with respect to the instant Order, and is based upon the technology that is available to the Government in this District. Because the Court cannot know how that technology may change, it intends to identify specifically, in any future orders authorizing the provision of cell site information, the character of the information that may be provided by a carrier. Specifically, any such Order will make clear that it contemplates the production only of: (1) information regarding cell site location that consists of the tower receiving transmissions from the target phone (and any information on what portion of that tower is receiving a transmission, if available); (2) tower information that is tied to a particular telephone call made or received by the user; and (3) information that is transmitted from the provider to the Government. If the Government seeks to obtain other information, it should provide additional briefing on why such information is permissible under the relevant authorities.

Dated: December 20, 2005
New York, New York

GABRIEL W. GORENSTEIN
United States Magistrate Judge

⁹United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004), suggests in dictum that there might be a Fourth Amendment concern where a law enforcement agent purposely dialed the target cellphone in order to obtain location data. The court viewed such an act as demonstrating that the user was not voluntarily providing the cell site data. Here, we have no request to authorize such an act.