

**AMERICAN CIVIL LIBERTIES UNION**  
**POSITION PAPER / SAMPLE BRIEF**

**PROSPECTIVE CELL PHONE LOCATION TRACKING**

The American Civil Liberties Union (“ACLU”) has prepared this position paper and sample brief in support of our view that the government must obtain a warrant based on probable cause and particular description before tracking the location of cell phones. We are aware that in many jurisdictions, the government has attempted to track individuals’ cell phone location information under the Electronic Communications Privacy Act (“ECPA”), Pub. L. No. 99-508, 100 Stat. 1848 (1986), by showing merely that the information sought is relevant and material to an ongoing criminal investigation. The government’s strained interpretation of ECPA, however, contravenes the plain language of the statute; moreover, its claimed authority to infringe on Americans’ reasonable expectations of privacy without warrants, if allowed, would violate the Fourth Amendment. Courts faced with an application for cell phone location tracking should therefore join the majority of judges who have recently rejected the government’s contentions in unsealed orders and have concluded that the statutory scheme and constitutional concerns prohibit the government from obtaining prospective cell phone location information under ECPA.<sup>1</sup>

**FACTUAL BACKGROUND**

Cellular phone technology has given law enforcement a new surveillance tool of previously unimagined magnitude. As of December 2009, over 90% of the overall population of the United States subscribed to cell phone service—an estimated 285.6 million people.<sup>2</sup> These cell phones yield several types of information about their users’ past and present location and movements that are of interest to the government: cell site location data, triangulation data, and GPS data.

**I. CELL SITE LOCATION DATA**

The most basic type of cell phone location information is “cell site” data, or “cell site location information,” which refers to the identity of the cell tower from which the phone is

---

<sup>1</sup> The scope of this brief is limited to prospective cell phone tracking. Our arguments regarding access to historical cell phone location information are detailed in an *amici curiae* brief filed in the Third Circuit. Brief of *Amici Curiae* Electronic Frontier Foundation, the American Civil Liberties Union, the ACLU-Foundation of Pennsylvania, Inc., and the Center for Democracy and Technology in Support of Affirmance of the District Court, *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t*, No. 08-4227 (3d Cir. filed March 16, 2009), available at <http://www.aclu.org/files/assets/FiledCellTrackingBrief.pdf>.

<sup>2</sup> CTIA The Wireless Association, US Wireless Quick Facts, <http://www.ctia.org/advocacy/research/index.cfm/AID/10323> (last visited July 28, 2010).

receiving the strongest signal at the time and the sector of the tower facing the phone.<sup>3</sup> This data is generated because, whenever users have their cell phones on, the phones automatically scan for the cell tower and the sector of that tower that provides the best reception and, approximately every seven seconds, the phones register their location information with the network.<sup>4</sup> The carriers keep track of the registration information in order to identify the cell tower through which calls can be made and received.<sup>5</sup> The towers also monitor the strength of the telephone's signal during the progress of the call in order to manage the hand-off of calls from one adjacent tower to another if the caller is moving during the call.<sup>6</sup>

Government requests for cell site location data are usually of two types: historical cell site data, which can be used to retrace previous movements,<sup>7</sup> or prospective cell site data, which can be used to track the phone in real-time.<sup>8</sup> Prospective data may encompass cell site information at the beginning and end of phone calls,<sup>9</sup> during the course of the calls,<sup>10</sup> and whenever the phone is on.<sup>11</sup>

The precision of cell site location information depends, in part, on the size of the coverage area of each cell tower.<sup>12</sup> This means that as the numbers of cell towers have increased and the coverage area for each cell tower has shrunk in response to demand for wireless technology, cell site location information has become more precise.<sup>13</sup> The government's expert stated in 2006 that cell site location information can be as accurate as 200 meters in some

---

<sup>3</sup> See, e.g., *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, 412 F. Supp. 2d 947, 948-49 (E.D. Wis. 2006) (Callahan), *aff'd*, No. 06-MISC-004, 2006 WL 2871743 (E.D. Wis. Oct. 6, 2006) (Adelman). For ease of reference, after the first full citation subsequent citations to opinions on cell phone tracking will be referred to by the district court, year, and the judge issuing the opinion.

<sup>4</sup> See *In re the Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (Lenihan), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *appeal docketed*, No. 08-4227.

<sup>5</sup> *Id.*

<sup>6</sup> See Declaration of Henry Hodor at 7 n.6, available at [http://www.aclu.org/pdfs/freespeech/cellfoia\\_release\\_4805\\_001\\_20091022.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_release_4805_001_20091022.pdf). The Hodor Declaration offers a technical overview of cell phone tracking. The ACLU and the Electronic Frontier Foundation (EFF) obtained it pursuant to an ongoing Freedom of Information Act lawsuit that they filed to access records related to the government's use of cell phone tracking. See *ACLU v. Dep't of Justice*, No. 08-1157, 2010 WL 1140868 (D.D.C. Mar. 26, 2010), *appeal docketed*, No. 10-5159.

<sup>7</sup> See, e.g., W.D. Pa. 2008 (Lenihan), 534 F. Supp. 2d at 586 n.4.

<sup>8</sup> See, e.g., *In re the Application of the U.S. for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 817 (S.D. Tex. 2006) (Smith).

<sup>9</sup> See, e.g., E.D. Wis. 2006 (Callahan), 412 F. Supp. 2d at 948-49.

<sup>10</sup> See, e.g., *In re the Application of the U.S. for an Order (1) Authorizing the Use of a Pen Register and a Trap and Trace Device and (2) Authorizing the Release of Subscriber Info. and/or Cell Site Information*, 396 F. Supp. 2d 294, 296 (E.D.N.Y. 2005) (Orenstein).

<sup>11</sup> See, e.g., *In re the Application of the U.S. for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification Sys. on Tel. No. [Sealed] and [Sealed] and the Prod. of Real Time Cell Site Info.*, 402 F. Supp. 2d 597, 598 (D. Md. 2005) (Bredar).

<sup>12</sup> Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary, 111th Cong. (2010) (statement of Professor Matt Blaze at 7-9), <http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf> (hereinafter, "Blaze testimony").

<sup>13</sup> *Id.*; CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* at 9 (2009) (showing increase in the number of active cellular towers), [http://files.ctia.org/pdf/CTIA\\_Survey\\_Midyear\\_2009\\_Graphics.pdf](http://files.ctia.org/pdf/CTIA_Survey_Midyear_2009_Graphics.pdf).

areas.<sup>14</sup> But the latest generation of cellular towers now may cover an area as small as a tunnel, subway, specific roadway, particular floor of a building, or even an individual home or office.<sup>15</sup> Further improvement in precision can be expected given the explosive demand for wireless technology and its new services, to the point that “[t]he gap between the locational precision in today’s cellular call detail records and that of a GPS tracker is closing, especially as carriers incorporate the latest technologies into their networks.”<sup>16</sup>

In any event, regardless of the precise range of accuracy of cell site location information, the government has been using the information or has attempted to use the information to locate people and to present this evidence at criminal trials.<sup>17</sup> In a case in the Eastern District of Pennsylvania, for example, the government presented the expert testimony of a FBI agent who used cell site location information to attempt to map the movement of the defendant and to show that she was at a private residence.<sup>18</sup> The agent testified that analysis of cell site information over time can narrow the geographical area in which the phone is likely located, and that he has used the information close to 150 times to locate people such as fugitives.<sup>19</sup> He testified, for example, that the fact that the phone registered in alternation with two adjacent cell towers is “extremely consistent with the phone being somewhere in the middle of the two cell site sectors.”<sup>20</sup> Conversely, according to the agent, the fact that the phone was consistently registering with the same cell site over a period of time “usually means that the phone is very close to the tower.”<sup>21</sup> In addition, he stated that where the phone registered with a series of different towers, it is likely that the person carrying the phone was on the move in a certain trajectory.<sup>22</sup>

The government has thus taken the position that even already existing cell site location information is sufficiently accurate as evidence of an individual’s whereabouts. Future improvements in technology will further refine the accuracy of this data.

## II. TRIANGULATION DATA

The government can currently obtain precise location data at a high level of accuracy through “triangulation,” which entails collecting and analyzing data of the precise time and angle

---

<sup>14</sup> Hodor Decl., *supra* note 6, at 9.

<sup>15</sup> Blaze testimony, *supra* note 12, at 9; Thomas Farely & Ken Schmidt, Cellular Telephone Basics: Basic Theory and Operation (2006), [http://www.privateline.com/mt\\_cellbasics/iv\\_basic\\_theory\\_and\\_operation/](http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/).

<sup>16</sup> Blaze testimony, *supra* note 12, at 13-14.

<sup>17</sup> See, e.g., Testimony of FBI agent William B. Shute, *United States v. Sims*, No. 06-674 (E.D. Pa. Nov. 13, 2007), available at <http://www.eff.org/files/filenode/celltracking/shutetestimony.pdf> (hereinafter, “Shute testimony”); Br. for American Civil Liberties Union, the ACLU of Connecticut, and the Electronic Frontier Foundation as *Amici Curiae* Supporting Motion to Suppress, *United States v. Soto*, No. 3:09-cr-200 (AWT), (D. Conn. June 18, 2010), available at <http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf>; Recent Development, *Who Knows Where You’ve Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J.L. & Tech. 307, 311 (2004) (describing how state used cell site location information in the Scott Peterson murder as evidence of the defendant’s movements, including his presence at home).

<sup>18</sup> Shute testimony, *supra* note 17.

<sup>19</sup> *Id.* at 16-18.

<sup>20</sup> *Id.* at 24.

<sup>21</sup> *Id.* at 23.

<sup>22</sup> See *id.* at 19-20, 21.

at which the cell phone's signal arrives at multiple cell towers.<sup>23</sup> Current technology can pinpoint the location of the cell phone to an accuracy of within 50 meters or less anytime the cell phone is on, and the accuracy will improve with newer technology.<sup>24</sup> The availability of the information and the length of time during which this information is stored depend on the policies of the cell phone carrier, but some carriers appear to be already recording and storing "frequently updated, highly precise, location information not just when calls are made or received, but about every device as it moves about the networks."<sup>25</sup> It is expected that, as technology progresses, more carriers will store more detailed records of individuals' locations for a longer period of time.<sup>26</sup>

### III. GPS DATA

For cell phones that have special GPS satellite receiver hardware built into them, the cell phone can determine its precise location by receiving signals from global position satellites.<sup>27</sup> An increasing number of phones, particularly smartphones, contain such GPS chips; market research shows that North American subscriptions to services using GPS-enabled cell phones will surpass 20 million by 2011.<sup>28</sup>

How often the cell phone reports location information using the GPS to the network depends on the application software that the phone is running.<sup>29</sup> Current GPS technology is able to pinpoint location with accuracy when it is outdoors, typically achieving accuracy of within 10 meters.<sup>30</sup> With "assisted GPS" technology which combines GPS and triangulation, it is possible to obtain such accurate location information even when the cell phone is inside a home or a building.<sup>31</sup>

### ARGUMENT

Prosecutors in various jurisdictions have been seeking to prospectively track people's cell phone location information on less than a showing of probable cause. Specifically, they have argued that they have the authority to obtain such data under the combination of two parts of the ECPA—the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq.*, and the Pen Registers and Trap and Trace Devices Statute ("Pen/Trap Statute"), 18 U.S.C. § 3121 *et seq.*—

---

<sup>23</sup> Blaze testimony, *supra* note 12, at 10.

<sup>24</sup> *Id.*

<sup>25</sup> *Id.* at 11.

<sup>26</sup> *Id.*

<sup>27</sup> *Id.* at 5.

<sup>28</sup> CTIA The Wireless Association, 100 Wireless Facts, <http://www.ctia.org/advocacy/research/index.cfm/AID/10384> (last visited Aug. 4, 2010); *see also* ABI Research, GPS-enabled Handsets Expected to Bypass the Economic Downturn (Jan. 20, 2009), <http://www.abiresearch.com/press/1351-GPS-enabled+Handsets+Expected+to+Bypass+the+Economic+Downturn>.

<sup>29</sup> Blaze testimony, *supra* note 12, at 5-6.

<sup>30</sup> *Id.*

<sup>31</sup> *The Privacy Implications of Commercial Location-Based Services: Testimony Before the Subcomm. on Commerce, Trade, & Consumer Protection and Subcomm. on Communications, Technology, and the Internet of the H. Comm. on Energy & Commerce*, 111th Cong. (2010) (statement of John B. Morris, Jr., General Counsel, and Director of Internet Standards, Technology & Policy Project, Center for Democracy & Technology, at 4), [http://energycommerce.house.gov/Press\\_111/20100224/Morris.Testimony.2010.02.24.pdf](http://energycommerce.house.gov/Press_111/20100224/Morris.Testimony.2010.02.24.pdf); James Connell, *Can Galileo Locate the Money?*, International Herald Tribune, May 23, 2006.

upon merely offering “specific and articulable facts” establishing reasonable grounds that the information would be “relevant and material to an ongoing criminal investigation.” § 2703(d).<sup>32</sup> They appear to make this argument routinely to obtain prospective cell site location information; in addition, prosecutors in some jurisdictions have applied for triangulation and GPS data without showing probable cause, contravening even the Department of Justice’s recommendation that a warrant be obtained for such information.<sup>33</sup>

The government’s argument should be rejected for two reasons. First, the government’s statutory argument ignores the language and the structure of ECPA and, if adopted, would render the statute constitutionally suspect under the Fourth Amendment. For this reason, the government’s position has only been adopted in a few outlier opinions. The “strong majority” of district and magistrate judges have concluded in recently published opinions that the government lacks statutory authority to engage in prospective cell phone tracking on less than a showing of probable cause. *In re Applications of the U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d)*, 509 F. Supp. 2d 76, 78, n.4 (D. Mass. 2007) (Stearns) (listing cases). Second, a contrary conclusion would permit the government to monitor individuals’ location and movement in violation of their reasonable expectations of privacy, without the procedural protections of the Fourth Amendment.

## **I. THE GOVERNMENT HAS NO AUTHORITY UNDER THE ELECTRONIC COMMUNICATIONS PRIVACY ACT TO ENGAGE IN WARRANTLESS PROSPECTIVE CELL PHONE TRACKING.**

The government has based its authority to access prospective cell phone location information on the “hybrid” authority of two statutory sections within ECPA, the Pen/Trap Statute and the SCA. This argument fails: the Pen/Trap Statute does not authorize location tracking, the SCA regulates only retrospective surveillance, and there is no evidence that Congress intended the combination of the two to permit what neither statute authorizes on its own. ECPA should be interpreted to require a warrant when tracking cell phones, in accordance with its natural language and structure, and in order to avoid serious constitutional doubt.<sup>34</sup>

---

<sup>32</sup> This and subsequent citations to statutes are to Title 18 unless otherwise noted.

<sup>33</sup> Since at least 2007, the DOJ has recommended that U.S. Attorneys around the country obtain a warrant prior to engaging in precise forms of cell phone tracking. *See Email from Brian M. Klebba, Assistant U.S. Attorney* (Nov. 17, 2007, 10:37 AM), [http://www.aclu.org/pdfs/freespeech/cellfoia\\_dojrecommendation.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_dojrecommendation.pdf). Some U.S. Attorneys’ offices, however, have applied for precise forms of cell phone tracking under a lesser standard than a warrant. *See, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005) (rejecting application for triangulation data on less than a showing of probable cause); Letter from Executive Office for U.S. Attorneys to ACLU (Dec. 31, 2008), available at [http://www.aclu.org/pdfs/freespeech/cellfoia\\_released\\_074135\\_12312008.pdf](http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf) (stating, in a letter received as a result of a Freedom of Information Act lawsuit filed by the ACLU and EFF against the United States Attorneys Office for the Southern District of Florida, that six applications to “obtain GPS or similarly precise location data” were granted after November 16, 2007, without a judicial determination of probable cause).

<sup>34</sup> Some courts have compared cell phones to tracking devices, and thus have analyzed whether cell phones are a “tracking device” under § 3117(b). Section 3117(b) is irrelevant to the analysis because regardless of whether cell phones are tracking devices under that section, ECPA, as amended by the Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1001, does not permit prospective cell phone tracking without a warrant for the reasons explained in this brief. Similarly, regardless of § 3117(b), the SCA protects historical cell site information from disclosure as a “record . . . pertaining to a subscriber” under its plain language. This argument is explained in

## **A. The Government Cannot Obtain Cell Phone Location Data Through the Pen/Trap Statute.**

As the government appears to have conceded in its cell phone tracking applications, cell phone location information cannot be obtained under an order pursuant to the Pen/Trap Statute.<sup>35</sup> The Communications Assistance for Law Enforcement Act (“CALEA”), 47 U.S.C. § 1001 *et seq.*, passed in 1994, plainly forbids the use of the Pen/Trap Statute to collect location information. It states that “with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices . . . 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). Legislative history confirms the intent of Congress to mandate that “the authority for pen registers and trap and trace devices cannot be used to obtain tracking or location information, other than that which can be determined from the phone number.” H.R. Rep. No. 103-827, at 19 (1994). A pen/trap order is thus plainly insufficient to obtain cell phone location information.

## **B. The Government Cannot Obtain Prospective Cell Phone Location Data Through the SCA, Which Governs Only Retrospective Access to Existing Information.**

The government has argued that because cell phone location information is a “record or other information pertaining to a subscriber to or customer of” an electronic communication service, § 2703(c)(1), it is permitted to obtain the information pursuant to an order issued under § 2703(d) on a showing of “specific and articulable facts . . . that there are reasonable grounds to believe that the . . . records or other information sought, are relevant and material to an ongoing criminal investigation.” § 2703(d). Although the government is correct that the SCA plainly protects cell phone location data, it only does so for historical and stored information; the SCA cannot be used to conduct *prospective* surveillance on individuals’ location information.

By its plain language, the SCA only regulates retrospective access to information. The SCA applies to “stored” communications, *see* S. Rep. No. 99-541, at 3 (1986), and it regulates “divulg[ing]” or “disclos[ing]” a “record or other information,” § 2702(a)(3), (c). Although the phrase “record or other information” is not defined, a “record” in this context means “something stored or archived.” *D. Mass. 2007 (Stearns)*, 509 F. Supp. 2d at 80. The plain language of a section that authorizes “disclos[ure]” of a “record or other information” in the present tense permits only the disclosure of a record or information that exists at the time that the government

---

more detail in other filed briefs. *See, e.g.*, Br. of *Amici Curiae*, In Re Application of the U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t at 2-3, *supra*, note 1; Br. of *Amici Curiae* the Electronic Frontier Foundation, the American Civil Liberties Union, the ACLU-Foundation of Penn., Inc., and the Center for Democracy and Technology in Opposition to the Government’s Request for Review at 4-13, *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc’n Serv. to Disclose Records to the Gov’t*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), available at <http://www.eff.org/files/filenode/celltracking/LenihanAmicus.pdf>.

<sup>35</sup> The Pen/Trap Statute permits the installation and use of a “pen register”—a “device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted,” § 3127(3)—where the government certifies that “the information likely to be obtained . . . is relevant to an ongoing investigation,” § 3123(a)(1).

is seeking it. If it does not exist, there is nothing to disclose. *See In re Application for Pen Register & Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 760 (S.D. Tex. 2005) (Smith) (“Like a request for production of documents under Federal Rule of Civil Procedure 34, § 2703(d) contemplates the production of existing records, not documents that may be created at some future date related to some future communication.”).

This reading is consistent with how even the government has interpreted another provision of the same section of the SCA, § 2703(f). This provision requires providers, at the request of the government, to “take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.” § 2703(f)(1). In its own manual, the Justice Department has stressed that this section cannot be used to compel providers to keep records that have yet to be created. *See Computer Crime & Intellectual Prop. Section, U.S. Dep’t of Justice, Searching & Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, Chapter 3 (3d ed. 2009), available at <http://www.cybercrime.gov/ssmanual/03ssma.html> (instructing against using § 2703(f) prospectively). If “records and other evidence” in § 2703(f)(1) is interpreted as encompassing only *existing* records, it would be inconsistent to construe “record or other information” in § 2703(c)(1) as including records that do not yet exist.

The structural differences between the SCA and other statutes like the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Pen/Trap Statute that authorize prospective surveillance also make it evident that Congress intended the SCA to apply only to already-existing information. *See In re Application of the U.S. for Orders Authorizing the Installation & Use of Pen Registers & Caller Identification Devices on Tel. Nos. [Sealed] and [Sealed]*, 416 F. Supp. 2d 390, 395 n.7 (D. Md. 2006) (Bredar); *In re Application of the U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info.*, No. 06-MISC-004, 2006 WL 2871743, at \*6 (E.D. Wis. Oct. 6, 2006) (Adelman); *S.D. Tex. 2005 (Smith)*, 396 F. Supp. 2d at 760. First, the Wiretap Act and the Pen/Trap Statute contain provisions regulating ongoing surveillance. For example, both statutes require the communications service provider to supply technical assistance to law enforcement in acquiring information. *See, e.g.*, § 2518(4); § 3124(a), (b). Both statutes also set forth procedural safeguards: they mandate maximum surveillance periods, *see, e.g.*, § 2518(5) (30 days for wiretapping); § 3123(c)(1) (60 days for pen/trap devices), and the Wiretap Act gives courts authority to order periodic reports from law enforcement concerning the progress of its surveillance, § 2518(6). By contrast, the SCA does not contain any language regarding ongoing surveillance. It is difficult to imagine that Congress, which in enacting CALEA expressed more concern about the privacy of cell phone location information than that of other information obtainable by a pen register, *see* 47 U.S.C. § 1002(a)(2), nonetheless permitted the government to continuously monitor location information without the procedural protections governing pen/trap orders.

Second, both the Wiretap Act and the Pen/Trap Statute mandate the automatic sealing of court records and the imposition of a gag order against the communications provider of the existence of the surveillance order. *See, e.g.*, § 2518(8)(b); § 3123(d). The automatic sealing and nondisclosure order are necessary in every case of prospective surveillance because announcing the initiation of surveillance will undoubtedly undermine the investigation. Yet, the SCA does not provide for either mechanism, instead giving the court the option to issue a gag

order if the disclosure of the § 2703(d) order would result in certain enumerated adverse consequences. § 2705(b)(1)-(5).

Consistent with the foregoing reasoning, most commentators and even the government, in its manual on electronic surveillance, agree that the SCA regulates only retrospective access to information. *See, e.g.*, U.S. Internet Service Provider Ass'n, *Electronic Evidence Compliance—A Guide for Internet Service Providers*, 18 Berkeley Tech. L.J. 945, 949 (2003); Deirdre Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 Geo. Wash. L. Rev. 1557, 1565 (2004); Computer Crime & Intellectual Prop. Section, *supra*, at Chapter 3 (“If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4,” the Wiretap Act and the Pen/Trap Statute). The government therefore cannot rely on the SCA to obtain prospective cell phone location information.

### C. The “Hybrid” Authority of the Pen/Trap Statute and the SCA Does Not Authorize What Neither Statute Does On Its Own.

Perhaps recognizing the weakness of its argument that the SCA authorizes prospective surveillance, the government has argued in recent applications that it is not the SCA alone but the “hybrid” authority of the Pen/Trap Statute and the SCA that permits location tracking on less than a showing of probable cause. Although this is a creative solution to the government’s dilemma—the government purports to remedy the SCA’s lack of any of the procedural protections invariably found in prospective surveillance statutes by borrowing those of the Pen/Trap Statute—nothing in the statutes contemplates such cutting and pasting of different statutory provisions to create new surveillance authority. “Congress . . . does not alter the fundamental details of a regulatory scheme in vague terms or ancillary provisions—it does not, one might say, hide elephants in mouseholes.” *Whitman v. Am. Trucking Ass’ns., Inc.*, 531 U.S. 457, 468 (2001).

Congress, which enacted the Pen/Trap Statute and the SCA at the same time and then comprehensively revised surveillance law through CALEA, has had opportunities to make clear its intent to allow “hybrid” authority. It has not done so. To the contrary, the SCA specifically enumerates five ways in which the government can compel the disclosure of a “record or other information”: a Rule 41 warrant, a § 2703(d) order, the consent of the subscriber or customer, a formal request relevant to a law enforcement investigation concerning telemarketing fraud, or a subpoena for limited types of information like name and address. *See* § 2703(c). The Pen/Trap Statute, or the Pen/Trap Statute in combination with a § 2703(d) order, is not one of them. When Congress enumerates an exclusive list, the court should assume, under the maxim of *expressio unius est exclusio alterius*, that it meant to exclude what it did not enumerate. *See Tenn. Valley Auth. v. Hill*, 437 U.S. 153, 188 (1978).

Even if the government’s hybrid theory were not otherwise awkward and implausible, the principle of constitutional avoidance requires the court to presume that Congress did not intend to enact a statutory scheme that raises constitutional doubt. *See Clark v. Martinez*, 543 U.S. 371, 380-81 (2005) (“[W]hen deciding which of two plausible statutory constructions to adopt, a court must consider the necessary consequences of its choice. If one of them would raise a multitude

of constitutional problems, the other should prevail . . .”).<sup>36</sup> The government has conceded that its hybrid theory would allow access to any type of prospective cell phone location information—not only the increasingly precise cell site location information but also the already precise triangulation and GPS data—under the relevance and materiality standard of § 2703(d). See *D. Md. 2006 (Bredar)*, 416 F. Supp. 2d at 396; *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 218 (W.D.N.Y. 2006) (Feldman). As we establish in more detail below, this type of surveillance runs headlong into the Fourth Amendment warrant requirement. See *S.D. Tex. 2005 (Smith)*, 396 F. Supp. 2d at 765 (“[P]ermitting surreptitious conversion of a cell phone into a tracking device without probable cause raises serious Fourth Amendment concerns, especially when the phone is monitored in the home or other places where privacy is reasonably expected.”).

The few court opinions in the minority that have accepted the government’s “hybrid” theory have failed to consider, or failed to appreciate, the gravity of the constitutional questions that would be raised by that theory. For example, one judge dismissed the possibility of the government conducting accurate cell phone location tracking using the hybrid theory as “hypothetical,” *In re Application of the U.S. for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d 202, 209 (E.D.N.Y. 2008) (Garaufis), but the government has already requested and received accurate GPS and triangulation data on less than a showing of probable cause. See *supra*, note 31. Moreover, these opinions noted that the government only sought limited cell site data in the applications before it, without appreciating that once access to limited cell site location information is permitted under the hybrid theory, there is nothing to stop the government from requesting other types of more intrusive and accurate cell phone location information—including triangulation and GPS location information which is already available, and the more accurate cell site location information of the future—under the same theory. See, e.g., *E.D.N.Y. 2008 (Garaufis)*, 632 F. Supp. 2d at 208; *In re the Application of the U.S. for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber and Other Info.*, 622 F. Supp. 2d 411, 417-19 (S.D. Tex. 2007) (Rosenthal); *In re Application of the U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel.*, 460 F. Supp. 2d 448, 461 (S.D.N.Y. 2006) (Kaplan).

The use of these new types of technology raises a multitude of unresolved issues about the constitutional limits of permissible mass surveillance. See *United States v. Knotts*, 460 U.S. 276, 283-84 (1983) (reserving for another day the constitutionality of “dragnet type law enforcement practices”); *Smith v. Maryland*, 442 U.S. 735, 740 n.5 (1979) (noting that further normative inquiry would be required if “the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry”). But this Court need not reach the larger question of the limits of mass surveillance; as a “strong majority” of judges have held, the plain language of the CALEA, Pen/Trap Statute, and the SCA compel

---

<sup>36</sup> As even a court that has accepted the government’s theory has acknowledged, “[i]t is clear that the hybrid theory is not the only way that the Pen Register Statute and the SCA may be construed.” *In re U.S. for an Order Authorizing the Use of Two Pen Register & Trap & Trace Devices*, 632 F. Supp. 2d 202, 208 (E.D.N.Y. 2008) (Garaufis); see also *In re the Application of the U.S. for an Order Authorizing the Installation & Use of a Pen Register*, 415 F. Supp. 2d 211, 214, 219 (W.D.N.Y. 2006) (Feldman) (noting that “the government’s concerns over the ‘ambiguity of the statutes’ are well founded,” and rejecting the hybrid theory in part because “it simply is not found in the plain language of any of the three statutes upon which the government relies”).

the conclusion that the government lacks statutory authority to conduct prospective cell phone tracking based on its hybrid theory. *D. Mass. 2007 (Stearns)*, 509 F. Supp. 2d at 78, n.4 (listing cases).

**D. Federal Rule of Criminal Procedure 41 Is the Appropriate Vehicle for Obtaining Cell Phone Location Information.**

CALEA provides that location information cannot be disclosed “solely pursuant” to the Pen/Trap Statute. Because it also cannot be disclosed pursuant to the SCA or the hybrid authority of the Pen/Trap Statute and the SCA, Federal Rules of Criminal Procedure Rule 41 is the appropriate vehicle for obtaining this information. Rule 41 grants magistrate judges the general authority to issue a warrant to search for a person or property, Fed. R. Crim. P. 41(b), and has been considered sufficiently broad to authorize electronic surveillance, *see, e.g., United States v. Torres*, 751 F.2d 875, 877-80 (7th Cir. 1984) (permitting video surveillance under Rule 41), including cell phone tracking, *see, e.g., In re the Application of the U.S. for an Order Authorizing Monitoring of Geolocation & Cell Site Data for a Sprint Spectrum Cell Phone No.*, No. 06-0186, 187, 188, 2006 WL 6217584, at \*4 (D.D.C. Aug. 25, 2006) (Hogan) (granting a Rule 41 warrant for cell site location information on the showing of probable cause, and citing other courts that have concluded that such information would be available under Rule 41). This reading of the statutes eliminates the awkwardness of trying to find authority for prospective surveillance in the SCA, while satisfying the government’s concerns of maintaining surveillance capacity.

Consistent with Congress’s statutory scheme, then, courts should require law enforcement to obtain a warrant based on probable cause under Rule 41 before engaging in cell phone tracking. As explained in further detail below, this Rule 41 warrant must also meet the constitutional requirements of particularity for electronic surveillance: certification by a judge that normal investigative procedures have failed or reasonably appear to be unlikely to succeed or be too dangerous; a particular description of information sought and relationship to the particular offense; a period of surveillance that is no longer than is necessary, and in any event no longer than thirty days; and minimization. *Cf., e.g., Torres*, 751 F.2d at 883-86 (holding that a Rule 41 warrant for video surveillance must meet particularity requirements codified in Title I of the ECPA for “electronic surveillance that picks up more information than is strictly necessary”).

**II. THE FOURTH AMENDMENT REQUIRES THAT THE GOVERNMENT OBTAIN A WARRANT BASED ON PROBABLE CAUSE AND PARTICULAR DESCRIPTION TO ENGAGE IN CELL PHONE TRACKING.**

It is not only ECPA, but also the Fourth Amendment that requires that the government obtain a warrant based on probable cause and particular description prior to engaging in cell phone tracking. This is because cell phone location tracking is a “search” under the Fourth Amendment that infringes on the reasonable expectation of privacy that Americans have traditionally enjoyed in their whereabouts. The fact that 90% of Americans now have cell phones that track this information does not justify warrantless government access to this private

information. Rather, it highlights the massive threat to Americans' privacy if such information is not protected against government invasion.<sup>37</sup>

#### **A. Individuals Have a Reasonable Expectation of Privacy in Their Location and Movement Information.**

Cell phone location information is protected by the Fourth Amendment because individuals have a reasonable expectation of privacy in their location and movement information, which can reveal intimate details of their lives—their presence in protected locations like their home or office, their doctors' visits, shopping habits, attendance at church, or association with others.

Over a quarter of a century ago, the Supreme Court in *United States v. Karo*, 468 U.S. 705 (1984), held that location tracking implicates Fourth Amendment privacy interests because it may reveal information about individuals in areas where they have reasonable expectations of privacy. In *Karo*, the police placed a primitive tracking device known as a beeper inside a can of ether and used it to infer that the ether remained in a particular private residence. In considering the Fourth Amendment challenge to the use of the beeper, the Court held that using an electronic device to infer facts about the inside of a protected place like a home was just as unreasonable as searching it without a warrant. *Id.* at 714-15; see also *Kyllo v. United States*, 533 U.S. 27, 36 (2001) (explaining and relying on the role of inference in *Karo* when holding that unwarranted thermal imaging of the home violates the Fourth Amendment). The Court reasoned:

The beeper tells the agent that a particular article is actually located at a particular time in the private residence and is in the possession of the person or persons whose residence is being watched. Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises.

*Karo*, 468 U.S. at 715.

*Karo* compels the conclusion that cell phone tracking implicates Fourth Amendment interests because, at minimum, just as the beepers of the *Karo* era, it reveals information about whether the cell phone is inside a protected location and whether it remains there. The most obvious example of such a protected place in which warrantless cell phone tracking violates constitutional protections is in the home: an area in which “there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*.” *Kyllo*, 533 U.S. at 34 (emphasis in original). In the home, “*all* details are intimate details,” regardless of quality or quantity. *Id.* at 37 (emphasis in original). The cell phone travels through many such protected locations during the day where, under *Karo*, the government cannot warrantlessly intrude on individuals’ reasonable expectations of privacy. See, e.g., *See v. City of Seattle*, 387 U.S. 541, 543 (1967) (business premises); *Stoner v. California*, 376 U.S. 483, 486 (1964) (hotel room).

---

<sup>37</sup> These same constitutional arguments require the government to obtain a warrant before accessing stored historical cell phone location information.

Moreover, the individual's privacy interest in his location information is not limited to the home or other protected locations: "what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected." *Katz v. United States*, 389 U.S. 347, 351 (1967). It is not only the cell phone's location in each constitutionally protected space, but the sum of the information gathered from the sweeping surveillance of a person's movement that "reveals an intimate picture of the subject's life that he expects no one to have—short perhaps of his spouse," and thus supports an expectation of privacy that society recognizes as reasonable. *United States v. Maynard*, No. 08-3030, 2010 WL 3063788, at \*14 (D.C. Cir. Aug. 6, 2010) (holding that continuous GPS surveillance of an individual's movements without a warrant violates his reasonable expectation of privacy); *In re Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585, 586 n.6 (W.D. Pa. 2008) (Lenihan) (stating that historical cell-site location information is likely to reveal "precisely the kind of information that an individual wants and reasonably expects to be private"), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *appeal docketed*, No. 08-4227.

Government monitoring of cell phone location and movement information—often for as long as 60 days—implicates privacy concerns of a greater magnitude than the beepers of a quarter of a century ago. Cf. *United States v. Knotts*, 460 U.S. 276, 284-85 (1983) (permitting "limited use" of beeper without a warrant to aid the police in following a five-gallon drum of chloroform during a single trip as it was moved in a car between two locations). First, as the Supreme Court has recognized, electronic surveillance that continuously and indiscriminately captures details of one's life "involves an intrusion on privacy that is broad in scope." *Berger v. New York*, 388 U.S. 41, 56-58 (1967). Individuals have the reasonable expectation of being free from such continuous and indiscriminate surveillance, even in areas potentially visible to the public. See *Maynard*, 2010 WL 3063788, at \* 13 ("The whole of one's movements over the course of a month is not constructively exposed to the public because . . . that whole reveals far more than the individual movements it comprises."); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251 (5th Cir. 1987) (holding the indiscriminate video surveillance of an individual's backyard requires a warrant even if the police could have seen the backyard via a "one-time overhead flight or a glance over the fence by a passer-by"). As the highest courts of several states and the District of Columbia Circuit have acknowledged, location monitoring that is now possible, and which by its nature is continuous and indiscriminate, represents a far greater invasion of privacy than beepers that were monitored for as little as a day for the discrete purpose of ascertaining the destination of a particular object. See, e.g., *Maynard*, 2010 WL 3063788, at \*7-16; *People v. Weaver*, 909 N.E. 2d 1195, 1198-99 (N.Y. 2009) (holding that the warrantless use of a GPS device, which, unlike the beepers of the past, "facilitates a new technological perception of the world in which the situation of any object may be followed and exhaustively recorded over . . . a practically unlimited period," violated state constitution); *State v. Jackson*, 76 P.3d 217, 223 (Wash. 2003) (holding that the state constitution required a warrant for the two and one-half week, 24 hour surveillance of a GPS tracking device because "the intrusion into private affairs . . . is quite extensive"); *State v. Campbell*, 759 P.2d 1040, 1048 (Or. 1988) (holding that use of radio transmitter to locate defendant's vehicle was a search under the state constitution, and stating that "[a]ny device that enables the police quickly to locate a person

or object anywhere within a 40-mile radius, day or night, over a period of several days, is a significant limitation on freedom from scrutiny").<sup>38</sup>

Second, the technological progress heralded by cell phone tracking means that this form of tracking must be treated more restrictively than the beepers of the past because the technology is no longer tied to what can be ascertained through "naked-eye surveillance." *Kyllo*, 533 U.S. at 33, 35 n.2 (holding that a warrant is required to use thermal imaging technology, which involves more than "naked-eye surveillance," even if "equivalent information could be . . . obtained by other means," for example by observing snowmelt on the roof); cf. *Knotts*, 460 U.S. at 285 (holding that the use of the beeper did not violate the Fourth Amendment where it did not reveal information that could not be obtained by visual surveillance); *Maynard*, 2010 WL 3063788, at \*15-16 (rejecting comparison of GPS monitoring to visual surveillance); *Weaver*, 909 N.E. 2d at 1200 ("The science at issue in *Knotts* was . . . quite modest, amounting to no more than an incremental improvement over following a car by the unassisted eye."); *Jackson*, 76 P.3d at 223 ("[T]he GPS device does not merely augment the officers' senses, but rather provides a technological substitute for traditional visual tracking"). Accessibility of cell phone location information at low cost permits the government to engage in surveillance of the magnitude that would not have been possible through visual surveillance.

In fact, recent uses of cell phone tracking by the government illustrate that "dragnet type law enforcement practices" that the Court has warned of is quickly becoming reality. See *Knotts*, 460 U.S. at 283-84 (reserving for another day the constitutionality of such practices). For example, the government commonly appears to obtain location information not only about the target of the investigation but about the "community of interest," i.e., all persons with whom the target communicated.<sup>39</sup> The government also engages in "cell site dump" searches, in which it obtains records of all cellular phones using the cell tower closest to the scene of the crime.<sup>40</sup> These practices threaten privacy, chill associational activities, and open the door to abuse if not checked by proper Fourth Amendment standards.<sup>41</sup> See *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007) (permitting warrantless GPS tracking when the police have a suspect in their sights, but stating that "[t]echnological progress poses a threat to privacy by enabling an extent of surveillance that in earlier times would have been prohibitively expensive" and reserving decision on constitutionality of programs of mass surveillance); *W.D. Pa. 2008 (Lenihan)*, 534 F.

---

<sup>38</sup> Although other courts have held that use of a GPS tracking device is not a search under *Knotts*, see *United States v. Marquez*, 605 F.3d 604 (8th Cir. 2010); *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Cir. 2010); *United States v. Garcia*, 474 F.3d 994 (7th Cir. 2007), these cases did not address the inapplicability of *Knotts* to long-term surveillance and left open the question whether mass surveillance requires a warrant. See *Maynard*, 2010 WL 3063788, at \*9.

<sup>39</sup> See, e.g., Br. for American Civil Liberties Union, the ACLU of Connecticut, and the Electronic Frontier Foundation as Amici Curiae Supporting Motion to Suppress, *United States v. Soto*, No. 3:09-cr-200(AWT) (D. Conn. June 18, 2010) (citing the defendant's memorandum stating that the government obtained location data of 180 individuals who made or received calls to the target number), available at <http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf>; *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties of the H. Comm. on Judiciary*, 111th Cong. (2010) (statement of Albert Gidari, Partner, Perkins Coie LLP, at 5-6), available at <http://judiciary.house.gov/hearings/pdf/Gidari100505.pdf>.

<sup>40</sup> See, e.g., *United States v. Duffey*, No. 3:08-CR-0167-B, 2009 WL 2356156, at \*1 (N.D. Tex. June 30, 2009).

<sup>41</sup> A recent *Newsweek* article reported some abuses that have already occurred. For example, some Michigan police officers, "purportedly concerned about a possible 'riot,' pressed [a] telecom for information on all the cell phones that were congregating in an area where a labor-union protest was expected." Michael Isikoff, *The Snitch in Your Pocket*, *NEWSWEEK*, Feb. 19, 2010.

Supp. 2d at 612 (“newly-emergent technologies create a potential to monitor associational activities in a manner that could have a chilling effect”).

The existing cases in which courts have denied motions to suppress cell site and other cell phone location information compare cell phone tracking to beepers without appreciating the greater Fourth Amendment interests at stake with the advent of this technology. Some of the cases also dismiss the cell phone tracking technology used as too inaccurate to trigger Fourth Amendment scrutiny. But even the least precise form of cell phone tracking like cell site location information is no less sophisticated than beepers. *Cf. United States v. Berry*, 300 F. Supp. 2d 366, 368 (D. Md. 2004) (“[A] beeper is unsophisticated, and merely emits an electronic signal that the police can monitor with a receiver. The police can determine whether they are gaining on a suspect because the strength of the signal increases as the distance between the beeper and the receiver closes.”). Indeed, the government has taken the position that cell site location information is accurate enough to present as evidence of an individual’s location during criminal trials. *See supra*, Factual Background I.

In any event, the appropriate constitutional rule must be articulated with regard to “more sophisticated [technologies] that are already in use or in development.” *Kyllo*, 533 U.S. at 36. Currently available technology like GPS and triangulation, as well as cell site location technology of the future, yields location data that is far more accurate than current cell site data. *See supra* Factual Background I-III. It may be that the current cell site technology “is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure.” *Silverman v. United States*, 365 U.S. 505, 512 (1961) (internal quotation marks omitted).

The Fourth Amendment protects an individual’s reasonable expectations of privacy in information that he “seeks to preserve as private.” *Katz*, 389 U.S. at 351. It cannot be correct that that Amendment has nothing to say about whether government, enabled by technology, may subject Americans to round-the-clock surveillance of their movements for as long as it likes.

#### **B. That the Cell Phone Provider, a Third Party, Has Access to Cell Phone Location Information Does Not Undermine the Cell Phone Users’ Reasonable Expectations of Privacy in Their Location and Movement Information.**

The fact that cell phone providers collect cell phone location information does not vitiate the privacy rights of the 90% of Americans who use a cell phone. Cases applying the so-called “third-party doctrine,” which holds that a person loses her expectation of privacy in information when she voluntarily communicates it to a third-party, *see Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *United States v. Miller*, 425 U.S. 435 (1976), were decided on the notion, inapplicable here, that by knowingly and voluntarily disclosing this information, a person assumes the risk that the third-party will reveal the information to others. *See Smith*, 442 U.S. at 743-44.

Unlike those third-party doctrine cases, cell phone users do not knowingly and voluntarily take the risk of having their location information revealed to the public. For

example, unlike the phone numbers dialed by the telephone user in *Smith*, cell phone location information is not information that the user directly conveys to an operator orally or dials on his phone in order to connect the call. That information is generated and recorded automatically by the interaction of cell phones and the cell towers or GPS satellites in a manner unrelated to the individual's use of the phone.<sup>42</sup> That cell phone location information is generated without the individual's knowledge means that he has not voluntarily and knowingly communicated this information to the public. *See W.D. Pa. 2008 (Lenihan)*, 534 F. Supp. 2d at 615 (“[Cell site data] is not ‘voluntarily and knowingly’ conveyed (certainly *not* in the way of transactional bank records or dialed numbers); rather, the information is automatically registered by the cell phone”); *S.D. Tex. 2005 (Smith)*, 396 F. Supp. 2d at 756-57 (“[Unlike dialed numbers, cell site data] is transmitted automatically during the registration process, entirely independent of the user’s input, control, or knowledge.”).

In addition, unlike the phone numbers in *Smith*, this information typically does not appear in a cell phone user's bill, thus providing users with no subjective awareness that the information is being generated and recorded. *Cf. Smith*, 442 U.S. at 742 (“All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.”).

Finally, in the world where massive quantity of personal information is stored or processed by businesses, the third-party doctrine must have its limits. The Supreme Court has recognized as much. The Court has concluded, for example, that individuals have a reasonable expectation of privacy in the content of their telephone calls, *see Katz*, 389 U.S. at 352-53, even though “[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment.” *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

Like the contents of a communication, cell site location information is personally revealing and people reasonably expect privacy in their movements. *See supra* Part II.A. In its continuous and indiscriminate nature, cell phone tracking raises Fourth Amendment concerns similar to the surveillance of the content of conversations. *Cf. Berger*, 388 U.S. at 56-58. The third-party doctrine does not extend to such intimate information, particularly when an individual has done little to voluntarily convey the information to a third party.

### **C. Because Cell Phone Tracking Is a Search, Law Enforcement Must Obtain a Warrant Based on Probable Cause and Particular Description to Engage in Cell Phone Tracking.**

Because cell phone tracking implicates an expectation of privacy that society is prepared to recognize as reasonable, the government must obtain a warrant based on probable cause prior to collecting this information. Furthermore, because cell phone tracking involves surveillance that is continuous and indiscriminate, the constitutional requirement of particularity applies: (1) certification by a judge that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous,” (2) “a particular

---

<sup>42</sup> *See W.D. Pa. 2008 (Lenihan)*, 534 F. Supp. 2d at 589-90 (cell site information is generated automatically every seven seconds, regardless of the use of the phone); Blaze testimony, *supra* note 12, at 5-6 (the frequency with which GPS technology communicates location information depends on the application that is running).

description of the type of [information] sought . . . and a statement of the particular offense to which it relates,” (3) a period of surveillance that is no “longer than is necessary to achieve the objective of the authorization, nor in any event longer than thirty days (though renewals are possible),” and (4) requirement that the surveillance “be conducted in such a way as to minimize the [collection of information] not otherwise subject to surveillance.” *Torres*, 751 F.2d at 883-84 (internal quotation marks omitted) (adopting the four requirements for video surveillance).

“Each of these four requirements is a safeguard against electronic surveillance that picks up more information than is strictly necessary and so violates the Fourth Amendment’s requirement of particular description.” *Id.* at 884. They were first articulated by the Court in *Berger* in the context of eavesdropping, *Berger*, 388 U.S. at 55-60, have been codified in Title I of the ECPA governing wiretapping, *see* § 2518, and have been adopted by courts evaluating the constitutionality of video surveillance, *see, e.g.*, *Torres*, 751 F.2d at 885.<sup>43</sup> Because cell phone tracking is just as continuous and indiscriminate as eavesdropping, wiretapping, and video surveillance, a warrant for this type of surveillance must also meet the four particularization requirements in Title I, *see* § 2518(3)(c), § 2518(4)(c), § 2518(5).

The “relevance and materiality” standard under § 2703(d) which the government has relied on to engage in cell phone tracking falls far short of the requisite warrant based on the constitutional requirements of probable cause and particularization. Demanding that the government obtain a warrant will have “the salutary effect” of protecting against abuse and preventing violations of Fourth Amendment rights. *Karo*, 468 U.S. at 717.

## CONCLUSION

For the above statutory and constitutional reasons, if the government wishes to engage in cell phone tracking, it must obtain a warrant under Rule 41 that meets probable cause and particularization requirements. The unacceptable alternative to requiring a warrant to engage in cell phone tracking is to permit the government to continuously and indiscriminately monitor the locations and movements of any cell phone user on simply a showing of relevance and materiality to an ongoing investigation. The government should not be allowed to engage in such intrusive collection of personal information on such a minimal standard.

---

<sup>43</sup> See also, e.g., *United States v. Falls*, 34 F.3d 674, 680 (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992) (en banc); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1437-38 (10th Cir. 1990); *Cuevas-Sanchez*, 821 F.2d at 252; *United States v. Biasucci*, 786 F.2d 504, 510 (2d Cir. 1986).