Third Circuit.

In the Matter of the APPLICATION OF the UNITED STATES of America FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMUNICATION SERVICE TO DISCLOSE RECORDS TO the GOVERNMENT.

Sept. 7, 2010.

SLOVITER, Circuit Judge.

The United States ("Government") applied for a court order pursuant to a provision of the Stored Communications Act, 18 U.S.C. § 2703(d), to compel an unnamed cell phone provider to produce a customer's "historical cellular tower data," also known as cell site location information or "CSLI." App. at 64. The Magistrate Judge ("MJ") denied the application. The Government appeals.[FN1]

FN1. Because the Government's application was *ex parte,* there was no adverse party to review or oppose it. However, we received amici briefs in support of affirmance of the District Court from a group led by the Electronic Frontier Foundation and joined by the American Civil Liberties Union, the ACLU–Foundation of Pennsylvania, Inc., and the Center for Democracy and Technology (hereafter jointly referred to as "EFF") and from Susan A. Freiwald, a law professor who teaches and writes in the area of cyberspace law and privacy law. Representatives on behalf of EFF and Professor Freiwald participated in the proceedings below and at the oral argument before us. We are grateful to the amici for their interest in the issue and their participation in this matter.

I.

The growth of electronic communications has stimulated Congress to enact statutes that provide both access to information heretofore unavailable for law enforcement purposes and, at the same time, protect users of such communication services from intrusion that Congress deems unwarranted. The Stored Communications Act ("SCA"), enacted in 1986, is directed to disclosure of communication information by providers of electronic communications ("providers"). Section 2703(a) covers the circumstances in which a governmental entity may require providers to disclose the *contents* of wire or electronic communications in electronic storage; section 2703(b) covers the circumstances in which a governmental entity may require providers to disclose the *contents* of wire or electronic communications held by a remote computing service. *See* 18 U.S.C. § 2703(a)-(b). Neither of those sections is at issue here. The Government does not here seek disclosure of the contents of wire or electronic communications. Instead, the Government seeks what is referred to in the statute as "a record or other information pertaining to a subscriber to or customer of such service," a term that expressly excludes the contents of communications. *Id.* 2703(c)(1).

Section 2703(c)(1) of the SCA provides:

(c) Records concerning electronic communication service or remote computing service.—(1) 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) only when the governmental entity—

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

Id. The formal separation of these options in § 2703(c)(1) evinces Congressional intent to separate the requirements for their application. Each option in § 2703(c)(1) is an independently authorized procedure. The only options relevant to the matter before us are § 2703(c)(1)(A) for obtaining a warrant and § 2703(c)(1)(B) for obtaining a court order under § 2703(d).

A third option covered by the statute provides for the governmental entity to use "an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena...." *Id.* § 2703(c)(2). The subpoena option covers more limited information—such as a customer's name, address, and certain technical information [FN3]—as distinguished from that referred to in § 2703(c)(1) which broadly covers "a record or other information pertaining to a subscriber or customer." The Government may seek such information under any of these three options *ex parte,* and no notice is required to a subscriber or customer. *See id.* § 2703(c)(3).

FN3. Subsection (2) of § 2703(c) provides:

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the—

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service....

18 U.S.C. § 2703(c)(2).

In submitting its request to the MJ in this case, the Government did not obtain either a warrant under § 2703(c)(1)(A), or a subpoena under § 2703(c)(2), nor did it secure the consent of the subscriber under §

2703(c)(1)(C). Instead it sought a court order as authorized by § 2703(c)(1)(B). The requirements for a court order are set forth in § 2703(d) as follows:

> (d) Requirements for court order.—A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity *offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.* In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

Id. § 2703(d) (emphasis added).

As the Government notes in its reply brief, there is no dispute that historical CSLI is a "record or other information pertaining to a subscriber ... or customer," and therefore falls within the scope of § 2703(c)(1). Instead, the dispute in this case concerns the standard for a § 2703(d) order. The Government states that the records at issue, which are kept by providers in the regular course of their business, include CSLI, i.e., the location of the antenna tower and, where applicable, which of the tower's "faces" carried a given call at its beginning and end and, inter alia, the time and date of a call.

The Government's application, which is heavily redacted in the Appendix, seeks

> historical cellular tower data i.e. transactional records (including, without limitation, call initiation and termination to include sectors when available, call handoffs, call durations, registrations and connection records), to include cellular tower site information, maintained with respect to the cellular telephone number [of a subscriber or subscribers whose names are redacted].

II. [FN6]

FN6. We acknowledge that numerous magistrate judges and district courts in other jurisdictions have addressed various issues regarding whether the Government can obtain prospective CSLI through the authorization found in § 2703(d) alone or in combination with the pen register and trap and trace statutes (the "hybrid" theory), and/or whether the Government can obtain historical CSLI through a § 2703(d) order. *See, e.g., MJOp.,* 534 F.Supp.2d at 599–600 (discussing "hybrid" theory and citing cases). Some of those cases hold that the government cannot obtain prospective, i.e., realtime, CSLI through the "hybrid" theory. *See, e.g., In re Application of the United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device; (2) Authorizing the Release of Subscriber & Other Info.; & (3) Authorizing the Disclosure of Location–Based Servs.,* Nos. 1:06–MC–6,–7, 2006 WL 1876847, at *1 (N.D.Ind. July 5, 2006); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.,* 396 F.Supp.2d 747, 765 (S.D.Tex.2005); *In re Application of the United States for an Order (1) Authorizing the Use of a Pen Register & a Trap & Trace Device & (2) Authorizing Release of Subscriber Info. & /or Cell Site Info.,* 396 F.Supp.2d 294, 327 (E.D.N.Y.2005). Others cases hold that the Government may obtain prospective cell site location information through the "hybrid" theory. *See, e.g., In re Application of the United States 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); *In re Application of the United States for an Order for Disclosure of Telecomm. Records & Authorizing the Use of a Pen Register & Trap & Trace,* 405 F.Supp.2d 435, 449 (S.D.N.Y.2005). Most relevant here, at least two cases expressly hold that historical CSLI can be obtained through a § 2703(d) order. *See In re Application of the*

United States for an Order: (1) Authorizing the Installation & Use of a Pen Register & Trap & Trace Device, & (2) Authorizing Release of Subscriber & Other Info., 622 F.Supp.2d 411, 418 (S.D.Tex.2007); *In re Applications of the United States for Orders Pursuant to Title 18, U.S.C. § 2703(d),* 509 F.Supp.2d 76, 82 (D.Mass.2007). Additionally, judges in at least two cases, *In re Applications,* 509 F.Supp.2d at 81 n. 11, and *In re Application of the United States for an Order for Disclosure of Telecommunications Records & Authorizing the Use of a Pen Register & Trap & Trace,* 405 F.Supp.2d 435, 449 (S.D.N.Y.2005), have specifically held that cell phones are not tracking devices under 18 U.S.C. § 3117. In contrast, Judge McMahon of the Southern District of New York held that CSLI is information from a tracking device under § 3117 and is therefore excluded from § 2703(c). *See In re Application of the United States for an Order Authorizing the Use of a Pen Register with Caller Identification Device Cell Site Location Auth. on a Cellular Tel.,* 2009 WL 159187, at *6–7 (S.D.N.Y. Jan.13, 2009).

The MJ held that even if the CSLI here is included within the scope of § 2703(c)(1), the Government must show probable cause because a cell phone acts like a tracking device. The MJ's holding that probable cause was the correct standard appeared to be influenced by her belief that CSLI, and cell phone location information generally, make a cell phone act like a tracking device in that the CSLI discloses movement/location information. *See MJOp.,* 534 F.Supp.2d at 609 ("In the case of movement/location information derived from an electronic device, the traditionally-applied legal standard has been a showing of probable cause; and nothing in the text, structure, purpose or legislative history of the SCA dictates a departure from that background standard as to either historic or prospective CSLI.").

In response, the Government notes that the historical CSLI that it sought in this case does not provide information about the location of the caller closer than several hundred feet. However, much more precise location information is available when global positioning system ("GPS") technology is installed in a cell phone. A GPS is a widely used device installed in automobiles to provide drivers with information about their whereabouts. The Government argues that it did not seek GPS information in this case.

We take no position whether a request for GPS data is appropriate under a § 2703(d) order. However, a § 2703(d) order requiring production of CSLI or GPS data could elicit location information. For example, historical CSLI could provide information tending to show that the cell phone user is generally at home from 7 p.m. until 7 a.m. the next morning (because the user regularly made telephone calls from that number during that time period). With that information, the Government may argue in a future case that a jury can infer that the cell phone user was at home at the time and date in question.

Amicus EFF points to the testimony of FBI Agent William B. Shute during a trial in the Eastern District of Pennsylvania in which he analyzed cell location records—seemingly the records of the towers used during calls—and concluded that it was "highly possible that [a cell phone user] was at her home," EFF App. at 20, and at another time that the user was "in the vicinity of her home," *id.* at 21. Later, Agent Shute testified that the cell phone records revealed a genuine probability that the individual was in another person's home. *Id.* at 25. Agent Shute also testified that at one point the phone was in an "overlap area" of less than eight blocks. *Id.* at 27–28. Moreover, Agent Shute said that he could track the direction that the individual was traveling based on when the individual switched from one tower to another. *Id.* at 21–22. According to Agent Shute, he has given similar testimony in the past. In other words, the Government has asserted in other cases that a jury should rely on the accuracy of the cell tower records to infer that an individual, or at least her cell phone, was at home.

The Government counters that Agent Shute acknowledged that historical cell site information provides only a rough indication of a user's location at the time a call was made or received. The Government correctly notes that Agent Shute did not state that the cell-site information "is reliable evidence" that the suspect was at home, as EFF asserts. EFF Br. at 15. Agent Shute only stated that it is "highly possible" that the user was at home or in the vicinity.

This dispute may seem to be a digression, but it is not irrelevant. The MJ proceeded from the premise

that CSLI can track a cell phone user to his or her location, leading the MJ to conclude that CSLI could encroach upon what the MJ believed were citizens' reasonable expectations of privacy regarding their physical movements and locations. The MJ regarded location information as "extraordinarily personal and potentially sensitive." *MJOp.,* 534 F.Supp.2d at 586. We see no need to decide that issue in this case without a factual record on which to ground the analysis. Instead, we merely consider whether there was any basis for the MJ's underlying premises.

For that purpose, we refer to two opinions of the Supreme Court, both involving criminal cases not directly applicable here, but which shed some light on the parameters of privacy expectations. In *United States v. Knotts,* 460 U.S. 276, 103 S.Ct. 1081, 75 L.Ed.2d 55 (1983), the Supreme Court held that the warrantless installation of an electronic tracking beeper/radio transmitter inside a drum of chemicals sold to illegal drug manufacturers, and used to follow their movements on public highways, implicated no Fourth Amendment concerns, as the drug manufacturers had no reasonable expectation of privacy while they and their vehicles were in plain view on public highways. The following year, in *United States v. Karo,* 468 U.S. 705, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), the Court held that where a beeper placed inside a chemical drum was then used to ascertain the drum's presence within a residence, the search was unreasonable absent a warrant supported by probable cause. More specifically, the Court stated that the "case ... present[ed] the question whether the monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence." *Id.* at 714, 104 S.Ct. 3296. The *Karo* Court distinguished *Knotts:*

> [M]onitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant. The case is thus not like *Knotts,* for there the beeper told the authorities nothing about the interior of Knotts' cabin .... here, as we have said, the monitoring indicated that the beeper was inside the house, a fact that could not have been visually verified.

Id. at 715, 104 S.Ct. 3296.

We cannot reject the hypothesis that CSLI may, under certain circumstances, be used to approximate the past location of a person. If it can be used to allow the inference of present, or even future, location, in this respect CSLI may resemble a tracking device which provides information as to the actual whereabouts of the subject. The *Knotts/ Karo* opinions make clear that the privacy interests at issue are confined to the interior of the home. There is no evidence in this record that historical CSLI, even when focused on cell phones that are equipped with GPS, extends to that realm. We therefore cannot accept the MJ's conclusion that CSLI by definition should be considered information from a tracking device that, for that reason, requires probable cause for its production.

In sum, we hold that CSLI from cell phone calls is obtainable under a § 2703(d) order and that such an order does not require the traditional probable cause determination. The MJ erred in allowing her impressions of the general expectation of privacy of citizens to transform that standard into anything else.

IV.

Because we conclude that the SCA does not contain any language that requires the Government to show probable cause as a predicate for a court order under § 2703(d) and because we are satisfied that the legislative history does not compel such a result, we are unable to affirm the MJ's order on the basis set forth in the MJ's decision. The Government argues that if it presents a magistrate court with "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal

investigation," 18 U.S.C. § 2703(d), the magistrate judge *must* provide the order and cannot demand an additional showing. The EFF disagrees, and argues that the requirements of § 2703(d) merely provide a floor—the minimum showing required of the Government to obtain the information—and that magistrate judges do have discretion to require warrants.

We begin with the text. Section § 2703(d) states that a "court order for disclosure under subsection (b) or (c) *may be* issued by any court that is a court of competent jurisdiction and *shall* issue *only if* " the intermediate standard is met. 18 U.S.C. § 2703(d) (emphasis added). We focus first on the language that an order "may be issued" if the appropriate standard is met. This is the language of permission, rather than mandate. If Congress wished that courts "shall," rather than "may," issue § 2703(d) orders whenever the intermediate standard is met, Congress could easily have said so. At the very least, the use of "may issue" strongly implies court discretion, an implication bolstered by the subsequent use of the phrase "only if" in the same sentence.

The Government argues that when the statutory scheme is read as a whole, it supports a finding that a magistrate judge does not have "arbitrary" discretion to require a warrant. We agree that a magistrate judge does not have arbitrary discretion. Indeed, no judge in the federal courts has arbitrary discretion to issue an order. Orders of a magistrate judge must be supported by reasons that are consistent with the standard applicable under the statute at issue. Nonetheless, we are concerned with the breadth of the Government's interpretation of the statute that could give the Government the virtually unreviewable authority to demand a § 2703(d) order on nothing more than its assertion. Nothing in the legislative history suggests that this was a result Congress contemplated.[FN8]

> FN8. We are puzzled by the Government's position. If, as it suggests, the Government needs the CSLI as part of its investigation into a large scale narcotics operation, it is unlikely that it would be unable to secure a warrant by disclosing additional supporting facts. In our experience, magistrate judges have not been overly demanding in providing warrants as long as the Government is not intruding beyond constitutional boundaries.

Because the MJ declined to issue a § 2703(d) order on legal grounds without developing a factual record, she never performed the analysis whether the Government's affidavit even met the standard set forth in § 2703(d). The Government's position would preclude magistrate judges from inquiring into the types of information that would actually be disclosed by a cell phone provider in response to the Government's request, or from making a judgment about the possibility that such disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home.

The Government argues that no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider. For support, the Government cites *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), in which the Supreme Court found that an individual's bank records were not protected by the Constitution because "all of the records [which are required to be kept pursuant to the Bank Secrecy Act,] pertain to transactions to which the bank was itself a party," *id.* at 441, 96 S.Ct. 1619 (internal quotation and citation omitted), and "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," *id.* at 442, 96 S.Ct. 1619.

The Government also cites *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979), in which the Supreme Court held that citizens have no reasonable expectation of privacy in dialed phone numbers because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *id.* at 744, 99 S.Ct. 2577, and a phone call "voluntarily convey[s] numerical information to the telephone company and 'expose[s]' that information to its equipment in the ordinary course of business," *id.* at 744, 99 S.Ct. 2577. The Court reasoned that individuals "assume[ ] the risk that the company w[ill] reveal to police the numbers ... dialed ... [and the] switching equipment that processed those

numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber." *Id.*

A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell phone user receives a call, he hasn't voluntarily exposed anything at all." EFF Br. at 21.

Because the statute as presently written gives the MJ the option to require a warrant showing probable cause, we are unwilling to remove that option although it is an option to be used sparingly because Congress also included the option of a § 2703(d) order. However, should the MJ conclude that a warrant is required rather than a § 2703(d) order, on remand it is imperative that the MJ make fact findings and give a full explanation that balances the Government's need (not merely desire) for the information with the privacy interests of cell phone users.

V.

For the reasons set forth, we will vacate the MJ's order denying the Government's application, and remand for further proceedings consistent with this opinion.

TASHIMA, Circuit Judge, concurring:

I concur in the result and in most of the reasoning of the majority opinion. I write separately, however, because I find the majority's interpretation of the discretion granted to a magistrate judge by 18 U.S.C. § 2703(d) troubling.

Granting a court unlimited discretion to deny an application for a court order, even after the government has met statutory requirements, is contrary to the spirit of the statute. *Cf. Huddleston v. United States,* 485 U.S. 681, 688, 108 S.Ct. 1496, 99 L.Ed.2d 771 (1988) (noting, in interpreting Federal Rule of Evidence 404(b), that the word "may" does not vest with the trial judge arbitrary discretion over the admissibility of evidence); The Federalist No. 78, p. 529 (J. Cooke ed. 1961) (" 'To avoid an arbitrary discretion in the courts, it is indispensable that they should be bound down by strict rules and precedents, which serve to define and point out their duty in every particular case that comes before them.' ").

As the majority notes, "a magistrate judge does not have arbitrary discretion. Indeed, no judge in the federal courts has arbitrary discretion to issue an order." Maj. Op. at 316. I respectfully suggest, however, that the majority's interpretation of the statute, because it provides *no* standards for the approval or disapproval of an application for an order under § 2703(d), does just that—vests magistrate judges with arbitrary and uncabined discretion to grant or deny issuance of § 2703(d) orders at the whim of the magistrate, [FN9] even when the conditions of the statute are met.

> FN9. Unless the admonition that the magistrate's naked power should "be used sparingly," Maj. Op. at 319, is accepted as a meaningful and objectively enforceable guideline.

I would cabin the magistrate's discretion by holding that the magistrate may refuse to issue the § 2703(d) order here only if she finds that the government failed to present specific and articulable facts sufficient to meet the standard under § 2703(d) or, alternatively, finds that the order would violate the Fourth Amendment absent a showing of probable cause because it allows police access to information which reveals a cell phone user's location within the interior or curtilage of his home.[FN10] *See Kyllo v. United States,* 533 U.S. 27, 35–36, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001); *United States v. Pineda–Moreno,* 2010 WL 3169573 (9th Cir.2010) (Kozinski, C.J., dissenting from denial of rehearing en

banc).

> FN10. Alternatively, the magistrate may condition her order by requiring minimization to exclude those portions which disclose location information protected by the Fourth Amendment, *i.e.,* within the home and its curtilage.

With this caveat as to the magistrate's duty and the scope of her discretion on remand, I concur in the majority opinion and in the judgment.