PRECEDENTIAL

UNITED STATES COURT OF APPEALS FOR THE THIRD CIRCUIT

No. 08-4227

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

United States of America,
Appellant

On Appeal from the United States District Court
for the Western District of Pennsylvania
(D.C. No. 2-07-mj-00524-001)
District Judge: Honorable Terrence F. McVerry

Argued February 12, 2010

Before: SLOVITER, ROTH, and TASHIMA,[*] Circuit Judges

(Filed: September 7, 2010)

Mary Beth Buchanan
Robert L. Eberhardt
Office of the United States Attorney
Pittsburgh, PA 15219

---

[*] Honorable A. Wallace Tashima, Senior Judge of the United States Court of Appeals for the Ninth Circuit, sitting by designation.

Mark Eckenwiler (Argued)
United States Department of Justice
Office of Enforcement Operations
Washington, DC 20530

Attorneys for Appellant

Lisa B. Freeland
Office of Federal Public Defender
Pittsburgh, PA 15222

Jennifer Granick
Kevin S. Bankston (Argued)
Matthew Zimmerman
Electronic Frontier Foundation
San Francisco, CA 94110

Jim Dempsey
Harley Geiger
Center for Democracy and Technology
Washington, DC 20006

Witold J. Walczak
American Civil Liberties Union of Pennsylvania
Pittsburgh, PA 15213

Catherine Crump
American Civil Liberties Union Foundation
New York, NY 10004

Susan A. Freiwald (Argued)
University of San Francisco School of Law
San Francisco, CA 94117

Attorneys for Amici Appellees

OPINION OF THE COURT

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. *See In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 534 F. Supp. 2d 585, 616 (W.D. Pa. 2008) (hereafter "*MJOp.*"). In doing so, the MJ wrote an extensive opinion that rejected the Government's analysis of the statutory language, the legislative history, and the Government's rationale for its request. On the Government's appeal to the District Court, the Court recognized "the important and complex matters presented in this case," but affirmed in a two page order without analysis. *In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, No. 07-524M, 2008 WL 4191511, at *1 (W.D. Pa. Sept. 10, 2008). The Government appeals.

We have de novo review. *See DIRECTV Inc. v. Seijas*, 508 F.3d 123, 125 (3d Cir. 2007). This appeal gives us our first opportunity to review whether a court can deny a Government application under 18 U.S.C. § 2703(d) after the Government has satisfied its burden of proof under that provision, a task that to our knowledge has not been performed by any other court of appeals.[1]

---

[1] 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

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"), was enacted in 1986 as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. §§ 2701-2711 (2010)), which amended the Omnibus Crime Control and Safe Streets Act of 1968 (the "Wiretap Act"), Pub. L. No. 90-351, 82 Stat. 197 (1968).[2] In 1994, Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"), Pub. L. No. 103-414, 108 Stat. 4279, 4292 (1994) (codified in relevant part at 18 U.S.C. § 2703 (2010)), in part to amend the SCA.

The SCA 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

---

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.

[2] Title II of the ECPA was formally entitled "Stored Wire and Electronic Communications and Transactional Records Access." Pub. L. No. 99-508, 100 Stat. 1848 (1986).

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[3] –

---

[3] 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 . . . .

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).

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).

---

18 U.S.C. § 2703(c)(2).

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].

App. at 64. The Government does not foreclose the possibility that in a future case it will argue that the SCA may be read to authorize disclosure of additional material.

II.

The MJ concluded, "as a matter of statutory interpretation, that nothing in the provisions of the electronic communications legislation authorizes it [i.e., the MJ] to order a [provider's] covert disclosure of CSLI absent a showing of probable cause under Rule 41." *MJOp.*, 534 F. Supp. 2d at 610. Rule 41(d) of the Federal Rules of Criminal Procedure, referred to by the MJ, provides:

> **(d) Obtaining a Warrant.**

> **(1) In General.** After receiving an affidavit or other information, a magistrate judge--or if authorized by Rule 41(b), a judge of a state court of record--must issue the warrant if there is *probable cause* to search for and seize a person or property or to install and use a tracking device.

Fed. R. Crim. P. 41(d) (emphasis added).

The Government argues that 18 U.S.C. § 2703(d) on its face requires only that it make a showing of "specific and articulable facts establishing reasonable grounds" that the information sought is "relevant and material to an ongoing criminal investigation." It argues that it made such a showing in this case by the statement in its application that the requested cell phone records are relevant and material to an ongoing investigation into large-scale narcotics trafficking and various related violent crimes, that nothing more is required, and that the MJ erred in holding that something more, in particular probable cause, is required before issuing the requested order. Thus, the counterpoised standards are "probable cause," the standard for a Rule 41 warrant, and the "relevant and material" language in 18 U.S.C. § 2703(d).

We begin with the MJ's opinion. We note, preliminarily, that the MJ's opinion was joined by the other magistrate judges in that district. This is unique in the author's experience of more than three decades on this court and demonstrates the impressive level of support Magistrate Judge Lenihan's opinion has among her colleagues who, after all, routinely issue warrants authorizing searches and production of documents.

One of the principal bases for the MJ's conclusion that the Government must show probable cause for a § 2703(d) order was her explanation that probable cause is the standard which the Government has long been required to meet in order to obtain court approval for the installation and use by law enforcement agents of a device enabling the Government to record, or "track," movement of a person or thing. *See MJOp.*, 534 F. Supp. 2d at 613-14. The MJ also held that a cell phone is

a "tracking device" under 18 U.S.C. § 3117, and that the Government cannot obtain information from a "tracking device" under § 2703(d). *See id.* at 601-02. A statute, incorporated by reference in § 2711(1) of the SCA, defines a "tracking device" as "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. § 3117(b).[4]

Section 2703(c) applies only to "provider[s] of electronic communication service[s]." 18 U.S.C. § 2703(c)(1). An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).[5] The

---

[4] We note that the Senate Report on the ECPA, which encompasses the SCA, defines "electronic tracking devices" as follows:

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

S. Rep. No. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564.

[5] "'[W]ire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce . . . ." 18 U.S.C. § 2510(1).

definition of "electronic communication" found in § 2510(12) excludes the communications from a "tracking device." *See id.* § 2510(12) ("'[E]lectronic communication' . . . does not include . . . any communication from a tracking device . . . ."). The MJ held that CSLI that allows the Government to follow where a subscriber was over a period of time is information from a tracking device deriving from an electronic communications service, and that therefore the Government cannot obtain that information through a § 2703(d) order. *See MJOp.*, 534 F. Supp. 2d at 589, 601. If CSLI could be characterized as information from a tracking device, and a tracking device is not covered by the SCA, this would be a relatively straightforward case because the Government, when seeking judicial permission to install or use a tracking device, must ordinarily obtain a warrant. *See* Fed. R. Crim. P. 41.

The Government vigorously objects to treating CSLI from cell phone calls as information from a tracking device. It

---

"'[E]lectronic 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, but does not include --

> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds . . . ."

Id. § 2510(12).

explains that cellular calls are wire communications, that tracking devices are excluded from the definition of electronic communications but not from the definition of wire communications, and that, in any event, it hasn't sought records from a tracking device in this case.

Section 2510(1) defines "wire communication" as "any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) . . . ." 18 U.S.C. § 2510(1). The CSLI requested by the Government consists of records of information collected by cell towers when a subscriber makes a cellular phone call. That historical record is derived from a "wire communication" and does not itself comprise a separate "electronic communication." Thus, even if the record of a cell phone call does indicate generally where a cell phone was used when a call was made, so that the resulting CSLI was information from a tracking device, that is irrelevant here because the CSLI derives from a "wire communication" and not an "electronic communication." *See id.* § 2703(c) (providing that the Government may require "a provider of electronic communication service" to disclose records); *id.* § 2510(15) (defining "electronic communication service" to include providers of "wire *or* electronic communications") (emphasis added).[6]

---

[6] 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)*

As with other issues under the SCA, the issue of the

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).

standard by which the Government may obtain CSLI is not easily avoided. 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.

Nonetheless, the Government does not argue that it cannot or will not request information from a GPS device through a § 2703(d) order. In fact, a publication of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice contains a "Sample 18 U.S.C. § 2703(d) Application and Order" seeking "[a]ll records and other information relating to the account(s) and [the relevant] time period" including "telephone records, . . . caller identification records, cellular site and sector information, *GPS data*," and other information. U.S. Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations*, 222 (3d ed. 2009) (emphasis added), *available at*

http://www.cybercrime.gov/ssmanual/ssmanual2009.pdf (last visited Aug. 3, 2010).

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 (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 (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." *Karo*, 468 U.S. at 714. 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.

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. Instead, the standard is governed by the text of § 2703(d), i.e., "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 MJ erred in allowing her impressions of the general expectation of privacy of citizens to transform that standard into anything else. We also conclude that this standard is a lesser one than probable cause, a conclusion that, as discussed below, is supported by the legislative history.

III.

On different occasions in the MJ's opinion, the MJ referred to her understanding that the "relevant legislative history indicates that Congress did not intend its electronic communications legislation to be read to require, on its authority, disclosure of an individual's location information . . . ." *MJOp.*, 534 F. Supp. 2d at 610. We also have reviewed the legislative history of the SCA and find no support for this conclusion.

The legislative history of the ECPA begins in 1985 with the introduction by Representative Kastenmeier of H.R. 3378. *See* 131 Cong. Rec. 24,397 (1985) (statement of Rep. Robert W. Kastenmeier). At the hearings on H.R. 3378, Senator Leahy explained that "the bill provides that law enforcement agencies must obtain a court order based on a reasonable suspicion standard before . . . being permitted access to records of an electronic communication system which concern specific communications." *Electronic Communications Privacy Act: Hearings on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 7 (1985) (statement of Sen. Patrick Leahy). H.R. 3378 was not enacted.

The statute that was enacted the following year, the ECPA, was designed "to protect against the unauthorized interception of electronic communications. The bill amends the 1968 law [the Wiretap Act,] to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986). The Senate Report states that Title II of the ECPA, the SCA, "addresses access to stored wire and electronic communications and transactional records. It is modeled after [legislation that] protects privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." *Id.* at 3; *see also* 132 Cong. Rec. 27,633 (1986) (statement of Sen. Leahy that the ECPA "provides standards by which law enforcement agencies may obtain access to . . . the records of an electronic communications system."). During House consideration and

passage of the ECPA, Representative Moorhead explained that "the legislation establishes clear rules for Government access to new forms of electronic communications as well as the transactional records regarding such communications [and] . . . removes cumbersome procedures from current law that will facilitate the interests of Federal law enforcement officials." 132 Cong. Rec. 14,887 (1986) (statement of Rep. Carlos J. Moorhead).

Eight years later, in 1994, Congress amended the statute to keep pace with technological changes through CALEA, which altered the standard in 18 U.S.C. § 2703 to its current state. Pub. L. No. 103-414, 108 Stat. 4922 (1994). In Senate Report No. 103-402, which accompanied the CALEA legislation, it noted that the bill "also expands privacy and security protection for telephone and computer communications. The protections of the [ECPA] are extended to cordless phones and certain data communications transmitted by radio." S. Rep. No. 103-402, at 10 (1994).

The legislative history strongly supports the conclusion that the present standard in § 2703(d) is an "intermediate" one. For example, Senate Report No. 103-402 states that § 2703(d)

> imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable-cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

Id. at 31; *see also* H.R. Rep. No. 103-827, pt. 1, at 31 (1994) (noting same), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511. We are aware of no conflicting legislative history on the matter, and

we will accept the intermediate standard as applicable to all attempts to obtain transaction records under § 2703(d).

In its interpretation of the standard to be applied to § 2703(d) orders, the MJ referred to the testimony of then-FBI Director Louis Freeh supporting the passage of CALEA. *See MJOp.*, 534 F. Supp. 2d at 596-97 (citing *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Technology and the Law of the S. Comm. on the Judiciary and the Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103d Cong. 2, 22-23, 27-29 (1994) (statement of Louis J. Freeh, Director, Federal Bureau of Investigation) ("Freeh Testimony")). The MJ described Director Freeh's testimony as follows:

> Freeh addressed Congress' concern that with advances in cell phone technology, law enforcement could obtain-by CSLI-information of an individual's physical movement previously obtainable only through visual surveillance or the covert installation of a radio-wave transmitter. During the course of his testimony, Director Freeh reassured Congress that law enforcement was not attempting to obtain via the 1994 enactments, or to otherwise alter the standards applicable to, movement/location information.

Id. at 596.

Director Freeh's testimony, referred to by the MJ, does not provide support for the MJ's conclusion that a warrant is required to obtain CSLI. Director Freeh's testimony regarding allegations of "tracking" persons focused on the Government's ability to obtain information through a pen register or trap and trace device, which is governed by a different, and lower, standard than that applicable to a § 2703(d) order. *See* Freeh Testimony at 33. To obtain information from pen register and trap and trace devices, the Government need only certify "that the information likely to be obtained by such installation and use

is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1). In contrast, § 2703(d) requires "specific and articulable facts," "reasonable grounds to believe," and "material[ity]" to an ongoing criminal investigation, a higher standard. *Id.* § 2703(d). Thus, the protections that Congress adopted for CSLI in 47 U.S.C. § 1002(a)(2)[7] have no apparent relevance to § 2703(d), and the legislative history does not show that Congress intended to exclude CSLI or other location information from § 2703(d). Although the language of § 2703(d) creates a higher standard than that required by the pen register and trap and trace statutes, the legislative history provides ample support for the proposition that the standard is an intermediate one that is less stringent than probable cause.

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

---

[7] *See* 47 U.S.C. § 1002(a)(2)(B) ("with regard to information acquired solely pursuant to the authority for pen registers and trap and trace devices" a telecommunications carrier need not allow the government access to "call-identifying information . . . that may disclose the physical location of the subscriber (except to the extent that the location may be determined from the telephone number) . . . .").

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 EFF argues that the statutory language that an order can be issued "only if" the showing of articulable facts is made indicates that such a showing is necessary, but not automatically sufficient. EFF Br. at 4. If issuance of the order were not discretionary, the EFF asserts, the word "only" would be superfluous. *Id.* at 5. The EFF compares the use of the words "only if" with the clearly mandatory language of the pen register statute, 18 U.S.C. § 3123(a)(1), which states that a court "shall" enter an ex parte order "if" the court finds that information relevant to an ongoing criminal investigation would be found. In other words, the difference between "shall . . . if" (for a pen register) and "shall . . . only if" (for an order under § 2703(d)) is dispositive.

We addressed the effect of the statutory language "only . . . if" in the Anti-Head Tax Act, which provides that a "State or political subdivision of a State *may* levy or collect a tax on or related to a flight of a commercial aircraft or an activity or service on the aircraft *only if* the aircraft takes off or lands in the State or political subdivision as part of the flight." 49 U.S.C. § 40116(c) (emphasis added). In *Township of Tinicum v. United States Department of Transportation*, 582 F.3d 482 (3d Cir. 2009), we stated that the "phrase 'only if' describe[d] a necessary condition, not a sufficient condition," *id.* at 488 (citing

California v. Hodari D., 499 U.S. 621, 627-28 (1991) (explaining that "only if" describes "a *necessary,* but not a *sufficient*, condition")), and that while a "necessary condition describes a prerequisite[,]" *id.*, a "sufficient condition is a guarantee[,]" *id*. at 489. Adopting the example of the baseball playoffs and World Series, we noted that while "a team may win the World Series *only if* it makes the playoffs . . . a team's meeting the necessary condition of making the playoffs does not guarantee that the team will win the World Series." *Id.* at 488. In contrast, "winning the division is a sufficient condition for making the playoffs because a team that wins the division is ensured a spot in the playoffs . . . [and thus] a team makes the playoffs *if* it wins its division." *Id.* at 489. The EFF's argument, essentially, is that our analysis of the words "only if" in § 2703(d) should mirror that in *Tinicum*.

This is a powerful argument to which the Government does not persuasively respond. Under the EFF's reading of the statutory language, § 2703(c) creates a "sliding scale" by which a magistrate judge can, at his or her discretion, require the Government to obtain a warrant or an order. EFF Br. at 6. As the EFF argues, if magistrate judges were required to provide orders under § 2703(d), then the Government would never be required to make the higher showing required to obtain a warrant under § 2703(c)(1)(A). *See id.*

The Government's only retort to the argument that it would never need to get a warrant under § 2703(c)(1)(A) if it could always get CSLI pursuant to an order under § 2703(d) is that the warrant reference in § 2703(c)(1)(A) is "alive and well" because a prosecutor can "at his or her option . . . employ a single form of compulsory process (a warrant), rather than issuing a warrant for content and a separate subpoena or court order for the associated non-content records." Appellant's Reply Br. at 14. In other words, the Government asserts that obtaining a warrant to get CSLI is a purely discretionary decision to be made by it, and one that it would make only if a warrant were, in the Government's view, constitutionally required. We believe it trivializes the statutory options to read the § 2703(c)(1)(A) option as included so that the Government may proceed on one

paper rather than two.

In response to the EFF's statutory argument, the Government argues that the "shall issue" language is the language of mandate. It also asserts that without the word "only", the sentence would read that an order "may be issued by [a] court . . . and shall issue if the government" makes the correct showing. Appellant's Reply Br. at 12. The difficulty with the Government's argument is that the statute does contain the word "only" and neither we nor the Government is free to rewrite it.

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.[8]

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

---

[8] 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.

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 (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 (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.

The Government also cites *Smith v. Maryland*, 442 U.S. 735 (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, 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. 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.

The EFF has called to our attention an FCC order requiring cell phone carriers to have, by 2012, the ability to locate phones within 100 meters of 67% of calls and 300 meters for 95% of calls for "network based" calls, and to be able to locate phones within 50 meters of 67% of calls and 150 meters of 95% of calls for "hand-set" based calls. EFF Br. at 12 n.5 (citing 47 C.F.R. § 20.18(h)(1)(2008)). The record does not demonstrate whether this can be accomplished with present technology, and we cannot predict the capabilities of future technology. *See Kyllo v. United States*, 533 U.S. 27, 36 (2001) ("While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in use or in development."); *see also id.* ("the novel proposition that inference insulates a search is blatantly contrary to [*Karo*], where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home.").

Although CSLI differs from information received from a beeper, which the Supreme Court held in *Karo* required a warrant before disclosure of information from a private home, the remarks of the Supreme Court in *Karo* are useful to contemplate, particularly in connection with the Government's extreme position. The Supreme Court stated:

> We cannot accept the Government's contention that it should be completely free from the constraints of the Fourth Amendment to determine by means of an electronic device, without a warrant and without probable cause or reasonable suspicion, whether a particular article-or a person, for that matter-is in an individual's home at a particular time. Indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy

> interests in the home to escape entirely some sort of Fourth Amendment oversight.

Karo, 468 U.S. at 716.

The Government is also not free from the warrant requirement merely because it is investigating criminal activity. A similar argument was rejected in *Karo* where the Court stated:

> We also reject the Government's contention that it should be able to monitor beepers in private residences without a warrant if there is the requisite justification in the facts for believing that a crime is being or will be committed and that monitoring the beeper wherever it goes is likely to produce evidence of criminal activity. Warrantless searches are presumptively unreasonable, though the Court has recognized a few limited exceptions to this general rule. *See, e.g.*, *United States v. Ross*, 456 U.S. 798, 102 S. Ct. 2157, 72 L. Ed. 2d 572 (1982) (automobiles); *Schneckloth v. Bustamonte*, 412 U.S. 218, 93 S. Ct. 2041, 36 L. Ed. 2d 854 (1973) (consent); *Warden v. Hayden*, 387 U.S. 294, 87 S. Ct. 1642, 18 L. Ed. 2d 782 (1967) (exigent circumstances). The Government's contention that warrantless beeper searches should be deemed reasonable is based upon its deprecation of the benefits and exaggeration of the difficulties associated with procurement of a warrant. The Government argues that the traditional justifications for the warrant requirement are inapplicable in beeper cases, but to a large extent that argument is based upon the contention, rejected above, that the beeper constitutes only a minuscule intrusion on protected privacy interests. The primary reason for the warrant requirement is to interpose a "neutral and detached magistrate" between the citizen and "the officer engaged in the often competitive enterprise of ferreting out crime." *Johnson v. United States*,

> 333 U.S. 10, 14, 68 S. Ct. 367, 369, 92 L. Ed. 436 (1948). Those suspected of drug offenses are no less entitled to that protection than those suspected of nondrug offenses. Requiring a warrant will have the salutary effect of ensuring that use of beepers is not abused, by imposing upon agents the requirement that they demonstrate in advance their justification for the desired search.

Id. at 717.

Similar reasoning lay behind the MJ's refusal to grant a § 2703(d) order. In the issue before us, which is whether the MJ may require a warrant with its underlying probable cause standard before issuing a § 2703(d) order, we are stymied by the failure of Congress to make its intention clear. A review of the statutory language suggests that the Government can proceed to obtain records pertaining to a subscriber by several routes, one being a warrant with its underlying requirement of probable cause, and the second being an order under § 2703(d). There is an inherent contradiction in the statute or at least an underlying omission. A warrant requires probable cause, but there is no such explicit requirement for securing a § 2703(d) order. We respectfully suggest that if Congress intended to circumscribe the discretion it gave to magistrates under § 2703(d) then Congress, as the representative of the people, would have so provided. Congress would, of course, be aware that such a statute mandating the issuance of a § 2703(d) order without requiring probable cause and based only on the Government's word may evoke protests by cell phone users concerned about their privacy. The considerations for and against such a requirement would be for Congress to balance. A court is not the appropriate forum for such balancing, and we decline to take a step as to which Congress is silent.

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.

We again note that although the Government argues that it need not offer more than "specific and articulable facts showing that there are reasonable grounds to believe that the . . . information sought . . . [is] relevant and material to an ongoing criminal investigation," 18 U.S.C. § 2703(d), the MJ never analyzed whether the Government made such a showing. We leave that issue for the MJ on remand.

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.

The majority begins its analysis of § 2703(d) correctly:

> 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. Instead, the standard is governed by the text of § 2703(d), i.e., "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the record or other information sought, are relevant."

Maj. Op. at 16-17 (quoting § 2703(d)). But the majority then appears to contradict its own holding later in its opinion, when it states "[b]ecause 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." *Id.* at 28. Thus, the majority suggests that Congress did not intend to circumscribe a magistrate's discretion in determining whether or not to issue a court order, while at the same time acknowledging that "[o]rders of a magistrate judge must be supported by reasons that are consistent with the standard applicable under the statute at issue." *Id.* at 24. I do not believe that these contradictory signals give either magistrate judges or prosecutors any standards by which to judge whether an application for a § 2703(d) order is or is not legally sufficient.

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 (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 24. 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,[9] even when the conditions of the statute are met.

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.[10] *See Kyllo v. United States*, 533 U.S. 27, 35-36 (2001); *United States v. Pineda-Moreno*, 2010 WL 3169573 (9th Cir. 2010) (Kozinski, C.J., dissenting from denial of rehearing en banc).

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.[11]

---

[9] Unless the admonition that the magistrate's naked power should "be used sparingly," Maj. Op. at 28, is accepted as a meaningful and objectively enforceable guideline.

[10] 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.

[11] I am also troubled by the majority's assumption, without any support in the record, that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." Maj. Op. at 25. In *Smith v. Maryland*, 442 U.S. 735 (1979), the Supreme Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Id.* at 743-44. Subsequent cases in this fast-changing technological era have found that this is a fact-intensive inquiry. *Compare United States v. Maynard*, 2010 WL 3063788 (D.C. Cir. 2010) (holding that there is an expectation of privacy in long-term GPS surveillance records), *with U.S. Telecom Ass'n v. FCC*, 227 F.3d 450, 459 (D.C. Cir. 2000) (finding no legitimate expectation of privacy in information, including cell

site location information, conveyed to the phone company in order to complete calls); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) ("[E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

Like the magistrate's failure to find whether the government made a sufficient showing under § 2703(d), *see* Maj. Op. at 28 ("the MJ never analyzed whether the Government made such a showing"), I would also "leave [the expectation of privacy] issue for the MJ on remand," *id.* at 29, in the first instance, if determination of that issue becomes relevant.