

United States Court of Appeals,  
Third Circuit.

In the Matter of the APPLICATION OF the UNITED STATES of America  
FOR AN ORDER DIRECTING A PROVIDER OF ELECTRONIC COMMU-  
NICATION SERVICE TO DISCLOSE RECORDS TO the GOVERNMENT.  
United States of America, Appellant.

Filed: Sept. 7, 2010.

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. Comm’n Serv. to Disclose Records to the Gov’t](#), 534 F.Supp.2d 585, 616 (W.D.Pa.2008) (hereafter “[MJOp.](#)”). . . . The Government appeals.

\* \* \*

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 \(1968\)](#).<sup>FN2</sup> . . .

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 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).

\*2 [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<sup>FN3</sup>—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.

\*3 *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].

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.

[1] 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.

\*4 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](#).

\* \* \*

[T]he 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.

\*6 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.” [Karo, 468 U.S. 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.

\*7 [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. 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.

\* \* \*

#### IV.

\*9 [2] 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 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, 111 S.Ct. 1547, 113 L.Ed.2d 690 \(1991\)](#) (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](#).

**\*10** 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.*

\* \* \*

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.<sup>FNS</sup>

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.

\*11 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.

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, 121 S.Ct. 2038, 150 L.Ed.2d 94 (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.”).

\*12 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, 104 S.Ct. 3296.

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); [Schneekloth 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 of-

ficer 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.

\*13 [Id.](#) at 717, 104 S.Ct. 3296.

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.”

\*14 Maj. Op. at ---- - ---- (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 ----. 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 ----. 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, 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 ----. 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,<sup>FN9</sup> 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.<sup>FN10</sup> 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).

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.