620 F.3d 304
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 COMMUNICATION SERVICE TO DISCLOSE RECORDS TO the GOVERNMENT.
United States of America, Appellant.

No. 08–4227. | Argued Feb. 12, 2010. | Filed: Sept. 7, 2010.

* * *

SLOVITER, Circuit Judge.

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

* * *

I.

* * *

As the Government notes in its reply brief, there is no dispute that historical ***308** 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. [The magistrate's statutory theory was that CSLI is information from a "tracking device," such information is excluded from the "electronic communication" definition, and therefore it cannot be compelled with a 2703(d) order. The panel rejects this interpretation, grounding its reasoning in lax Fourth Amendment precedent about location tracking.]

* * *

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), 1986 U.S.C.C.A.N. 3555, 3555. 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, 1986 U.S.C.C.A.N. 3555, 3557; *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 ***314** 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.

* * *

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 ***315** 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 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.

***316** 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.*

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 ***317** 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 cell phone provider in response to the Government's request, or from making a judgment about the possibility that such disclosure would implicate the Fourth Amendment, as it could if it would disclose location information about the interior of a home.

The Government argues that no CSLI can implicate constitutional protections because the subscriber has shared its information with a third party, i.e., the communications provider. For support, the Government cites *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976), in which the Supreme Court found that an individual's

bank records were not protected by the Constitution because "all of the records [which are required to be kept pursuant to the Bank Secrecy Act,] pertain to transactions to which the bank was itself a party," *id.* at 441, 96 S.Ct. 1619 (internal quotation and citation omitted), and "[a]ll of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business," *id.* at 442, 96 S.Ct. 1619.

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

A cell phone customer has not "voluntarily" shared his location information with a cellular provider in any meaningful way. As the EFF notes, it is unlikely that cell phone customers are aware that their cell phone providers *collect* and store historical location information. Therefore, "[w]hen a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed and there is no indication to the user that making that call will also locate the caller; when a cell ***318** 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.").

[The panel makes two uncontroversial observations about Supreme Court precedent. First, there is special Fourth Amendment protection for precise location tracking within the home. Second, suspicion of criminal conduct is not sufficient to undo Fourth

Amendment protections.]

* * *

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 ***320** 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 313 (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 319. 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 316–17. 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 316. I respectfully suggest, however, that the majority's interpretation of the statute, because it provides *no* standards for the approval or disapproval of an application for an order under § 2703(d), does just that—vests magistrate judges with arbitrary and uncabined discretion to grant or deny issuance of § 2703(d) orders at the whim of the magistrate,[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, 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).

***321** 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]

Footnotes

[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 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.

[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) 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).

[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)....").

[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.

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

[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 317. In *Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (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, 99 S.Ct. 2577. Subsequent cases in this fast-changing technological era have

found that this is a fact-intensive inquiry. *Compare United States v. Maynard,* 615 F.3d 544 (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 319 ("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 319, in the first instance, if determination of that issue becomes relevant.