CRIMINAL LAW — STORED COMMUNICATIONS ACT — THIRD CIRCUIT ALLOWS GOVERNMENT TO ACQUIRE CELL PHONE TRACKING DATA WITHOUT PROBABLE CAUSE. — *In re The Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010).

The Stored Communications Act[1] (SCA) articulates the standard the government must meet to obtain electronic communications records from phone companies.[2] In addition to the traditional option of obtaining a warrant by showing probable cause,[3] § 2703(d) of the SCA permits magistrate judges to grant court orders for acquisition of these records if the government meets a lower standard by "offer[ing] specific and articulable facts showing that there are reasonable grounds to believe" that the records "are relevant and material to an ongoing criminal investigation."[4] The government has often attempted, with varying degrees of success, to use § 2703(d) to obtain cell-site location information (CSLI),[5] which uses a cell phone's communication with cell towers to determine the approximate location of an individual over time.[6] Recently, in *In re The Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*,[7] the Third Circuit held that § 2703(d) applies to CSLI and that magistrates may grant court orders to obtain CSLI when the government meets § 2703(d)'s "specific and articulable facts" standard.[8] But the court also gave magistrates the power — "to be used sparingly" — to require the government to show probable cause and obtain a warrant for CSLI.[9] The Third Circuit failed to clarify exactly how often magistrates may require a warrant and did not explain what factors magis-

---

1 18 U.S.C. §§ 2701–2711 (2006).

2 *See id.* § 2703(c)(1).

3 *See id.* § 2703(c)(1)(A); FED. R. CRIM. P. 41(d)(1).

4 18 U.S.C. § 2703(d); *see also id.* § 2703(c)(1)(B). While it is not entirely clear how stringent the § 2703(d) standard is, it is definitely less stringent than probable cause. *See* Paul Ohm, *Probably Probable Cause: The Diminishing Importance of Justification Standards*, 94 MINN. L. REV. 1514, 1520–21 (2010).

5 *See ECPA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 81–85 (2010) [hereinafter *Hearing*] (statement of Stephen Wm. Smith, U.S. Mag. J.); *see also id.* at 93–94 (collecting cases).

6 For detailed information on different types of CSLI and the accuracy with which such CSLI identifies cell phone locations, see Kevin McLaughlin, Note, *The Fourth Amendment and Cell Phone Location Tracking: Where Are We?*, 29 HASTINGS COMM. & ENT. L.J. 421, 426–27 (2007).

7 620 F.3d 304 (3d Cir. 2010). Before this case, no court of appeals had addressed the § 2703(d) standard.

8 *See id.* at 313.

9 *Id.* at 319.

trates should balance in order to make this determination. As a result, *In re Application* provides little guidance to magistrates about how often and in what circumstances they may deny § 2703(d) orders.

As part of a 2007 criminal investigation targeting a suspected drug trafficker, the government applied for a § 2703(d) order requiring a cell phone service provider to turn over CSLI.[10] The government argued that this information would help determine the suspect's approximate whereabouts and might have provided information regarding the location of the suspect's drug supply, stash houses, and distribution networks.[11]

In an opinion joined by many of the magistrates in the Western District of Pennsylvania,[12] Magistrate Judge Lenihan denied the government's request for a § 2703(d) order.[13] She noted that the SCA applies only to wire or electronic communications, "which are expressly defined to exclude communications from a device 'which permits the tracking of the movement of a person or object.'"[14] Because triangulation of CSLI could enable the government to place a person within fifty feet of her physical location, Magistrate Judge Lenihan held that cell phones are "tracking device[s]."[15] Further, she stated that because § 2703(d) allows disclosure "only if" the government meets the "specific and articulable facts" standard — as opposed to "if" or "whenever" the government meets that standard — showing specific and articulable facts "is a *necessary*, but not necessarily *sufficient*, condition for issuance of an Order."[16] Finally, she noted that the constitutional avoidance doctrine counseled in favor of "a limiting interpretation that does not require the Courts repeatedly, on an *ex parte ad hoc* basis, to delineate the precise bounds of Fourth Amendment protection."[17] Because most Americans are unaware that cellular service providers retain CSLI,[18] there is a reasonable expectation of privacy in this data. Thus, probable cause and a warrant are required to retrieve CSLI.[19]

---

[10] *See In re* The 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, 588 (W.D. Pa. 2008).

[11] *See id.* at 588 & n.12. The facts about the investigation and suspect in this case are sparse because the underlying application for a court order was sealed "in order not to jeopardize an ongoing criminal investigation." *Id.* at 616.

[12] *See id.* at 616. The Third Circuit noted that the support of the other magistrates was "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." *In re Application*, 620 F.3d at 308.

[13] *In re Application*, 534 F. Supp. 2d at 616.

[14] *Id.* at 601 (quoting 18 U.S.C. § 3117(b) (2006)).

[15] *Id.* at 602.

[16] *Id.* at 608 (internal quotation marks omitted).

[17] *Id.* at 611.

[18] *See id.*

[19] *See id.* at 615–16.

Judge McVerry, in the Western District of Pennsylvania, authored a short opinion affirming Magistrate Judge Lenihan's opinion.[20] He noted simply that it was "not clearly erroneous or contrary to law."[21]

The Third Circuit vacated and remanded.[22] Writing for the panel, Judge Sloviter[23] held that CSLI is not excluded from the scope of the SCA.[24] While the SCA applies to both wire and electronic communications, the "tracking device" exception, perhaps counterintuitively, does not apply to all tracking devices — the SCA defines electronic communications to exclude communications made from a tracking device, but has no similar exception for wire communications.[25] Judge Sloviter held that, because CSLI is collected by cell towers, "[t]hat historical record is derived from a 'wire communication'" and is not "a separate 'electronic communication.'"[26] Thus, the court did not reach the issue of whether the phone was used as a tracking device.

Judge Sloviter then discussed a set of cases relating to beeper signal tracking.[27] *United States v. Knotts*[28] held that the warrantless monitoring of a beeper signal on public highways does not violate reasonable expectations of privacy, because vehicles on these roads are open to public view.[29] In contrast, *United States v. Karo*[30] held that the warrantless monitoring of a beeper inside of a private residence does impinge on a justifiable expectation of privacy and thus violates the Fourth Amendment.[31] Here, the Third Circuit found no evidence that CSLI allows suspects to be tracked precisely enough to place them at home, and thus held that there is no violation of privacy interests.[32] Therefore, the court concluded that probable cause and a warrant are not necessarily required by the Fourth Amendment.

The court then turned to one of Magistrate Judge Lenihan's alter-

---

[20] *In re* The 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).

[21] *Id.*

[22] *In re Application*, 620 F.3d at 319.

[23] Judge Sloviter was joined by Judge Roth.

[24] *See In re Application*, 620 F.3d at 313.

[25] *See* 18 U.S.C. § 2510(1), (12)(C) (2006); *see also In re Application*, 620 F.3d at 309.

[26] *In re Application*, 620 F.3d at 310.

[27] *See id.* at 312–13.

[28] 460 U.S. 276 (1983).

[29] *See id.* at 281–82.

[30] 468 U.S. 705 (1984).

[31] *See id.* at 714.

[32] *See In re Application*, 620 F.3d at 312–13. This discussion is likely intended as a response to Magistrate Judge Lenihan's constitutional avoidance concerns. *See In re* The 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, 612–13 (W.D. Pa. 2008) (harmonizing *Knotts* and *Karo* and proposing to require probable cause for all CSLI to "avoid repeated Constitutional adjudication and trespass into protected areas," *id.* at 613 (citing *Karo*, 468 U.S. at 718)).

native arguments: that § 2703(d) *allows* lower courts to issue orders for CSLI upon a showing of "specific and articulable facts," but does not *mandate* that an order issue absent probable cause. Judge Sloviter noted that "§ 2703(d) states that a 'court order for disclosure . . . *may be* issued by any . . . court of competent jurisdiction and *shall* issue *only if*' the intermediate standard is met."[33] While the phrase "shall . . . if" is the language of mandate, the construction "shall . . . only if" is the language of permission, and thus magistrates have some discretion to require probable cause and a warrant for the government to collect CSLI.[34]

Finally, Judge Sloviter attempted to articulate a standard for when magistrates may require a showing of probable cause. She admitted to being "stymied by the failure of Congress to make its intention clear" and "respectfully suggest[ed] that if Congress intended to circumscribe the discretion it gave to magistrates under § 2703(d) then Congress . . . would have so provided."[35] However, the court did note that "a magistrate judge does not have arbitrary discretion. . . . Orders of a magistrate judge must be supported by reasons that are consistent with the standard applicable under the statute at issue."[36] The court also stated that "[a] court is not the appropriate forum for such balancing [of the privacy costs versus public safety benefits of mandatory orders], and we decline to take a step as to which Congress is silent."[37] But the court then instructed that "should the [magistrate] conclude that a warrant is required[,] . . . it is imperative that the [magistrate] make fact findings and give a full explanation that balances the Government's need . . . for the information with the privacy interests of cell phone users."[38] Finally, the court admonished magistrates that requiring a showing of probable cause "is an option to be used sparingly because Congress also included the option of a § 2703(d) order."[39]

Judge Tashima filed a concurrence.[40] Although he agreed with the

---

[33] *In re Application*, 620 F.3d at 315 (quoting 18 U.S.C. § 2703(d) (2006) (emphasis added)).

[34] *See id.* at 315–16. Judge Sloviter also discussed whether obtaining CSLI could *ever* qualify as a Fourth Amendment search. *See id.* at 317–19. She found that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way" because customers are unlikely to be aware that service providers collect and store CSLI. *Id.* at 317 (distinguishing *Smith v. Maryland*, 442 U.S. 735 (1979), which held that there is no expectation of privacy in dialed phone numbers because users voluntarily turn them over to the phone company). Cell phone users thus do have a reasonable expectation of privacy in CSLI, and its acquisition can implicate constitutional protections. *See id.* at 318–19 (drawing support from the logic in *Karo*, 468 U.S. at 716–17).

[35] *Id.* at 319.

[36] *Id.* at 316–17.

[37] *Id.* at 319.

[38] *Id.*

[39] *Id.*

[40] *Id.* (Tashima, J., concurring).

result that the majority reached, Judge Tashima felt that the "contradictory signals" in the majority opinion failed to "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."[41] Because the majority failed to articulate any true standards, he argued that the majority's interpretation in fact granted magistrates unlimited discretion.[42] He would have cabined this discretion by holding that, once the government presents specific and articulable facts, a magistrate may require a demonstration of probable cause only when the magistrate "finds that the [§ 2703(d)] 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."[43]

The Third Circuit's failure to provide a clear standard for when magistrates may require a warrant for CSLI makes it difficult to know what magistrates should do when confronted with § 2703(d) requests. In sum, the Third Circuit provided two sets of instructions to magistrates: First, a court should not engage in balancing, but if it decides to require a warrant, it must engage in balancing. Second, Congress intended discretionary authority under § 2703(d) to be uncircumscribed, but this authority should not be used often or arbitrarily. These statements give rise to two basic questions: First, how much discretion to require a showing of probable cause do magistrates possess? And second, what factors should a magistrate consider in exercising that discretion?

Regarding the first question, magistrates generally lack any discretion when issuing warrants.[44] In the context of § 2703(d) orders, this lack of discretion might suggest that standard-setting power should lie at the appellate rather than at the trial level. However, the case law on magistrate discretion regarding search warrants is dependent on the text of the standard for obtaining a warrant, which states that "a magistrate judge . . . *must* issue the warrant if there is probable cause . . . to install and use a tracking device."[45] Because the Third

---

[41] *Id.* at 320.

[42] *See id.*

[43] *Id.*

[44] *See, e.g.*, *Ex parte* United States, 287 U.S. 241, 250 (1932) ("The authority conferred upon the trial judge to issue a warrant of arrest upon an indictment does not . . . carry with it the power to decline to do so under the guise of judicial discretion . . . ."); Abraham S. Goldstein, *The Search Warrant, the Magistrate, and Judicial Review*, 62 N.Y.U. L. REV. 1173, 1196 (1987) ("The few cases on the issue hold that a judge has a 'ministerial' duty to issue a warrant after 'probable cause' has been established."); Orin S. Kerr, *Ex Ante Regulation of Computer Search and Seizure*, 96 VA. L. REV. 1241, 1261 (2010) ("A review of [Supreme Court] case law indicates that existing Fourth Amendment doctrine contemplates a surprisingly narrow role for magistrate judges.").

[45] FED. R. CRIM. P. 41(d)(1) (emphasis added).

Circuit interpreted § 2703(d)'s language to be permissive, there is no comparable basis in this statute to suggest that granting a court order for CSLI is a largely ministerial function.[46]

There are a variety of normative arguments in favor of granting broad discretion to magistrates. Because magistrates deal with requests for CSLI more frequently than do other judges, allowing magistrates discretion would promote flexibility in responding to frequent technological changes in the communications field.[47] In addition, allowing this flexibility would not unduly hamper the ability of the government to obtain CSLI, because magistrates are typically fairly lenient in issuing warrants, provided that doing so would not violate the Constitution.[48] And formulating a policy that is more lenient to defendants (although not overly so) could serve as a preference-eliciting default rule,[49] which would most likely prompt the legislature to update a statute that was designed when cell phones were only a few years old and weighed several pounds.[50]

However, the text of the Third Circuit's opinion indicates that magistrates should require warrants sparingly[51] and that appeals courts exercise de novo review over these cases.[52] These conclusions suggest that the court might have wanted to impose substantive constraints on when magistrates can deny § 2703(d) orders and require warrants.[53] The problem with this argument is that the Third Circuit

---

[46] The text of the Magistrate Judge Act, 28 U.S.C. § 636 (2006), indicates that magistrates can only act in limited areas, but it supplies no explicit restraint on their discretion provided they are acting within one of these areas.

[47] *See* United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1007 (9th Cir. 2009) ("[W]e must rely on the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity.").

[48] *See In re Application*, 620 F.3d at 317 n.8. While no exact data are available on the number of requested and issued electronic surveillance orders, Magistrate Judge Smith estimates that the total number granted exceeds 10,000 per year. *See Hearing*, *supra* note 5, at 80 (statement of Stephen Wm. Smith, U.S. Mag. J.).

[49] *See* EINER ELHAUGE, STATUTORY DEFAULT RULES 168–81 (2008) (describing how canons of construction favorable to defendants, such as the rule of lenity, are more likely to prod the legislature into action).

[50] *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶¶ 58–70, 73 (arguing that the standard for obtaining electronic communications merits heightened protection); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233–42 (2004) (describing possible updates to the SCA); Ohm, *supra* note 4, at 1522 (finding that "[s]cholars who have considered the question unanimously agree that Congress should amend the SCA . . . to strengthen privacy protection").

[51] *See In re Application*, 620 F.3d at 319.

[52] *See id.* at 305. *But see Comprehensive Drug Testing*, 579 F.3d at 1003 (applying an abuse of discretion standard of review).

[53] One possible rationale for imposing substantive constraints is that disuniformity among magistrates might create constitutional uncertainty, *see* Kerr, *supra* note 44, at 1278, which might

could have imposed such a restriction explicitly but never clearly articulated a standard for magistrates to follow.[54] One might interpret the court's constitutional discussion as articulating a standard allowing magistrates to require a warrant where CSLI acquisition would constitute a Fourth Amendment search.[55] However, this proposed standard would be no different from declaring § 2703(d) mandatory, because magistrates must in any case refuse to grant orders that are inconsistent with the Fourth Amendment.[56] Alternatively, one might find that the court's requirement that the magistrate balance the government's need for information with cell phone users' privacy interests[57] provides a standard. But the requirements of findings of fact and a full explanation suggest that this constraint is more procedural than it is substantive, and the court never described what factors to balance.

Regarding the second question, the Third Circuit provided little guidance about which factors magistrates should balance when deciding whether to grant a § 2703(d) order. Typically, magistrates weigh a variety of factors when making this determination. If the need for CSLI is particularly time-sensitive, a magistrate will almost certainly grant the order.[58] In more typical cases, a magistrate is more likely to grant an order when the CSLI request is limited to single tower data (which provides much less precise location information than triangulating from multiple towers or using GPS data),[59] and when the request is for historical rather than prospective or real-time CSLI.[60] In short, magistrates currently appear to be concerned about how invasive the tracking likely appears to the average user.

However, some magistrates might take the Third Circuit's command to require a warrant "sparingly" as a constraint on the factors that they may consider. Magistrates might focus more narrowly on

---

in turn encourage the government to shop for magistrates who are known to grant § 2703(d) orders without requiring a showing of probable cause.

54 *See In re Application*, 620 F.3d at 320 (Tashima, J., concurring).

55 This interpretation is the standard that Judge Tashima wanted to adopt. *See id.*; *see also* Orin Kerr, *Third Circuit Rules that Magistrate Judges Have Discretion to Reject Non-Warrant Court Order Applications and Require Search Warrants to Obtain Historical Cell-Site Records*, THE VOLOKH CONSPIRACY (Sept. 8, 2010, 2:23 PM), http://volokh.com/2010/09/08/third-circuit-rules-that-magistrate-judges-have-discretion-to-reject-court-order-application-and-require-search-warrants-to-obtain-historical-cell-site-records ("[W]hat is the standard? To be candid, I'm not sure. [The court's] discussion . . . suggests that perhaps magistrates should . . . conduct an ex ante constitutional analysis of whether the cell-site surveillance would require a warrant under the Fourth Amendment.").

56 *See* Johnson v. United States, 333 U.S. 10, 13–14 (1948).

57 *See In re Application*, 620 F.3d at 319.

58 *Cf.* Ohm, *supra* note 4, at 1546 ("One imagines that every request made during a kidnapping or while tracking a fugitive meets probable cause.").

59 *See Hearing*, *supra* note 5, at 83–84, 93–94 (statement of Stephen Wm. Smith, U.S. Mag. J.).

60 *See id.* at 84.

whether the request for CSLI raises constitutional doubts.[61] By limiting the discretion of magistrates to require probable cause, this standard might unintentionally introduce a one-way ratchet into the CSLI system. Factors such as whether data is historical or how precisely a suspect can be tracked would not be included in a purely constitutional analysis given that, under *Knotts* and *Karo*, a cell phone user's expectation of privacy is dependent only on whether monitoring invades his home.[62] Thus, magistrates would be unable to cabin the scope of CSLI requests and would have to grant more and broader requests.[63]

Regardless of how tightly the Third Circuit wanted to cabin magistrate discretion, it should have clearly articulated the standard it was applying.[64] Had the court done so, magistrates could determine more easily when to grant a § 2703(d) order. As it stands now, some magistrates will likely grant all § 2703(d) orders that are constitutionally permissible (applying a theory of limited discretion), while other magistrates will likely impose more stringent standards, taking into account factors such as how precisely CSLI can track a phone's user (applying a theory of broader discretion). This state of affairs results in the worst of both worlds, realizing drawbacks from both theories — including magistrate shopping and unexpected intrusion into private activity — without fully realizing either the consistency of the more ministerial standard or the flexibility of the more discretionary standard.

---

[61] *See supra* note 55.

[62] The D.C. Circuit, in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), arrived at a different interpretation of *Knotts* in the context of GPS tracking of a car on public highways. The court noted that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance," *id.* at 562, and held that because this type of surveillance reveals such an "intimate picture of the subject's life," *id.* at 563, the GPS tracking qualified as a search, *id.* *But see* United States v. Pineda-Moreno, 591 F.3d 1212, 1216–17 (9th Cir. 2010) (finding *Knotts* controlling in the GPS tracking context and holding that such tracking is not a search). One magistrate recently analyzed a request for a § 2703(d) order under the framework of *Maynard* — he held that acquiring CSLI necessarily functions as a search because it, like GPS data, "effectively convey[s] details that reveal the most sensitive information about a person's life." *In re* An Application of the United States for an Order Authorizing the Release of Historical Cell-Site Info., No. 10-MC-0897, 2010 WL 5437209, at *3 (E.D.N.Y. Dec. 23, 2010).

[63] Two procedural considerations would compound the effect of this one-way ratchet. First, courts have generally found that there is no exclusion remedy contained in the SCA. *See, e.g.*, United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998). Thus, defendants could ask for exclusion only under the terms of the Fourth Amendment. Second, under the good faith exception to the exclusionary rule, police officers are allowed to rely on the decisions of magistrates, and evidence will not be excluded if the magistrate makes a reasonable but incorrect decision. *See* United States v. Leon, 468 U.S. 897, 920–21 (1984).

[64] Indeed, Magistrate Judge Smith noted in one of his opinions that it was "written in the full expectation and hope that the government will seek appropriate review by higher courts so that authoritative guidance will be given the magistrate judges who are called upon to rule on these applications on a daily basis." *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 765 (S.D. Tex. 2005).