IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

United States Court of Appeals
Fifth Circuit
FILED
July 30, 2013
Lyle W. Cayce
Clerk

No. 11-20884

IN RE: APPLICATION OF THE UNITED STATES OF AMERICA FOR HISTORICAL CELL SITE DATA

UNITED STATES OF AMERICA,

Appellant

Appeal from the United States District Court
for the Southern District of Texas

Before REAVLEY, DENNIS, and CLEMENT, Circuit Judges.

EDITH BROWN CLEMENT, Circuit Judge:

We are called on to decide whether court orders authorized by the Stored Communications Act to compel cell phone service providers to produce the historical cell site information of their subscribers are per se unconstitutional. We hold that they are not.

I. FACTUAL AND PROCEDURAL BACKGROUND

In early October 2010, the United States filed three applications under § 2703(d) of the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712, seeking evidence relevant to three separate criminal investigations. Each application requested a court order to compel the cell phone service provider for a particular cell phone to produce sixty days of historical cell site data and other subscriber information for that phone. The Government requested the same cell

site data in each application: "the antenna tower and sector to which the cell phone sends its signal." It requested this information for both the times when the phone sent a signal to a tower to obtain service for a call and the period when the phone was in an idle state.[1] *In re Application of the United States for Historical Cell Site Data*, 747 F. Supp. 2d 827, 829 (S.D. Tex. 2010).

For each application, the magistrate judge granted the request for subscriber information but denied the request for the historical cell site data, despite finding that the Government's showing met the "specific and articulable facts" standard set by the SCA for granting an order to compel the cell site data. Shortly thereafter, the magistrate judge invited the Government to submit a brief justifying the cell site data applications. Four days after the Government submitted its brief, the magistrate judge issued a written opinion taking judicial notice of a host of facts about cell phone technology, primarily derived from the testimony of a computer science professor at a congressional hearing, but also including information from published studies and reports and service provider privacy policies. He concluded his opinion by declaring that, based on these facts viewed in light of Supreme Court precedent, "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment." *Id.* at 846.

The Government filed objections with the district court to the magistrate judge's ruling on the constitutionality of the SCA and his judicial notice of facts. Although there was no party adverse to the Government's ex parte application, the ACLU and Electronic Frontier Foundation ("EFF"), among others, participated as amici curiae. As part of its submissions, the Government provided the court with additional evidence in the form of an affidavit from one

[1] According to the Government, it now believes that cell phone service providers do not create cell site records when a phone is in an idle state, and it is willing to exclude such information from the scope of its applications.

of the service providers detailing its cell site records. After the parties submitted their briefs, the district judge issued a single-page order. He concluded:

> When the government requests records from cellular services, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause. The records would show the date, time called, number, and location of the telephone when the call was made. These data are constitutionally protected from this intrusion. The standard under the Stored Communications Act is below that required by the Constitution.

The Government appealed once again, and the ACLU and EFF,[2] along with Professor Orin Kerr and others, requested and were granted leave to participate as amici.

II. STANDARD OF REVIEW

This court reviews constitutional challenges to federal statutes de novo. *United States v. Pierson*, 139 F.3d 501, 503 (5th Cir. 1998). It reviews a district court's findings of fact for clear error. *United States v. Keith*, 375 F.3d 346, 348 (5th Cir. 2004). "A finding of fact is clearly erroneous 'when although there is evidence to support it, the reviewing court on the entire evidence is left with a firm and definite conviction that a mistake has been committed.'" *In re Missionary Baptist Found. of Am., Inc.*, 712 F.2d 206, 209 (5th Cir.1983) (quoting *United States v. U.S. Gypsum Co.*, 333 U.S. 364, 395 (1948)). The court reviews use of judicial notice under Federal Rule of Evidence 201 for abuse of discretion. *Taylor v. Charter Med. Corp.*, 162 F.3d 827, 829 (5th Cir. 1998). Although the Federal Rules of Evidence may not apply to applications for § 2703(d) orders, Rule 201 "embodies 'the traditional view' of judicial notice . . . 'consistent with' the common law," WRIGHT, MILLER & COOPER, 21B FED. PRAC. & PROC. EVID.

[2] These two amici, which filed jointly, are referred to as "the ACLU" for simplicity.

§ 5102 (2d ed.), so the court will apply the same standard to common law judicial notice.

III. DISCUSSION

The Government raises two issues on appeal. First, it challenges the district court's adoption of the magistrate judge's conclusion that the SCA unconstitutionally lowers the standard the Government must meet to compel disclosure of historical cell site information below that required by the Fourth Amendment. Second, it claims that the magistrate judge's judicial notice of certain facts, to the extent they were adopted by the district court, was improper. To these merits issues presented by the Government, amicus Professor Orin Kerr adds two threshold issues: whether this case is ripe and whether 28 U.S.C. § 1291 gives the court appellate jurisdiction over it.

A. Jurisdiction

1. Ripeness

Professor Kerr claims that this controversy is not ripe. He asserts that the issue of whether a court order complies with the Fourth Amendment must be addressed after officers execute the order, not before. According to Professor Kerr, exclusively ex post review of such orders is "essential because Fourth Amendment law is extremely fact-specific." Although we agree that this approach is preferable in most cases, *see Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) (en banc) ("The Fourth Amendment is designed to account for an unpredictable and limitless range of factual circumstances, and accordingly it *generally* should be applied after those circumstances unfold, not before." (emphasis added)), we also agree that, as he says, here we are presented with the unusual circumstance of "an abstract question of [Fourth Amendment] law with no connection to a genuine factual record." Because the district court concluded that the § 2703(d) order provision was categorically unconstitutional with respect to an entire class of records – historical cell site information – that

is covered under the plain text of § 2703(c), our review of its decision addresses only whether the fact that the Government's request was for such records is, by itself, sufficient to make its applications for § 2703(d) orders unconstitutional.[3]

This issue satisfies our test for ripeness. Such cases are ripe when they meet two criteria. "First, they are fit for judicial decision because they raise pure questions of law. Second, [the plaintiff] would suffer hardship if review were delayed." *Opulent Life Church v. City of Holly Springs, Miss.*, 697 F.3d 279, 287-88 (5th Cir. 2012). Here, the Government applied for three § 2703(d) orders, and the magistrate judge denied its applications on the basis that the SCA's authorization of such orders for cell site information violates the Constitution. The district court adopted the magistrate judge's decision to deny the applications on constitutional grounds. The Government's claim that this denial is improper and deprives it of a legitimate investigatory tool is a question of law, amenable to judicial resolution. Moreover, this is the only time that the Government can challenge the denial of its order. It cannot wait until after it executes the order, because there is no order to execute. The dispute is ripe for review.

The cases cited by Professor Kerr do not alter this conclusion. He points out that in *Warshak,* the Sixth Circuit, sitting en banc, discussed how expectations of privacy, particularly in the context of "ever-evolving technologies," typically turn on concrete, case-by-case determinations of a "limitless range of factual circumstances." 532 F.3d at 527-28. However, we are only asked to decide whether every instance of one particular factual circumstance – § 2703(d) orders for historical cell site information – is unconstitutional. If we conclude that such orders are not categorically

[3] For our review, it does not matter how any eventual search would be carried out. Of course, if the Government executed the order in an unconstitutional manner, any evidence it obtained might be subject to suppression. But that is not the issue presented here.

unconstitutional, specific orders within that category certainly may be unconstitutional because of additional facts involved in the case. But we do not need such facts to determine if orders for historical cell site records are per se unconstitutional.

Moreover, *Warshak* involved a plaintiff who sought an injunction against the United States to prevent it from obtaining and executing any § 2703(d) order against him in the future. *Id.* at 524-25. Because no order existed, or might ever exist, the Sixth Circuit held that his claim was too speculative to be ripe for adjudication. *Id.* at 525-31. Similarly, Professor Kerr notes that we dismissed, sua sponte, as unripe a pre-enforcement challenge brought by two unions against a state railway safety law, which they claimed authorized drug testing of railroad employees without probable cause. *See United Transp. Union v. Foster*, 205 F.3d 851, 857-59 (5th Cir. 2000). We held that the unions' claims were speculative and, thus, premature. *Id.* But to trigger the drug tests in the law challenged in *Foster*:

> [T]he following train of events would necessarily have to occur: First, a train must be involved in a collision at a Louisiana railroad crossing . . . Second, even assuming that such a collision occurs, . . . a law enforcement officer must have "reasonable grounds to believe the person to have been operating or in physical control of the locomotive engine while under the influence" of alcohol or other illegal controlled substances. . . . Third, "reasonable grounds to believe" would have to be interpreted to mean something other than "probable cause." . . . Finally, a Louisiana officer would have to order such testing without actually having "probable cause."

Id. at 858; *see also Chandler v. Miller*, 520 U.S. 305, 309-10, 318-22 (1997) (invalidating a state law mandating drug testing for political candidates without requiring the candidates to wait until after they were tested to challenge the law). Unlike the plaintiffs in *Warshak* and *Foster*, the Government's claims are not speculative. It has already been denied the use of § 2703(d) orders for historical cell site information by the district court.

2. Appellate jurisdiction

Professor Kerr does not believe that the order denying the Government's application is a final order over which this court has appellate jurisdiction under 28 U.S.C. § 1291.[4] He argues instead that the Court must treat the Government's appeal as a petition for a writ of mandamus. But federal appellate courts have long treated denials of similar orders under the Wiretap Act as appealable final orders, basing their jurisdiction to review them expressly on § 1291. *See Application of the United States*, 563 F.2d 637, 641 (4th Cir. 1977); *Application of the United States*, 427 F.2d 639, 642 (9th Cir. 1970). The Third Circuit also appears to have based its jurisdiction to review a denial of a § 2703(d) order on § 1291. *See In re Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't*, 620 F.3d 304 (3d Cir. 2010); *see also* WRIGHT, MILLER & COOPER, 15B FED. PRAC. & PROC. § 3919.9 (2d ed.) ("Denial of a government application for a search warrant concludes the only matter in the district court. . . . Appeal is available as from a final decision."). *But see United States v. Savides*, 658 F. Supp. 1399, 1404 (N.D. Ill. 1987), *aff'd sub nom. United States v. Pace*, 898 F.2d 1218 (7th Cir. 1990) ("[T]he government has no right to appeal if it believes the magistrate erred in denying the warrant."). We proceed under § 1291, recognizing that an application for this type of order is an independent proceeding, not tied to any

[4] Professor Kerr also alleges that there is an Article III problem with allowing magistrate judges to address constitutional questions. But, because the order is appealable under § 1291, the magistrate judge's opinion is subject to de novo review by a district judge. *See* FED. R. CRIM. P. 59(b)(3); *see also id.* advisory committee note (explaining that the task of clarifying whether a matter is "dispositive" and therefore subject to de novo review is left to courts, and also that "the district judge retains the authority to review any magistrate judge's decision or recommendation whether or not objections are timely filed [by the losing party]"). This plenary review of the magistrate judge's conclusions by an Article III judge satisfies the constitutional requirements of Article III. *See Peretz v. United States*, 501 U.S. 923, 939 (1991); *Thomas v. Arn*, 474 U.S. 140, 154-55 (1985).

current criminal case, and that denying or granting the order finally disposes of the proceeding.[5]

B. Fourth Amendment challenge

The district court held that the SCA violates the Fourth Amendment because the Act allows the United States to obtain a court order compelling a cell phone company to disclose historical cell site records merely based on a showing of "specific and articulable facts," rather than probable cause.[6] We review this ruling, applying *Katz v. United States* and its progeny to determine whether the Government's acquisition of these electronic records constitutes a search or a seizure subject to the Fourth Amendment's probable cause. 389 U.S. 347, 353 (1967).

The SCA regulates disclosure of stored electronic communications by service providers. With regard to compelled disclosure of non-content records or other subscriber information, the Act requires the Government to, as relevant here, secure either a warrant or a court order for the records. 18 U.S.C. § 2703(c).[7] If the Government seeks a court order, such an order:

> [M]ay be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers

---

[5] Particularly in the case where a court denies the Government's application despite finding that the Government has met its evidentiary burden, in contrast to a case where the court finds that the application is not supported by evidence that satisfies the relevant standard, the order is final, because in such a case the Government cannot return to the court with additional evidence sufficient to convince the court to grant its application. *Cf. Savides*, 658 F. Supp. at 1404 ("*A probable cause determination* on an application for a search warrant by a magistrate is not a final order." (emphasis added)).

[6] Amicus Susan Freiwald expresses concern that the SCA allows executive branch officials to police themselves. We have difficulty understanding this fear. An official must prove to a neutral magistrate that his application for a § 2703(d) order meets the "specific and articulable facts" standard set by Congress. Moreover, if the official executes the order improperly, an injured party may seek judicial review of his actions. These safeguards adequately protect against executive overreaching.

[7] The Government is not required to provide notice to the subscriber. § 2703(c)(3).

> 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.

§ 2703(d). The "specific and articulable facts" standard is a lesser showing than the probable cause standard that is required by the Fourth Amendment to obtain a warrant. U.S. CONST. amend. IV; *see In re Application of the United States*, 620 F.3d at 315 (holding that "§ 2703(d) creates a higher standard than that required by the pen register and trap and trace statutes" but "a less stringent [standard] than probable cause"); *Warshak*, 631 F.3d at 291.

1. Discretion

The ACLU contends that we can avoid the constitutional issue by holding that the magistrate judge had discretion under the SCA to require the Government to seek a warrant rather than a § 2703(d) order to obtain historical cell site information. In support of its argument, the ACLU relies on a Third Circuit decision in which the majority of the panel held that the SCA "gives the [magistrate judge] the option to require a warrant showing probable cause." *In re Application of the United States*, 620 F.3d at 319. The majority reached this conclusion after analyzing the text of the statute. First, it noted that an order "may be issued" by any court with jurisdiction, which is "language of permission, rather than mandate." *Id.* at 315. It concluded that Congress's use of this phrase "strongly implies court discretion." *Id.* Second, it observed that this implication was "bolstered by the subsequent use of the phrase 'only if' in the same sentence." *Id.*; *see* § 2703(d) ("[An order] shall issue only if the governmental entity offers specific and articulable facts that there are reasonable grounds to believe [that the records] sought, are relevant and material to an ongoing criminal investigation."). The majority explained that both the Third Circuit and the Supreme Court had determined that "'only if' describe[s] a necessary condition, not a sufficient condition." *In re Application*

of the United States, 620 F.3d at 316 (quoting *Twp. of Tinicum v. U.S. Dep't of Transp.*, 582 F.3d 482, 488 (3d Cir. 2009)); *see California v. Hodari D.*, 499 U.S. 621, 628 (1991). Therefore it held that the specific and articulable facts standard was necessary to allow, but not sufficient to require, the magistrate judge to issue a § 2703(d) order.

This construction of the SCA, however, ignores the intervening "shall" in the provision. "The word 'shall' is ordinarily 'the language of command.'" *Alabama v. Bozeman*, 533 U.S. 146, 153 (2001) (quoting *Anderson v. Yungkau*, 329 U.S. 482, 485 (1947)); *see Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach*, 523 U.S. 26, 35 (1998) ("The Panel's instruction comes in terms of the mandatory 'shall,' which normally creates an obligation impervious to judicial discretion."). Including this "shall" in our interpretation of the SCA, as we should, *see Kaltenbach v. Richards*, 464 F.3d 524, 528 (5th Cir. 2006) ("It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant." (quoting *TRW Inc. v. Andrews*, 534 U.S. 19, 21 (2001))), we reach a different conclusion from that of the Third Circuit.

Reading the provision as a whole, we conclude that the "may be issued" language is permissive – it grants a court the authority to issue the order – and the "shall issue" term directs the court to issue the order if all the necessary conditions in the statute are met. These conditions include both the requirements specified by § 2703(b) (for orders seeking the contents of electronic communications) or those specified by § 2703(c) (for orders seeking non-content records of such communications) and the "specific and articulable facts standard" laid out in § 2703(d) itself. Therefore, to obtain an order for the historical cell site records of a particular cell phone owner, the Government may apply to a court that has jurisdiction. And that court must grant the order if the

Government seeks an order (1) to "require a provider of electronic communication service or remote computing service" (2) "to disclose a [non-content] record or other information pertaining to a subscriber to or customer of such service" when the Government (3) meets the "specific and articulable facts" standard. If these three conditions are met, the court does not have the discretion to refuse to grant the order.[8] *See In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, 830 F. Supp. 2d 114, 148 (E.D. Va. 2011) ("The fact that 'only if' creates a necessary but not sufficient condition . . . does not automatically create a gap in the statute that should be filled with judicial discretion. The Court considers it more likely that the 'only if' language in § 2703(d) clarifies that any conditions established by (b) and (c) are cumulative with respect to the standard set forth in paragraph (d). The default rule remains that the judicial officer 'shall issue' an order when the government meets its burden.").

Even if the text of the statute supported the ACLU's argument that magistrate judges have discretion to require the Government to secure a warrant for cell site information, such discretion would be beside the point here. The district court did not simply decide that the Government must secure a warrant in this case. It held, adopting the magistrate judge's conclusion, that

[8] The Third Circuit observed that "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." *In re Application of the United States*, 620 F.3d at 319. While we disagree with the Third Circuit that the Government need only give its word to obtain a § 2703(d) order – rather, the Government must show "specific and articulable facts" – we agree with the Third Circuit's statement of Congress's authority. But we believe Congress has weighed these considerations and set this balance. The text of the statute shows that Congress does not want magistrate judges second-guessing its calculus. *See id.* at 320 (Tashima, J., concurring) ("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.").

"[w]hen the government requests records from cellular services, data disclosing the location of the telephone at the time of particular calls may be acquired only by a warrant issued on probable cause. . . . The standard under the Stored Communications Act is below that required by the Constitution." *See also Historical Cell Site Data*, 747 F. Supp. 2d at 846 (concluding that "[c]ompelled warrantless disclosure of cell site data violates the Fourth Amendment," despite the fact that historical cell site information clearly falls within a category of data for which the SCA requires only a § 2703(d) order); *cf. In re Application of the United States*, 620 F.3d at 307-08. Thus, the district court held that all § 2703(d) orders for cell site information were unconstitutional, so it had no discretion to grant such an order. *See In re Application of the United States*, 620 F.3d at 319 (holding, in a case where the magistrate judge below had not ruled on the constitutionality of the SCA, that a magistrate judge has discretion under the statute to require the Government to seek a warrant). Therefore, we cannot avoid the question of whether the SCA's authorization of § 2703(d) orders under a "specific and articulable facts" standard is constitutional.

2. The constitutional question

The Government and the ACLU focus their analysis of the constitutionality of the SCA as applied to historical cell site data on distinct questions. The ACLU focuses on what information cell site data reveals – location information – and proceeds to analyze the § 2703(d) orders under the Supreme Court's precedents on tracking devices. In contrast, the Government focuses on who is gathering the data – private cell service providers, not government officers – and analyzes the provision under the Court's business records cases.

The ACLU contends that individuals have a reasonable expectation of privacy in their location information when they are tracked in a space, like the home, that is traditionally protected or when they are tracked for a longer period

of time and in greater detail than society would expect.[9] The ACLU relies on the concurrences in *United States v. Jones*, 132 S. Ct. 945 (2012), which concluded that prolonged GPS monitoring of a vehicle could constitute a search, *id.* at 964 (Alito, J., concurring in the judgment) (joined by Justices Ginsburg, Breyer, and Kagan); *see id.* at 955 (Sotomayor, J., concurring) (expressly agreeing with Justice Alito's concurrence on this point).[10] The ACLU points out that individuals are only in vehicles for discrete periods, but most people carry cell phones on their person at all times, making the tracking more detailed and invasive. The Government responds that cell site data are only collected when a call is made, which is a discrete event, just like a car ride.

Moreover, the Government argues that cell site information is less precise than GPS location information. It contends that these data are not sufficiently accurate to reveal when someone is in a private location such as a home. But the ACLU points out that the reason that the Government seeks such information is to locate or track a suspect in a criminal investigation. The data must be precise enough to be useful to the Government, which would suggest that, at least in some cases, it can narrow someone's location to a fairly small area. *See* FCC Commercial Mobile Services, 47 C.F.R. § 20.18(h)(1) (2012) (requiring cell

---

[9] The ACLU argues that the extended time period – sixty days – for which the Government sought historical cell site records contravenes privacy expectations. But the Supreme Court has upheld a court order for records that included three monthly statements, or roughly ninety days of records. *United States v. Miller*, 425 U.S. 435, 438 (1976).

[10] The ACLU, as well as the magistrate judge's opinion, *Historical Cell Site Data*, 747 F. Supp. 2d at 841-43, also cite the protections in the Wireless Communication and Public Safety Act of 1999 as evidence that society recognizes a privacy interest in location information, though the ACLU recognizes that, under Supreme Court precedent, statutory protections are not determinative. *See City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010) ("Respondents point to no authority for the proposition that the existence of statutory protection renders a search *per se* unreasonable under the Fourth Amendment. And the precedents counsel otherwise."). But the SCA is a statute as well, and there is little reason to think that absence of statutory protection for a certain type of information is any less evidence of society's *lack* of a privacy interest in that information than presence of legal protection is evidence of such an interest.

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). And the Supreme Court held in *United States v. Karo* that without a warrant the Government cannot determine by means of a beeper whether a particular article (in that case a cannister of ether) is in an individual's home at a particular time. 468 U.S. 705, 719 (1984). In response, the Government argues that a pen register can similarly locate someone to his home. If a person makes a call from his home landline, he must be located in his home at the landline's receiver. Yet the Court in *Smith v. Maryland* nevertheless sanctioned the warrantless use of pen registers, installed by the phone company at the request of police, to record the numbers dialed from particular landlines. 442 U.S. 735, 745-46 (1979).

This argument highlights the difference between the Government's and the ACLU's approaches to this issue. Both *Karo* and *Smith* involved the Government's acquisition of information about the interior of a home: that a particular canister was located in the home or that a person was calling particular numbers from a phone in the home. But in *Karo* (as in *Jones*), the Government was the one collecting and recording that information. And this is the distinction on which the Government's affirmative argument turns. The Government recognizes that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz*, 389 U.S. at 351; *see also id.* at 350-51 ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.' That Amendment protects individual privacy against certain kinds of *governmental intrusion* . . . . But the protection of a person's general right to privacy – his right to be let alone by *other people* – is, like the protection of his

property and of his very life, left largely to the law of the individual States." (emphasis added)).

Therefore, the Government, when determining whether an intrusion constitutes a search or seizure, draws a line based on whether it is the Government collecting the information or requiring a third party to collect and store it, or whether it is a third party, of its own accord and for its own purposes, recording the information. Where a third party collects information in the first instance for its own purposes, the Government claims that it can obtain this information later with a § 2703(d) order, just as it can subpoena other records of a private entity. *Compare Smith*, 442 U.S. at 743 (finding significant that "the phone company does in fact record this information *for a variety of legitimate business purposes*" (emphasis added)), *with Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) (expressing concern over the application of existing Fourth Amendment doctrine to "the use of GPS tracking technology *for law enforcement purposes*" (emphasis added)). We agree.

This question of *who* is recording an individual's information initially is key because:

> [T]he individual must occasionally transact business with other people. When he does so, he leaves behind, as evidence of his activity, the records and recollections of others. He cannot expect that these activities are his private affair. To the extent an individual knowingly exposes his activities to third parties, he surrenders Fourth Amendment protections, and, if the Government is subsequently called upon to investigate his activities for possible violations of the law, it is free to seek out these third parties, to inspect their records, and to probe their recollections for evidence.

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir. 1978). Moreover, "[t]he fortuity of whether or not the [third party] in fact elects to make a quasi-permanent record" of information conveyed to it "does not . . . make any constitutional difference." *Smith*, 442 U.S. at 745.

The third party can store data disclosed to it at its discretion. And once an individual exposes his information to a third party, it can be used for any purpose, as "[i]t is established that, when a person communicates information to a third party *even on the understanding that the communication is confidential*, he cannot object if the third party conveys that information or records thereof to law enforcement authorities." *SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743 (1984) (emphasis added).[11]

The Government does concede that the subpoenaed third party must have possession of – the right to control – the records before officials can require it to turn them over. The Government, therefore, distinguishes cases where a landlord or hotel manager merely has the right to enter the apartment or room of another. The Government acknowledges that "the government may not subpoena the landlord to produce the tenant's personal papers from her apartment." However, it contrasts these situations from the one presented in *United States v. Miller*, 425 U.S. 435 (1976). In *Miller*, the Court rejected a bank depositor's Fourth Amendment challenge to a subpoena of bank records because, as the bank was a party to the transactions, the records belonged to the bank. *Id.* at 440-41 ("[T]he documents subpoenaed here are not respondent's private

[11] Although the ACLU contends that this sort of compulsory process requires notice and an opportunity to litigate the order's validity before it is executed, the Government notes that it is the party who owns the records, not the party whose information is recorded, that has this right to challenge the order. *See Jerry T. O'Brien*, 467 U.S. at 743 (concluding that Supreme Court precedents "disable respondents from arguing that notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers"). The SCA provides that "[a] governmental entity receiving records or information [of non-content data] is not required to provide notice to a subscriber or customer" before or after government officials obtain this information. § 2703(c)(3). Insofar as the ACLU believes that the SCA is constitutionally problematic because it does not require these officials to ever disclose to the subscriber that they sought and obtained his non-content records – whether or not information gleaned from the records led to a criminal prosecution, *cf. Jones*, 132 S. Ct. at 964 (showing special concern for situations where government officials "*secretly* monitor" individuals (emphasis added)) – we note that nothing in the non-content records provisions of the SCA prevents cell service providers from informing their subscribers of such government requests.

papers. . . . [R]espondent can assert neither ownership nor possession. Instead, these are the business records of the bank[]. . . . [They] pertain to transactions to which the bank was itself a party." (citation and internal quotation marks omitted)).

This qualification that the right to possession hinges on whether the third party created the record to memorialize its business transaction with the target, rather than simply recording its observation of a transaction between two independent parties, recently gained context and support from a case decided by the Sixth Circuit. In that case, *United States v. Warshak*, the court of appeals held that the "government may not compel a commercial [internet service provider] to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause." 631 F.3d 266, 288 (6th Cir. 2010). The court reasoned that the emails were communications between two subscribers, not communications between the service provider and a subscriber that would qualify as business records. The provider was merely the "intermediary." *Id.* at 286.

Defining business records as records of transactions to which the record-keeper is a party also fits well with the historical and statutory distinction between communications content and addressing information. *See United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) ("In a line of cases dating back to the nineteenth century, the Supreme Court has held that the government cannot engage in a warrantless search of the contents of sealed mail, but can observe whatever information people put on the outside of mail, because that information is voluntarily transmitted to third parties.") (collecting cases); *see, e.g.*, 18 U.S.C. § 2703(b)-(c). Communications content, such as the contents of letters, phone calls, and emails, which are not directed to a business, but simply sent via that business, are generally protected. However, addressing information, which the business needs to route those communications

appropriately and efficiently are not. *See Smith*, 442 U.S. at 741 (finding significant that pen registers, unlike the listening device employed in *Katz*, "do not acquire the *contents* of communications" and do not require a warrant); *Forrester*, 512 F.3d at 511 ("The government's surveillance of e-mail addresses also may be technologically sophisticated, but it is conceptually indistinguishable from government surveillance of physical mail. . . . E-mail, like physical mail, has an outside address 'visible' to the third-party carriers that transmit it to its intended location, and also a package of content that the sender presumes will be read only by the intended recipient.").

Under this framework, cell site information is clearly a business record. The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use. The Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained. The Government has neither "required [n]or persuaded" providers to keep historical cell site records. *Jones*, 132 S. Ct. at 961 (Alito, J., concurring in the judgment). In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created.

Moreover, these are the providers' own records of transactions to which it is a party. The caller is not conveying location information to anyone other than his service provider. He is sending information so that the provider can perform the service for which he pays it: to connect his call. And the historical cell site information reveals his location information for addressing purposes, not the

contents of his calls.[12] The provider uses this data to properly route his call, while the person he is calling does not receive this information.

The ACLU points out that this conveyance of location information to the service provider nevertheless must be voluntary in order for the cell phone owner to relinquish his privacy interest in the data. The ACLU asserts that here it is not. According to the ACLU, "[w]hen a cell phone user makes or receives a call, there is no indication to the user that making or receiving that call will . . . locate the caller." A user cannot voluntarily convey something which he does not know he has.

The Government disputes the assertion that cell phone users do not voluntarily convey location information. It contends that the users know that they convey information about their location to their service providers when they make a call and that they voluntarily continue to make such calls. We agree.

In *Smith*, the Supreme Court recognized that:

> All telephone users realize that they must "convey" phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making

---

[12] The Ninth Circuit has similarly concluded that "e-mail to/from addresses and IP addresses constitute addressing information and do not necessarily reveal any more about the underlying contents of communication than do phone numbers." *Forrester*, 512 F.3d at 510. It noted that:

> Like IP addresses, certain phone numbers may strongly indicate the underlying contents of the communication; for example, the government would know that a person who dialed the phone number of a chemicals company or a gun shop was likely seeking information about chemicals or firearms. Further, when an individual dials a pre-recorded information or subject-specific line, such as sports scores, lottery results or phone sex lines, the phone number may even show that the caller had access to specific content information. Nonetheless, the Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information that the government did not cross here.

Id. These observations are equally applicable to historical cell site data.

> permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.

442 U.S. at 742. Furthermore, it observed that "[m]ost phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'" *Id.* at 742-43.

A cell service subscriber, like a telephone user, understands that his cell phone must send a signal to a nearby cell tower in order to wirelessly connect his call. *See United States v. Madison*, No. 11-60285-CR, 2012 WL 3095357, at *8 (S.D. Fla. July 30, 2012) (unpublished) ("[C]ell-phone users have knowledge that when they place or receive calls, they, through their cell phones, are transmitting signals to the nearest cell tower, and, thus, to their communications service providers."). Cell phone users recognize that, if their phone cannot pick up a signal (or "has no bars"), they are out of the range of their service provider's network of towers. And they realize that, if many customers in an area attempt to make calls at the same time, they may overload the network's local towers, and the calls may not go through. Even if this cell phone-to-tower signal transmission was not "common knowledge," *California v. Greenwood*, 486 U.S. 35, 40 (1988), the Government also has presented evidence that cell service providers' and subscribers' contractual terms of service and providers' privacy policies expressly state that a provider uses a subscriber's location information to route his cell phone calls. In addition, these documents inform subscribers that the providers not only use the information, but collect it. *See also Madison*, 2012 WL 3095357, at *8 ("Moreover, the cell-phone-using public knows that communications companies make and maintain permanent records regarding cell-phone usage, as many different types of billing plans are available . . . . Some plans also impose additional charges when a cell phone is used outside its 'home area' (known commonly as 'roaming' charges). In order

to bill in these different ways, communications companies must maintain the requisite data, including cell-tower information."). Finally, they make clear that providers will turn over these records to government officials if served with a court order. Cell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that the landline users in *Smith* understood that the phone company recorded the numbers they dialed.

Their use of their phones, moreover, is entirely voluntary. *See United States v. Skinner*, 690 F.3d 772, 777 (6th Cir. 2012) ("There is no Fourth Amendment violation because Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."). The Government does not require a member of the public to own or carry a phone. As the days of monopoly phone companies are past, the Government does not require him to obtain his cell phone service from a particular service provider that keeps historical cell site records for its subscribers, either. And it does not require him to make a call, let alone to make a call at a specific location.

Nevertheless, the ACLU argues that, while an individual's use of his phone may be voluntary, he does not voluntarily convey his cell site information because he does not *directly* convey it to his service provider. The only information he directly conveys is the number he dials. *See In re Application of the United States*, 620 F.3d at 317 ("[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."). This crabbed understanding of voluntary conveyance would lead to absurd results. For example, if a user programmed a contact's telephone number into his phone's speed dial memory, he would only need to dial the speed dial reference number to make the call. Would that mean that the Government would be unable to obtain the contact's

actual telephone number from his service provider? Clearly not. The contact's telephone number is necessary for the service provider to connect the call; the user is aware of this fact; therefore, he is aware that he is conveying that information to the service provider and voluntarily does so when he makes the call.[13] A similar analysis for cell site information leads to the conclusion that a user voluntarily conveys such information when he places a call, even though he does not directly inform his service provider of the location of the nearest cell phone tower. Because a cell phone user makes a choice to get a phone, to select a particular service provider, and to make a call, and because he knows that the call conveys cell site information, the provider retains this information, and the provider will turn it over to the police if they have a court order, he voluntarily conveys his cell site data each time he makes a call.

Finally, the ACLU argues that advances in technology have changed society's reasonable expectations of privacy in information exposed to third parties. *See Jones*, 132 S. Ct. 963-64 (Alito, J., concurring in the judgment) ("In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. . . . Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."); *see also id.* at 957 (Sotomayor, J., concurring). We agree that technological

[13] In an analogous context, when a customer makes a credit card purchase at a store or restaurant, he does not *directly* convey the location of the transaction to his credit card company. Nevertheless, law enforcement officers can obtain his credit card records from the company with a subpoena, *see, e.g.*, *United States v. Maturo*, 982 F.2d 57, 59 (2d Cir. 1992) (DEA agents obtained a subpoena for the credit card records of an investigatory target.), and use them to track his location, *see, e.g.*, *United States v. Kragness*, 830 F.2d 842, 865 (8th Cir. 1987) ("The government introduced credit-card records and an airline-ticket stub which show that [the defendant] traveled from Minneapolis/St. Paul to Miami on August 16, 1980."); *see also* 12 U.S.C. §§ 3402, 3407, 3409 (prescribing that federal officials can obtain an individual's financial records, such as credit card statements, pursuant to judicial subpoena served on his financial institution if "there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry," and, subject to certain exceptions, the individual has notice and an opportunity to object to the disclosure before it occurs).

changes can alter societal expectations of privacy. *See id.* at 962 (Alito, J., concurring) ("Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."). At the same time, "[l]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." *Skinner*, 690 F.3d at 778 (citing *United States v. Knotts*, 460 U.S. 276, 284 (1983)). Therefore, "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment).

Congress has crafted such a legislative solution in the SCA. The statute conforms to existing Supreme Court Fourth Amendment precedent. This precedent, as it now stands, does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure when the records cover more than some specified time period or shed light on a target's activities in an area traditionally protected from governmental intrusion. We decline to create a new rule to hold that Congress's balancing of privacy and safety is unconstitutional.[14]

[14] The Government also argues on appeal that the district court erred by overruling the Government's objections to the magistrate judge's judicially-noticed findings of fact. Because we hold that the magistrate judge had no discretion to deny the Government's application for a § 2703(d) order, we need not reach the issue of whether its judicial notice of facts was improper.

We understand that cell phone users may reasonably want their location information to remain private, just as they may want their trash, placed curbside in opaque bags, *Greenwood*, 486 U.S. at 40-41, or the view of their property from 400 feet above the ground, *Florida v. Riley*, 488 U.S. 445, 451 (1989), to remain so. But the recourse for these desires is in the market or the political process: in demanding that service providers do away with such records (or anonymize them) or in lobbying elected representatives to enact statutory protections. The Fourth Amendment, safeguarded by the courts, protects only reasonable *expectations* of privacy.

Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders requesting data from all phones that use a tower during a particular interval, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods). Nor do we address situations where the Government surreptitiously installs spyware on a target's phone or otherwise hijacks the phone's GPS, with or without the service provider's help.

IV. CONCLUSION

Cell site data are business records and should be analyzed under that line of Supreme Court precedent. Because the magistrate judge and district court treated the data as tracking information, they applied the wrong legal standard. Using the proper framework, the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser "specific and articulable facts" standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional. Moreover, as long as the Government

meets the statutory requirements, the SCA does not give the magistrate judge discretion to deny the Government's application for such an order. Therefore, we VACATE district court's order and REMAND with instructions to grant the Government's applications.

DENNIS, Circuit Judge, dissenting:

In my view, this appeal should be decided by adhering to the Supreme Court's constitutional question avoidance doctrine and construing the applicable ambiguous provisions of the Stored Communications Act to require that the government must obtain a warrant in order to secure an order requiring an electronic communications provider to disclose data potentially protected by the Fourth Amendment, such as the historical cell site location data sought in this case. Because the government did not apply for a warrant, but instead sought such data based only on a showing of reasonable suspicion, the district court reached the correct result in denying the government's request for an order for the provider to disclose that data. Accordingly, I would affirm the result reached by the district court, and I respectfully dissent from the majority opinion's contrary interpretation of the Stored Communications Act and its unnecessary interpretation of the Fourth Amendment as not affording individuals protection of their historical cell site location data.

This appeal properly turns on construction of a statute, rather than on interpretation of the Fourth Amendment. Provisions of the 1986 Stored Communications Act codified at 18 U.S.C. § 2703 authorize the government to require a cellular service provider to disclose a customer's call records, "not including the contents of communications," without the customer's consent, "only when the government[] . . . obtains a warrant" or "obtains a court order for such disclosure under subsection [2703](d)." 18 U.S.C. § 2703(c)(1)(A)-(B). A § 2703(d) order, in turn, "may be issued by any court . . . of competent jurisdiction and shall issue only if the government[]" demonstrates reasonable suspicion "that . . . the records . . . are relevant and material to an ongoing criminal investigation." *Id.* § 2703(d). Critically, the statute is ambiguous as to when the government is to follow "warrant procedures" under § 2703(c)(1)(A).

The government argues that the statute nonetheless should be read as requiring courts to grant every § 2703(d) application that meets the statutory reasonable suspicion standard, regardless of the type of customer records sought. In the government's view, it need never follow "warrant procedures," notwithstanding that such procedures are the first mechanism provided for in the statute. *See id.* § 2703(c)(1)(A).

The majority adopts the government's interpretation of the statute, creating a circuit split with the only other Court of Appeals that has considered the interpretive question. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d 304, 315-17 (3d Cir. 2010). By doing so, the majority is forced to confront the serious and debatable constitutional question of whether cellular customers have a legitimate Fourth Amendment privacy interest in the "cell site location information" generated when we use our phones. The substantial difficulty of this question is reflected in the Supreme Court's conscientious avoidance of similar questions regarding the Fourth Amendment implications of modern telecommunications technologies. *See United States v. Jones*, 132 S. Ct. 945, 953-54 (2012); *City of Ontario v. Quon*, 130 S. Ct. 2619, 2629-30 (2010). The majority adopts the government's position on this issue as well, holding that cellular customers do not have a Fourth Amendment privacy interest in historical cell site location information. On this point too, the majority splits from the Third Circuit, the only other Court of Appeals to have considered the issue. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317-18. This divergence of authority illustrates the difficulty and uncertainty of the constitutional issue.

Respectfully, I believe that the majority's approach contravenes Supreme Court precedent applying the canon of constitutional avoidance, "[']a cardinal

principle' of statutory interpretation." *See Zadvydas v. Davis*, 533 U.S. 678, 689 (2001). "[T]he canon of constitutional avoidance . . . is a tool for choosing between competing plausible interpretations of a statutory text, resting on the reasonable presumption that Congress did not intend the alternative which raises serious constitutional doubts." *Clark v. Martinez*, 543 U.S. 371, 381 (2005). Here, because the government's interpretation "give[s] rise to [a] substantial constitutional question[]," *see INS v. St. Cyr*, 533 U.S. 289, 300 (2001), precedent requires that we "first ascertain whether a construction of the statute is fairly possible by which the constitutional question may be avoided," *United States v. Sec. Indus. Bank*, 459 U.S. 70, 78 (1982) (internal quotation marks omitted) (quoting *Lorillard v. Pons*, 434 U.S. 575, 577 (1978)).

Here, such an "alternative interpretation" is not only "fairly possible," *see St. Cyr*, 533 U.S. at 299-300, but indeed better accords with the statute's text, structure, and purpose than the interpretation advanced by the government and adopted by the majority. Section 2703(c) may be fairly construed to provide for "warrant procedures" to be followed when the government seeks customer records that may be protected under the Fourth Amendment, including historical cell site location information. *See* 18 U.S.C. § 2703(c)(1)(A). This construction gives meaning and effect to all of the statute's words and provisions without rendering any superfluous. It also accords with the enacting Congress's intent to create a statutory framework flexible enough to permit "the law [to] advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment." S. Rep. No. 99-541, at 5 (1986). Moreover, this construction effectuates a workable framework that does not require magistrates to speculate on societal expectations in ex parte application proceedings devoid of the concrete investigative facts upon which Fourth Amendment analysis depends.

Based on this analysis, I would hold that the government must obtain a warrant pursuant to § 2703(c)(1)(A) in order to compel disclosure of the cell site

location records it seeks here, which may be protected from disclosure or seizure absent a warrant. Thus, I would hold that the magistrate judge and district court erred in pronouncing upon the constitutional question and therefore would vacate the constitutional ruling below. However, the magistrate and the district court reached the right result by denying the government's application for an order compelling disclosure of cell site data without a showing of probable cause. I would affirm on statutory grounds the order denying the government's § 2703(d) application with respect to historical cell site location data.

I

The Stored Communications Act was enacted as Title II of the Electronic Communications Privacy Act of 1986, P.L. 99-508 (1986). The legislation's purpose was "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). Section 2703 "details the procedures the government may employ to obtain stored information from a third-party provider, depending upon whether the government is seeking the contents of a stored communication, or non-content information." *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d 283, 296 (4th Cir. 2013) (Wilson, J., concurring) (citing 18 U.S.C. § 2703(a)-(c)). Subsection 2703(c)(1) provides in relevant part:

> 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 or customer of such service (not including the contents of the 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; [or]

> **(B)** obtains a court order for such disclosure under subsection (d) . . . .

18 U.S.C. § 2703(c)(1)(A)-(B). Subsection 2703(d) provides in pertinent part:

> 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.

Id. § 2703(d). The "specific and articulable facts" standard set forth in § 2703(d), *id.*, "is essentially a reasonable suspicion standard," *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d at 287.[1]

The government and the majority maintain that these provisions unambiguously mean that a magistrate *must* issue a § 2703(d) order *whenever* the government's application meets the statutory reasonable suspicion standard. Under this reading, the statute never requires the government to follow the warrant procedures provided for in subsection 2703(c)(1)(A), regardless of the type of non-content records the government seeks.

Contrary to the government's argument, however, the statute is ambiguous as to when the "warrant procedures" described in subsection 2703(c)(1)(A) are to be followed. Thus, we must apply the avoidance canon, a "rule[] for resolving textual ambiguity," *Spector v. Norwegian Cruise Line Ltd.*, 545 U.S. 119, 140 (2005), "counseling that ambiguous statutory language be construed to avoid serious constitutional doubts," *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 516 (2009).

[1] *See, e.g.*, *United States v. Khanalizadeh*, 493 F.3d 479, 483 (5th Cir. 2007) ("Officers must base their reasonable suspicion on 'specific and articulable facts,' not merely 'inarticulate hunches' of wrongdoing."); *see also Terry v. United States*, 392 U.S. 1, 21 (1968).

II

"The appropriate starting point when interpreting any statute is its plain meaning." *United States v. Molina-Gazca*, 571 F.3d 470, 472 (5th Cir. 2009). "In ascertaining the plain meaning of the statute, the court must look to the particular statutory language at issue, as well as the language and design of the statute as a whole." *Id.* (quoting *K-Mart Corp. v. Cartier, Inc.*, 486 U.S. 281, 291 (1988)). "It is 'a cardinal principle of statutory construction' that 'a statute ought, upon the whole, to be so construed that, if it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant.'" *TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001) (quoting *Duncan v. Walker*, 533 U.S. 167, 174 (2001)). "Interpretation of a word or phrase depends upon reading the whole statutory text, considering the purpose and context of the statute, and consulting any precedents or authorities that inform the analysis." *Dolan v. U.S. Postal Serv.*, 546 U.S. 481, 486 (2006).

First, the plain language of subsection 2703(d) states that an order "*may* be issued by any court that is a court of competent jurisdiction." 18 U.S.C. § 2703(d) (emphasis added); *see In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 315-16 ("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." (citation omitted)).

The plain language of subsection 2703(d) also *prohibits* a court from issuing the statutory order if the government's application does not make out the statutory reasonable suspicion standard. The statute provides that an order "shall issue *only if* the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought[] are relevant and material to an ongoing criminal

investigation." 18 U.S.C. § 2703(d) (emphasis added). The best plain reading of this language is simply that an order *may not issue unless* the standard is met.[2] In other words, a showing of reasonable suspicion clearly is a necessary condition for the issuance of a § 2703(d) order, but not a sufficient condition. Contrary to the assertions of the government and the majority, nowhere does the statute by its terms *require* a court to issue a § 2703(d) order *whenever* the government's application demonstrates reasonable suspicion.

The Supreme Court has specifically contrasted the meanings of "whenever" and "only if," explaining that the latter "states a *necessary*, but not a *sufficient*, condition." *California v. Hodari D.*, 499 U.S. 621, 627-28 (1991). The Court reiterated this point in construing a statutory formulation similar to that here. In *Miller-El v. Cockrell*, 537 U.S. 322 (2003), the Court analyzed the language of 28 U.S.C. § 2253(c)(2), which governs the standard for issuance of a certificate of appealability ("COA") to a habeas petitioner. The Court explained:

> Section 2253(c)(2) . . . provides that "[a] certificate of appealability *may issue* . . . *only if* the applicant has made a substantial showing of the denial of a constitutional right." (Emphasis added.) A "substantial showing" does not entitle an applicant to a COA; it is a necessary and not a sufficient condition. Nothing in the text of § 2253(c)(2) prohibits a circuit justice or judge from imposing additional requirements, and one such additional requirement has been approved by this Court.

---

[2] *Cf. Barker v. Hercules Offshore*, 713 F.3d 208, 223 (5th Cir. 2013) (discussing "Congress's recent clarification of 28 U.S.C. § 1441(b)" whereby instead of stating that "'[a]ny other such action *shall be removable only if none* of the . . . defendants is a citizen of the State in which such action is brought,' the statute now explicitly specifies that a 'civil action otherwise removable solely on the basis of [diversity jurisdiction] *may not be removed if any* of the . . . defendants is a citizen of the State in which such action is brought" (emphasis omitted)); *Carver v. Lehman*, 558 F.3d 869, 876 n.12 (9th Cir. 2009) ("'May . . . only if' would be effectively identical to 'shall . . . unless'; 'may . . . if' is not." (elisions in original) (emphasis removed)).

Miller-El, 537 U.S. at 349 (second and third alterations in original). Other courts have applied this same understanding of "only if." *See Keweenaw Bay Indian Cmty. v. United States*, 136 F.3d 469, 475 (6th Cir. 1998) (explaining that under 25 U.S.C. § 2710(d)(1), which "provid[es] that Class III gaming activities 'shall be lawful on Indian lands *only if* such activities are . . . conducted in conformance with a valid Tribal–State compact,'" "[a] valid, approved compact is a necessary, but not a sufficient condition for Class III gaming"); *Williams v. Ward*, 556 F.2d 1143, 1158 n.6 (2d Cir. 1977) (characterizing the statutory formulations "release . . . shall . . . be granted . . . *only if* . . ." and "no prisoner shall be released on parole *unless* . . ." as both "phrased . . . as necessary rather than sufficient conditions" (emphasis added)). The Third Circuit's discussion of this point in its recent analysis of § 2703(d) is illustrative:

> [T]he "phrase 'only if' describe[s] a necessary condition, not a sufficient condition[.]' . . . [W]hile a 'necessary condition describes a prerequisite[,] a 'sufficient condition is a guarantee[.]' . . . [For] example[,] . . . 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." 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."

In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d at 317 (some alterations in original) (citations omitted) (quoting *Township of Tinicum v. U.S. Dep't of Transp.*, 582 F.3d 482, 489-90 (3d Cir. 2009)).

Following the government, the majority argues that this reading violates the superfluity canon by "ignor[ing]" the word "shall," Maj. Op. 10, in § 2703(d)'s statement that an "order may be issued by any court that is a court of competent jurisdiction and *shall* issue only if" reasonable suspicion is shown, 18 U.S.C. § 2703(d) (emphasis added). However, the government's own interpretation

renders superfluous the word "only" in the very same provision. That is, under the government's reading, the statute ought to simply say that an "order may be issued by any court that is a court of competent jurisdiction and shall issue . . . if the" government's application meets the statutory standard. *See id.*; *see also United States v. Nordic Village, Inc.*, 503 U.S. 30, 32 (1992) ("[It is a] settled rule that a statute must, if possible, be construed in such fashion that every word has some operative effect."); *Carver*, 558 F.3d at 876 n.12 ("The distinction between 'if' and 'only if[]' . . . is not a mere quibble over vocabulary — it goes right to the heart of whether [a condition is a] necessary or sufficient condition[] . . . .").

The government's argument would have some force if Congress had *actually* omitted the word "only" from the phrase "shall issue only if," as the government apparently believes Congress intended. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317 ("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."). Indeed, the warrant provision of the Federal Rules of Criminal Procedure — specifically adverted to in § 2703(c)(1)(A) and thus plainly part of the statutory context within which the text must be read[3] — would have served as a ready model. Rule 41 requires that "[a]fter receiving an affidavit or other information, a magistrate judge — or . . . authorized . . . judge of a state

[3] "It is a 'fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme.'" *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 133 (2000). Although "[t]he Federal Rules . . . are not enacted by Congress, . . . 'Congress participates in the rulemaking process,' and "the Rules do not go into effect until Congress has had at least seven months to look them over." *Bus. Guides, Inc. v. Chromatic Commc'ns. Enters., Inc.*, 498 U.S. 533, 552 (1991) (citation omitted) (citing 28 U.S.C. § 2074 (Rules Enabling Act)). Thus, courts "must assume that Congress [is] aware of th[e] [Federal] [R]ule[s] [of Criminal Procedure] when [legislation is] drafted." *United States v. Mitchell*, 723 F.2d 1040, 1046 (1st Cir. 1983); *see also, e.g.*, *United States v. Thompson*, 287 F.3d 1244, 1250 (10th Cir. 2002) ("Federal Rule of Criminal Procedure 6(f) sheds further light on the meaning of 'found' in 18 U.S.C. § 3282.").

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)(1) (emphasis added). Similarly, in a related section of Title 18, Congress explicitly provided for mandatory issuance of surveillance orders.[4] Section 3123 governs "[i]ssuance of an order for a pen register or a trap and trace device" and mandates that "upon an application" by a government attorney for such a device, "the court *shall* enter an ex parte order authorizing the installation and use of [the device], *if* the . . . information likely to be obtained . . . is relevant to an ongoing criminal investigation." 18 U.S.C. § 3123(a)(1) (emphasis added).[5] In rejecting the same interpretation of the statute advanced by the government here, the Third Circuit described "th[is] difference between 'shall . . . if' (for a pen register) and 'shall . . . only if' (for an order under § 2703(d))" as "a powerful argument to which the Government does not persuasively respond." *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 315-

[4] "We assume that Congress is aware of existing law when it passes legislation." *Miles v. Apex Marine Corp.*, 498 U.S. 19, 32 (1990). Additionally, "the meaning of one statute may be affected by other Acts." *Brown & Williamson Tobacco Corp.*, 529 U.S. at 133; *see also Green v. Bock Laundry Machine Co.*, 490 U.S. 504, 528 (1990) (Scalia, J., concurring) ("The meaning of terms on the statute books ought to be determined, [in part] . . . on the basis of which meaning is . . . most compatible with the surrounding body of law into which the provision must be integrated — a compatibility which, by a benign fiction, we assume Congress always has in mind."); *cf. Keene Corp. v. United States*, 508 U.S. 200, 208 (1993) ("[W]here Congress includes particular language in one section of a statute but omits it in another . . . , it is generally presumed that Congress acts intentionally in the disparate inclusion or exclusion." (alterations in original) (quoting *Russello v. United States*, 464 U.S. 16, 23 (1983))).

[5] This distinct "if . . . shall" formulation also appears in an analogous statute governing the issuance of orders for the production of records by judges of the Foreign Intelligence Surveillance Court. *See* 50 U.S.C. § 1861(c)(1) (providing that, upon government application for an order requiring the production of records for a counter-terrorism investigation, "*if* the judge finds that the application meets the [statutory] requirements" — including "a statement of facts showing that there are reasonable grounds to believe that the [records] sought are relevant to an authorized investigation" — the judge *shall* enter an ex parte order as requested" (emphasis added)).

16; *see also Carver*, 558 F.3d at 876 n.12 (noting the critical semantic "distinction between 'if' and 'only if'").

Accordingly, it cannot be said that the only plausible construction of the statute is that a magistrate must issue a § 2703(d) order whenever the government demonstrates reasonable suspicion. Because the statute is at least ambiguous as to when warrant procedures are to be followed, if the government's interpretation "raise[s] serious constitutional problems, [we must] construe the statute to avoid such problems unless such construction is plainly contrary to the intent of Congress." *Edward J. DeBartolo Corp. v. Fla. Gulf Coast Bldg. & Constr. Trades Council*, 485 U.S. 568, 575 (1988).

III

The government's interpretation raises the question of whether § 2703(c) offends the Fourth Amendment by authorizing law enforcement to obtain cell site location information without a warrant, which in turn depends on whether cellular customers have a reasonable expectation of privacy in that information. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 33 (2001) ("[A] Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." (citing *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)). This constitutes a "substantial constitutional question[]," *see St. Cyr*, 533 U.S. at 300, requiring application of the avoidance canon.

As the Eleventh Circuit recently observed, the Supreme Court has "underscore[d] its disinclination to establish broad precedents as to privacy rights vis-a-vis electronic devices and emerging technologies" because of "the difficulty in determining what privacy expectations are reasonable." *Rehberg v. Paulk*, 611 F.3d 828, 845 (11th Cir. 2010) (citing *City of Ontario v. Quon*, 130 S. Ct. 2619, 2630 (2010)). In *Quon*, the Supreme Court cautioned that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment

implications of emerging technology before its role in society has become clear." 130 S. Ct. at 2629. The Court avoided setting forth "[a] broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment." *Id.* at 2630. Instead, the Court held it "preferable to dispose of th[e] case on narrower grounds." *Id.* The Court achieved this narrower disposition by "assum[ing] several propositions *arguendo*," including that a municipal police officer "ha[s] a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City." *Id.* Particularly relevant here, the Court explained:

> In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. [*Katz*, 389 U.S. at 360-61 (Harlan, J., concurring).] It is not so clear that courts at present are on so sure a ground. . . . Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.

Quon, 130 S. Ct. at 2629.

Similarly, every member of the Court acknowledged last year that law enforcement's access to the location information generated by cell phones raises serious constitutional questions. *United States v. Jones*, 132 S. Ct. 945 (2012). In *Jones*, the Court unanimously held that attaching a global positioning system ("GPS") tracking device to a car and monitoring the car's movements without a valid warrant violated the Fourth Amendment, but divided in its reasoning. Notably, a majority eschewed engaging with the "particularly vexing problems" of applying a privacy analysis, *id.* at 953, and instead held that a search had occurred because of the trespass inherent in "physically occup[ying] private property for the purpose of obtaining information," *id.* at 949; *see also id.* at 950 ("The Government contends that . . . Jones had no 'reasonable expectation of privacy' in . . . the locations of the Jeep on the public roads, which were visible to all. But we need not address the Government's contentions, because Jones's

Fourth Amendment rights do not rise or fall with the *Katz* formulation."). The Court explained that even though "[i]t may be that [obtaining four weeks of location information] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, . . . [*Jones*] d[id] not require [the Court] to answer that question," which would "lead[] . . . needlessly into additional thorny problems." *Id.* at 953-54. The Court noted that "[it] may have to grapple with these 'vexing problems' in some future case." *Id.* at 954.

Justice Sotomayor cast the critical fifth vote in support of the majority opinion. However, her concurrence expressed serious doubt about extending the third party records doctrine applied in *Smith v. Maryland*, 442 U.S. 735 (1979)[6] — and relied upon by today's majority — to location information generated by modern devices such as "GPS-enabled smartphones." *Jones*, 132 S. Ct. at 955-57 (Sotomayor, J., concurring). Justice Sotomayor explained:

> [In future cases] considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements[,] . . . it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited

[6] *Smith* held that no Fourth Amendment "search" occurred, and thus "no warrant was required," when the government used a "pen register" to obtain the numbers that a telephone customer dialed because even if the customer "entertained [an] actual [i.e., subjective] expectation of privacy in the phone numbers he dialed, . . . his expectation was not 'legitimate,'" because the customer "voluntarily conveyed to [the phone company] information that it had facilities for recording and that it was free to record," such that the customer thereby "assumed the risk that the information would be divulged to police." 442 U.S. at 742-44 .

> purpose is, for that reason alone, disentitled to Fourth Amendment protection.

Id. at 957 (citations omitted); *see also id.* at 956 n.* ("Owners of GPS-equipped . . . smartphones do not contemplate that these devices will be used to enable covert surveillance of their movements."). Significantly, Justice Sotomayor explained that she "join[ed] the majority's opinion" "because the Government's physical intrusion on Jones' Jeep" made "[r]esolution of these *difficult questions* . . . unnecessary." *Id.* at 957 (emphasis added). Justice Alito, writing for four justices, expressed similar concerns. *See id.* at 963 (Alito, J., concurring in the judgment) ("Recent years have seen the emergence of many new devices that permit the monitoring of a person's movements. . . . Perhaps most significant, cell phones and other wireless devices now permit wireless carriers to track and record the location of users . . . . The availability and use of these and other new devices will continue to shape the average person's expectations about the privacy of his or her daily movements.").

Quon and *Jones* thus suggest that warrantless compulsion of cell site location records raises serious Fourth Amendment questions. The cautious approach taken by the Supreme Court makes clear that lower courts venture onto uncertain terrain in applying a reasonable expectation of privacy analysis to this law enforcement practice. Justice Sotomayor's decisive concurrence in *Jones* warns us not to "assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection." *See id.* at 957 (Sotomayor, J., concurring). "Although dicta, we do take such pronouncements from the Supreme Court seriously." *Croft v. Perry*, 624 F.3d 157, 164 (5th Cir. 2010). The divergent conclusions reached by the Third Circuit and today's majority starkly illustrate

this uncertainty.[7] In light of the difficulty of the constitutional question, "there is no reason for rushing forward to resolve [it] here." *See Jones*, 132 S. Ct. at 954. Rather, as in *Jones* and *Quon*, "[p]rudence counsels caution before . . . establish[ing] far-reaching premises that define the existence, and extent, of privacy expectations." *See Quon*, 130 S. Ct. at 2629.

IV

Because there is substantial doubt as to whether cell phone users have a reasonable expectation of privacy in cell site location information, it is not merely "preferable to dispose of this case on narrower grounds," *see id.*, but "incumbent upon us to read the statute to eliminate those doubts so long as such a reading is not plainly contrary to the intent of Congress," *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 78 (1994). "This cardinal principle has its roots in Chief Justice Marshall's opinion for the Court in *Murray v. The Charming Betsy*, 2 Cranch 64, 118 (1804), and has for so long been applied by th[e] [Supreme] Court that it is beyond debate." *Edward J. DeBartolo Corp.*, 485 U.S. at 575.

Rather than acknowledge this obligation, however the majority adopts the government's textually strained, constitutionally loaded construction after a cursory analysis; and boldly proceeds to pronounce upon the constitutional issue. The majority states that "we cannot avoid the [constitutional] question" because the district court below "held that all § 2703(d) orders for cell site information [are] unconstitutional." *See* Maj. Op. 11-12. However, this unsupported

[7] *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317-18 ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way. . . . [I]t 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.'" (final alteration in original)).

assertion is contrary to the Supreme Court's instruction that whatever the basis for a decision below, "we *must* independently inquire whether there is another interpretation, not raising . . . serious constitutional concerns, that may be fairly ascribed to [the statute]." *Edward J. DeBartolo Corp.*, 485 U.S. at 577 (emphasis added); *accord, e.g.*, *St. Cyr*, 533 U.S. at 299-300 ("[I]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is 'fairly possible,' *we are obligated* to construe the statute to avoid such problems." (emphasis added) (citations omitted)).[8]

As required by these precedents, I have endeavored to "ascertain whether a construction of the statute is fairly possible by which the constitutional question may be avoided." *See Sec. Indus. Bank*, 459 U.S. at 78. I conclude that such a construction is not only fairly possible, but better accords with the text, structure, and purpose of the statute than the government's interpretation.

V

A better interpretation is to read subsections 2703(c) and (d) together as implicitly directing that the warrant procedures incorporated into subsection 2703(c)(1)(A) are to be followed when law enforcement seeks records that may be protected by the Fourth Amendment. This alternative construction is both "plausible" and "fairly possible," *see Milavetz, Gallop & Milavetz, P.A. v. United States*, 130 S. Ct. 1324, 1334 (2010), and certainly is not "plainly contrary to the intent of Congress," *see X-Citement Video, Inc.*, 513 U.S. at 78; *Edward J. DeBartolo Corp.*, 485 U.S. at 575. Rather, this construction effectuates the text, structure, and purpose of the statute.

[8] Our obligation to "*independently* inquire" into plausible alternative interpretations, *see Edward J. DeBartolo Corp.*, 485 U.S. at 577 (emphasis added), is particularly pronounced in this ex parte proceeding.

For the reasons stated above, this alternative construction is not inconsistent with the ambiguous language of § 2703(d). Unlike the government's interpretation, this reading has the considerable virtue of "giv[ing] effect to all of th[e] [statute's] provisions." *See United States ex rel. Eisenstein v. City of New York*, 556 U.S. 928, 933 (2009). "[O]btain[ing] a warrant" is the first-listed procedure by which the government may seek to require the disclosure of non-content call records under § 2703(c). 18 U.S.C. § 2703(c)(1)(A). Subsection 2703(c)(1)(A) specifically adverts to the warrant "procedures described in the Federal Rules of Criminal Procedure" and "State warrant procedures." *Id.* § 2703(c)(1)(A); *see also, e.g.*, Fed. R. Crim. P. 41. The superfluity canon dictates that we should prefer a construction of § 2703(c) that gives meaning and significance to the warrant mechanism set forth in subsection 2703(c)(1)(A), rather than rendering this provision superfluous or insignificant. *See TRW Inc.*, 534 U.S. at 31. The construction I propose does precisely this, by construing subsection 2703(c)(1)(A) as applying when law enforcement seeks records that may be protected by the Fourth Amendment.

By contrast, the government's reading renders subsection 2703(c)(1)(A) largely insignificant if not entirely superfluous.[9] *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317 ("The Government's only retort to the argument that it

[9] I note that § 2703(d) provides that "[i]n the case of a State governmental authority, [a § 2703(d)] court order shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Thus, even under the government's reading, the "State warrant procedures" adverted to in § 2703(c)(1)(A) would presumably be utilized by the law enforcement agencies of such a state. However, because this limitation on the issuance of § 2703(d) orders applies only to "State governmental authorit[ies]," the government's construction nonetheless renders superfluous § 2703(c)(1)(A)'s specific citation to the warrant "procedures set forth in the Federal Rules of Criminal Procedure." *See* 18 U.S.C. § 2703(c)(1)(A). Moreover, the language of subsection 2703(c)(1)(A) is identical to the description of warrant procedures under subsection 2703(a), in which a warrant is the only means by which the government may obtain the contents of an email stored for 180 days or less. *See* 18 U.S.C. § 2703(a).

would never need to get a warrant under § 2703(c)(1)(A) if it could always get [cell site location information] 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.' In other words, the Government asserts that obtaining a warrant to get [cell site location information] 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." (elision in original) (citations to briefs omitted)).

This construction also accords with the larger structure of § 2703, which repeatedly categorizes records based on considerations of privacy and provides different and escalating mechanisms by which the government may access them. *See Brown & Williamson Tobacco Corp.*, 529 U.S. at 133 ("A court must . . . interpret [a] statute 'as a symmetrical and coherent regulatory scheme' and 'fit, if possible, all parts into an harmonious whole.'" (citations omitted)). First, subsection 2703(a) provides that the government "may require the disclosure by [an email service] of the contents of" a subscriber email stored for 180 days or less "only pursuant to a warrant." *See id.* § 2703(a). Under subsection 2703(b), the government may access the content of an email stored for longer than 180 days pursuant to either a subpoena or § 2703(d) order along with "prior notice . . . to the subscriber." *Id.* § 2703(a)-(b). Subsection 2703(c) then provides four different mechanisms by which the government may access non-content call records without customer consent. *Id.* § 2703(c). To require disclosure of more extensive and revealing types of non-content information, the government must employ increasingly formal procedures. At the most permissive end of this

hierarchy, a law enforcement agency conducting a telemarketing fraud investigation may obtain "the name, address and place of business of a subscriber who is engaged in telemarketing" using only "a formal written request" to the service provider. *Id.* § 2703(1)(D). To access somewhat more revealing customer information — such as a customer's "telephone connection records," "records of session times and durations," "length of service," "telephone or instrument number or other subscriber number or identity," and "means and source of payment" — the government must "use[] an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena." *Id.* § 2703(1)(E), (2). The government may seek information beyond such "essentially billing-related or business records," *In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d)*, 707 F.3d at 297 (Wilson, J., concurring), "*only when* [it] . . . obtains a warrant [or] . . . a [§ 2703(d)] order," 18 U.S.C. § 2703(c)(1)(A)-(B) (emphasis added). It accords with this statutory structure to construe subsection 2703(c)(1)(A)'s warrant provision — the most formal and exacting of the procedures described — as applying to those records that may be subject to Fourth Amendment protection.

Like the statutory language and structure, the legislative history suggests that Congress drafted § 2703(c) to be flexible enough to avoid constitutional concerns that might endanger the statute's validity. The Stored Communications Act was intended "to protect privacy interests in personal and proprietary information, while protecting the Government's legitimate law enforcement needs." S. Rep. No. 99-541, at 3 (1986) (Committee Report).[10] The drafters were explicitly mindful of the need for privacy protections to evolve with

[10] "In surveying legislative history [the Supreme Court] ha[s]repeatedly stated that the authoritative source for finding the Legislature's intent lies in the Committee Reports on the bill, which 'represen[t] the considered and collective understanding of those Congressmen involved in drafting and studying proposed legislation.'" *Garcia v. United States*, 469 U.S. 70, 76 (1984) (third alteration in original) (quoting *Zuber v. Allen*, 396 U.S. 168, 186 (1969)).

"dramatic changes in new . . . telecommunications technologies" such as "cellular . . . telephones." *See id.* at *1-2. The Committee Report stated:

> When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the [F]ourth [A]mendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions. . . .
>
> [T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id. at *1-2, 5 (1986). Congress was also mindful that "[i]n th[e] rapidly developing area of communications [such as] cellular non-wire telephone connections . . . , distinctions such as [whether there does or does not exist a reasonable expectation of privacy] are not always clear or obvious." *Id.* at *4 (final alteration in original).[11]

As Congress is well aware, "the Constitution invests the Judiciary, not the Legislature, with the final power to construe the law." *Nationwide Mut. Ins. Co. v. Darden*, 503 U.S. 318, 325 (1992). In drafting the Stored Communications Act, Congress certainly knew that a statute permitting law enforcement to access information about a suspect without a warrant or consent could be subject to constitutional challenge and potential invalidation. *See Marshall v. Barlow's, Inc.*, 436 U.S. 307 (1978) (holding statute unconstitutional insofar as it purported to authorize search without warrant or warrant equivalent); *Berger v. New York*, 388 U.S. 41 (1967) (holding facially unconstitutional statute

[11] *See also* H.R. Rep. No. 106-932, at 17 (2000) ("Currently, there are no clear legal standards governing when the government can collect location information from cell phone companies.").

authorizing issuance of orders for electronic eavesdropping without probable cause). The drafters of the Stored Communications Act were consciously engaged in an ongoing conversation between Congress and the Court regarding privacy protections. *See, e.g.*, S. Rep. No. 99-541, at 2 (1986) (citing *Berger*, 388 U.S. 41).[12]

"It is presumable that Congress legislates with knowledge of our basic rules of statutory construction," *McNary v. Haitian Refugee Ctr.*, 498 U.S. 479, 496 (1991), and the constitutional avoidance canon has long been recognized as "[']a cardinal principle' of statutory interpretation," *Zadvydas*, 533 U.S. at 689. Indeed, that canon "rest[s] on the reasonable presumption that Congress did not intend" its enactments to be construed so as to "raise[] serious constitutional doubts." *Clark*, 543 U.S. at 381. In § 2703(c), Congress appears to have created a framework capable of accommodating constitutional concerns that might arise by providing for the use of warrant procedures as a sort of safety valve by which such concerns could be avoided and thereby alleviated. Subsection 2703(c)(1)(A) strongly indicates that Congress intended warrant procedures to play a meaningful role in its legislative effort to balance "protect[ion] [of] privacy interests" with "legitimate law enforcement needs." *See* S. Rep. No. 99-541 at 3 (1986).[13]

---

[12] *See also Bartnicki v. Vopper*, 532 U.S. 514, 522-23 (2001) ("In *Berger*, we held that New York's broadly written statute authorizing the police to conduct wiretaps violated the Fourth Amendment. Largely in response to that decision, and to our holding in *Katz v. United States*, 389 U.S. 347 (1967), that the attachment of a listening and recording device to the outside of a telephone booth constituted a search, 'Congress undertook to draft comprehensive legislation both authorizing the use of evidence obtained by electronic surveillance on specified conditions, and prohibiting its use otherwise.[']").

[13] *See also In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317 n.8 ("In our experience, magistrate judges have not been overly demanding in providing warrants as long as the Government is not intruding beyond constitutional boundaries."); *cf. Johnson v. United States*, 333 U.S. 10, 13-14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement

In observing that the government's interpretation raises serious constitutional doubts and construing § 2703 in light of that observation, I take no position on the constitutional question of whether or when the Fourth Amendment itself would require the government to obtain a warrant for cell site location records. As the Supreme Court has emphasized, "the canon of constitutional avoidance . . . allows courts to *avoid* the decision of constitutional questions"; it "is not a method of adjudicating constitutional questions by other means." *Clark*, 543 U.S. at 381. In my view, we must accord Congress the respect inherent in "the reasonable presumption" upon which the avoidance canon rests, *see id.*, by reading the statute as adopted by a body mindful of the constitutional complexities of privacy legislation. Indeed, the legislative history reflects precisely such concerns. *See See* S. Rep. 99-541 at 1-5 (1986); *cf. Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."). Moreover, as the Supreme Court noted in *Clark*, "[i]t is not at all unusual to give a statute's ambiguous language a limiting construction called for by one of the statute's applications." *See Clark*, 543 U.S. at 380; *see also Zadvydas*, 533 U.S. at 689 ("We have read significant limitations into [numerous] statutes in order to avoid their constitutional invalidation.").[14]

---

agent."); *Jones*, 132 S. Ct. at 964 (Alito, J., concurring in the judgment) ("[W]here uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant.").

[14] In *Zadvydas*, the Court "read an implicit limitation into" an immigration detention statute, 8 U.S.C. § 1231(a)(6) (1994). 533 U.S. at 689. "[T]he Government[] argu[ed] that the statute . . . set[] no 'limit on the length of time beyond the removal period that an alien who falls within one of the [statutory] categories may be detained.'" *Id.* Applying the avoidance canon in light of a potential due process problem, the Court construed the statute as implicitly "limit[ing] an alien's post-removal-period detention to a period reasonably necessary to bring

VI

Having concluded that the statute is best construed as directing that warrant procedures be followed when the government seeks non-content records that may be protected by the Fourth Amendment, I would further hold that historical cell site location records constitute one example of this potentially protected information. Thus, I would hold that the government must obtain a warrant pursuant to § 2703(A)(1)(B) when it seeks to compel disclosure of historical cell site location data, because that individual data may be constitutionally protected.

The precise nature of the cell site location records sought in the present case is a matter of some dispute. In general, however, historical cell site location information appears to consist of, at minimum, a cellular service provider's records of which "cell sites" — i.e., "cell towers" or "base stations" mounted with antennae — a particular customer's cell phone has accessed over a particular period. The briefs submitted by the government and various amici provide different accounts of the precision of the information that such records contain. The magistrate judge below premised his Fourth Amendment analysis upon a series of "findings . . . based on expert testimony . . . given at a [June 2010] House Judiciary Subcommittee hearing . . . [intended] to educate Congress on the current state of location technology in the telecommunications industry." *In*

---

about that alien's removal from the United States." *Id.* In *Clark*, the Court applied the same limiting construction to all the statutory categories. 543 U.S. at 377-79.

Here, as with the statute construed in *Zadvydas* and *Clark*, it is not clear that Congress intended § 2703(c)'s statement that "[a] governmental entity *may* require a provider . . . to disclose [non-content customer] records" without the customer's consent "*only when* the governmental entity . . . obtains a warrant" or "a [§ 2703(d)] order," *see* 18 U.S.C. § 2703(c)(1) (emphasis added), to mean that the government has sole discretion as to when to follow warrant procedures. *See Zadvydas*, 533 U.S. at 697 ("We cannot find . . . any clear indication of congressional intent to grant the Attorney General the power to hold indefinitely in confinement an alien ordered removed. . . . The Government points to the statute's word 'may.' But while 'may' suggests discretion, it does not necessarily suggest unlimited discretion. In that respect the word 'may' is ambiguous.").

re Application of U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 830 (S.D. Tex. 2010) (Smith, M.J.). In particular, the magistrate judge looked to the testimony of Matt Blaze, "Associate Professor of Computer and Information Science, University of Pennsylvania." *Id.* at 830 n.13; *see also id.* at 831-33 nn. 7-28. A subsequent committee report summarized Professor Blaze's testimony at the June 2010 hearing as follows:

> Professor Blaze educat[ed] the Subcommittee on location technologies — specifically how different technologies interface with cell phones and locate their positions with varying degrees of specificity and precision in various types of environments, both indoors and out. Professor Blaze explained how, even if a network only records cell tower data (as opposed to GPS), the precision of that data will vary widely for any given customer over the course of a day and, for a typical user over time, some of that data will likely have locational precision similar to that of GPS. Indeed, in urban areas where providers are using microcell technology, the level of precision for cell tower location data can include individual floors and rooms within buildings.

H.R. Rep. No. 111-712, at 90 (2011).

The government disputes several of these assertions. As the majority acknowledges, however, it is undisputed that "the reason that the Government seeks such information is to locate or track a suspect in a criminal investigation" and that "[t]he data must be precise enough to be useful to the Government, which would suggest that, at least in some cases, it can narrow someone's location to a fairly small area." Maj. Op. 13. Moreover, there seems to be no serious question that the precision of these records is constantly increasing as cellular service providers construct ever denser networks of base stations and substations to keep pace with consumer demand and to comply with federal regulations requiring them to provide emergency dispatchers with increasingly precise coordinates for 911 calls placed by cell phone. *See* 47 C.F.R. § 20.18(h)(1). However, I will not attempt to wade into the empirical debate as

to whether or when network-based cell site location records will provide law enforcement with information regarding a suspect's location and movements that are equivalent to phone-based GPS location records.[15] Even were it possible to ascertain the nature of the records generated and stored by the various cellular service providers, such a determination is unnecessary here.

Although government access to cell site location information was not specifically envisioned or considered by Congress when it enacted the Stored Communications Act, presently these records appear to be the most personally revealing information that may be said to fall within § 2703(c)'s framework for the disclosure of "information pertaining to a subscriber or customer . . . not including the contents of communications." *See* 18 U.S.C. § 2703(c)(1). The general character of cell site location information and the purposes for which the government seeks it make it largely analogous to GPS location information, which the Supreme Court has indicated may implicate Fourth Amendment privacy interests. *See Jones*, 132 S. Ct. at 953-54; *id.* at 955-57 (Sotomayor, J., concurring); *id.* at 963-64 (Alito, J., concurring in the judgment).

Accordingly, I would hold that subsection 2703(c)(1)(A) applies to historical cell site location records, such that the statute requires the government to "obtain[] a warrant" to compel their disclosure. *See* 18 U.S.C. § 2703(c)(1)(A).

VII

The Third Circuit recently analyzed § 2703(c) without reference to avoidance principles. In contrast to today's majority, I agree with the Third Circuit that § 2703(c) is best read as not requiring a court to issue a § 2703(d)

[15] *Cf. Quon*, 130 S. Ct. at 2629 ("In *Katz*, the Court relied on its own knowledge and experience to conclude that there is a reasonable expectation of privacy in a telephone booth. It is not so clear that courts at present are on so sure a ground." (citation omitted)).

order whenever the government's application satisfies the statutory reasonable suspicion standard. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 314-17. However, the Third Circuit would give effect to subsection 2703(c)(1)(A) by instructing magistrates to determine whether to insist upon warrant procedures by engaging in a *Katz*-like inquiry that "balances the Government's need . . . for [cell site location] information with the privacy interests of cell phone users." *See id.* at 319.[16] Respectfully, it seems to me that this would require magistrates routinely to conduct a constitutional privacy analysis of the kind the Supreme Court has instructed courts to avoid whenever fairly possible.[17] In this respect, I believe that the Third Circuit failed to heed the Supreme Court's repeated admonitions regarding the difficulty and uncertainty of conducting this sort of privacy analysis at a time when communications technologies and our corresponding privacy expectations are both in flux.[18]

---

[16] The Third Circuit committed the same error as today's majority by unnecessarily pronouncing upon the ultimate constitutional question of whether cellular customers have a reasonable expectation of privacy in cell site location information. *See In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't*, 620 F.3d at 317-18.

[17] Similarly, the proposal set forth in Judge Tashima's Third Circuit concurrence is at odds with avoidance principles insofar as it suggests that magistrates should attempt to determine whether issuing a § 2703(d) order "would violate the Fourth Amendment absent a showing of probable cause." *See id.* at 320 (Tashima, J., concurring).

[18] *See Quon*, 130 S. Ct. at 2629; *see also Jones*, 132 S. Ct. at 962 (Alito, J., concurring in the judgment) ("The *Katz* expectation-of-privacy test . . . involves a degree of circularity and judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks. In addition, the *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes." (citations omitted)); *cf. Rehberg*, 611 F.3d at 846 ("[T]he questions of whether Fourth Amendment principles governing a search of [a suspect]'s home also should apply to subpoenas sent to a third-party [internet service provider (ISP)] for electronic data stored on the third-party's server, and whether [the suspect] had a reasonable privacy expectation in the contents of his personal emails sent voluntarily through

Moreover, ex parte application proceedings conducted in the absence of concrete investigative facts provide a poor vehicle for the development of Fourth Amendment doctrine. The *Quon* Court cautioned against using "the facts in [a single] case . . . to establish far-reaching" privacy principles. 130 S. Ct. at 2629. It seems to me even less prudent to set forth such principles in the context of an ex parte § 2703(d) application, in which there is literally *no factual record whatsoever*.[19] The speculative nature of this abstract constitutional analysis confirms that § 2703(c) is best construed to provide for warrant procedures when the government seeks information pertaining to individuals that may be constitutionally protected, such as historical cell site location records.

VIII

In sum, I conclude that the text of the Stored Communications Act is ambiguous as to when the government is to follow warrant procedures to compel

---

that third-party ISP, are complex, difficult, and 'far-reaching' legal issues that we should be cautious about resolving too broadly." (quoting *Quon*, 130 S. Ct. at 2629)).

[19] *See Sibron v. New York*, 392 U.S. 40, 59 (1968) ("The constitutional validity of a warrantless search is pre-eminently the sort of question which can only be decided in the concrete factual context of the individual case."); *Warshak v. United States*, 532 F.3d 521, 528 (6th Cir. 2008) (en banc) ("In determining the . . . the legitimacy of citizens' expectations of privacy, courts typically . . . reach[] case-by-case determinations that turn on the concrete, not the general, and offer[] incremental, not sweeping, pronouncements of law[,] . . . in two discrete, post-enforcement settings: (1) a motion to suppress in a criminal case or (2) a damages claim . . . against the officers who conducted the search. In both settings, the reviewing court looks at the claim in the context of an actual, not a hypothetical, search and in the context of a developed factual record of the reasons for and the nature of the search." (citations omitted)); Orin S. Kerr, Ex Ante Regulation of Computer Search and Seizure, 96 Va. L. Rev. 1241, 1281 (2010) ("[E]x ante predictions of reasonableness will be more error prone than ex post assessments [because] ex ante restrictions require courts to 'slosh [their] way through the factbound morass of reasonableness' without actual facts." (third alteration in original) (footnotes omitted) (quoting *Scott v. Harris*, 550 U.S. 372, 383 (2007))); *cf. Massachusetts v. EPA*, 549 U.S. 497, 517 (2007) (explaining that Article III standing doctrine works to "assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination" and "preserves the vitality of the adversarial process by assuring . . . that the legal questions presented . . . will be resolved, not in the rarified atmosphere of a debating society, but in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action" (second elision in original)).

disclosure of non-content customer call records. To resolve this ambiguity, I would apply the Supreme Court's constitutional avoidance jurisprudence. I would recognize that non-consensual, warrantless compulsion of customer cell site location records raises serious and debatable constitutional questions. In order to avoid these difficult questions, as we must if fairly possible, I would construe the statutory framework as implicitly directing that § 2703(c)(1)(A) warrant procedures be followed when the government seeks non-content records that may be constitutionally protected, including historical cell site location records. Thus, I would instruct magistrates to require the government to obtain a warrant pursuant to § 2703(c)(1)(A) when it seeks cell site location data. Accordingly, I would affirm the denial of the government's application to compel disclosure of such records here without consent or a warrant supported by probable cause, albeit on different grounds than those relied upon by the district court and magistrate judge. Therefore, and for the reasons set forth above, I respectfully dissent.