FOURTH AMENDMENT — WARRANTLESS SEARCHES — FIFTH CIRCUIT UPHOLDS STORED COMMUNICATIONS ACT'S NON-WARRANT REQUIREMENT FOR CELL-SITE DATA AS NOT PER SE UNCONSTITUTIONAL. — *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013).

The Fourth Amendment is traditionally understood to balance privacy and security.[1] But changes in technology[2] and the goals and methods of police work[3] have threatened to unsettle the meaning of the Fourth Amendment's protections.[4] The constitutional status of cell phones and the data they contain and produce is particularly contested.[5] Recently, in *In re Application of the United States for Historical Cell Site Data*,[6] the Fifth Circuit added an important new voice to this debate, holding that the Stored Communications Act[7] (SCA) provision allowing the government to demand cell-site location data[8] from service providers did not authorize a "search," and therefore that its lack of a warrant requirement was not per se unconstitutional. In reaching its holding, the Fifth Circuit assumed that its positive analysis — that cell phone users do not in fact expect their cell-site location data to be private — was dispositive of whether the Fourth Amendment's probable cause requirement ought to apply. It unwisely declined to apply a normative analysis asking whether location data *should* be protected by the Fourth Amendment. Both a recent Supreme Court case and relevant legislation could have signaled to the court that location data may warrant Fourth Amendment protections. Courts that review similar questions — including the Supreme Court[9] — should consider ask-

---

[1] *See, e.g.*, Zurcher v. Stanford Daily, 436 U.S. 547, 559 (1978) ("The Fourth Amendment has itself struck the balance between privacy and public need . . . .").

[2] *Compare* United States v. Wurie, 728 F.3d 1 (1st Cir. 2013) (holding that a warrantless search of a cell phone incident to arrest violated the Fourth Amendment, creating a circuit split), *with* People v. Diaz, 244 P.3d 501 (Cal. 2011) (upholding such a search), *cert. denied*, 132 S. Ct. 94 (2011).

[3] *See, e.g.*, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143–44 (2013) (discussing the Bush Administration's post-9/11 authorization of email surveillance under the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. §§ 1801–1885c (2006 & Supp. V 2011)).

[4] *Cf.* Carol S. Steiker, Response, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 830–44 (1994) (arguing that changes in police forces in addition to changing racial divisions spurred development of Fourth Amendment jurisprudence in the mid–twentieth century).

[5] *See Wurie*, 728 F.3d at 5 (noting that "[c]ourts have struggled to apply the Supreme Court's search-incident-to-arrest jurisprudence" to cell phones).

[6] 724 F.3d 600 (5th Cir. 2013).

[7] 18 U.S.C. §§ 2701–2712 (2012).

[8] The Fifth Circuit limited its holding to requests for data revealing the historical location of a cell phone only when "the user places and terminates a call." *In re Application*, 724 F.3d at 615.

[9] That the Fifth Circuit's decision created a circuit split, *see In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010), and that prominent amici, including Professor Orin Kerr, the

ing not only whether cell phone users do in fact expect privacy in their location data, but also whether they should.

In 2010, the United States submitted applications in three criminal investigations to Magistrate Judge Smith of the Southern District of Texas seeking to compel records from cell phone service providers.[10] The government requested historical cell-site location data for a two-month period detailing the location of certain cell phones to varying degrees of precision.[11] The United States' applications were filed under the SCA, which establishes that a court shall issue an order compelling disclosure of communications records if the government provides "specific and articulable facts" showing a reasonable belief that the records are relevant to an ongoing criminal investigation.[12]

Magistrate Judge Smith denied the United States' applications, finding that warrantless disclosure of cell-site data violates the Fourth Amendment based on three independent doctrines.[13] First, he held that "refinements in location-based technology" that allowed the government to trace suspects into their own homes could invade the privacy of the home in violation of the Fourth Amendment.[14] Second, he held that historical cell-site data was protected under the "prolonged surveillance doctrine" set forth by the D.C. Circuit in *United States v. Maynard*,[15] as that data can paint an "intimate picture" of a suspect's personal life.[16] Finally, he rejected the government's argument that the Fourth Amendment was inapplicable because cell phone users had disclosed voluntarily the data in question to service providers. Magistrate Judge Smith held that location information had not been "voluntarily conveyed" by the phone user to the service provider.[17]

ACLU, and the Electronic Frontier Foundation, submitted briefs in this case suggest that a similar case may be headed to the Supreme Court soon.

[10] *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 829 (S.D. Tex. 2010).

[11] *Id.* at 829, 833–35. In addition, the government submitted requests for other nonlocation data, which Magistrate Judge Smith granted. *See In re Application*, 724 F.3d at 602.

[12] 18 U.S.C. § 2703(d) ("A court order for disclosure [of information from a service provider] 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 records "are relevant and material to an ongoing criminal investigation.").

[13] *In re Application*, 747 F. Supp. 2d at 835–46. Magistrate Judge Smith had denied the requests in an earlier proceeding and invited the government to submit briefing on the legal issues related to cell-site location data. *Id.* at 829.

[14] *Id.* at 836 (citing United States v. Karo, 468 U.S. 705 (1984)). In *United States v. Karo*, 468 U.S. 705, the Supreme Court held that the government is not "completely free from the constraints of the Fourth Amendment" to determine, without a warrant, whether a particular person or thing is inside an individual's home. *Id.* at 716.

[15] 615 F.3d 544 (D.C. Cir. 2010).

[16] *Id.* at 563.

[17] *In re Application*, 747 F. Supp. 2d at 843. Thus, Magistrate Judge Smith reasoned, neither *United States v. Miller,* 425 U.S. 435 (1976), which held that individuals "lack . . . any legitimate

Judge Hughes issued a brief order upholding the Magistrate Judge's opinion.[18]

The Fifth Circuit vacated and remanded with instructions to grant the government's applications.[19] In an opinion by Judge Clement,[20] the court held that orders authorizing subpoenas for historical cell-site data under the SCA are not per se unconstitutional.[21] The court first considered whether it could avoid the constitutional issue.[22] The ACLU, an amicus curiae, had argued that the SCA could be read to afford a magistrate judge discretion to require that the government obtain a warrant, even where the government had met the "specific and articulable facts" standard under 18 U.S.C. § 2703(d).[23] The court rejected this statutory argument, breaking with the Third Circuit.[24] The SCA, Judge Clement explained, requires a magistrate judge to grant an application for cell-site records under § 2703(d) when the statutory requirements are satisfied; it leaves the magistrate judge no discretion to impose warrant procedures.[25]

The Fifth Circuit thus found itself compelled to answer the constitutional question: whether the Fourth Amendment bars the disclosure of historic cell-site records without a warrant, as the SCA allows. Judge Clement noted the differing lenses through which to view the case: the ACLU urged the court to focus on the *type* of information collected (that is, location), while the government argued that *who* was collecting the information (that is, private third parties) was the constitutional touchstone.[26] The court adopted the government's view.[27]

The Fourth Amendment's protections do not apply, the court reasoned, to information a private actor collects for its own purposes.[28]

---

expectation of privacy" in nonconfidential bank records held by their bank, *id.* at 442, nor *Smith v. Maryland,* 442 U.S. 735 (1979), which held that a suspect had no reasonable expectation of privacy in the numbers dialed from his home phone, *id.* at 745, governed. *In re Application*, 747 F. Supp. 2d at 843–44.

18 *In re Application*, 724 F.3d at 602–03.

19 *Id.* at 615.

20 Judge Clement was joined by Judge Reavley.

21 *In re Application*, 724 F.3d at 615.

22 The court also addressed two jurisdictional hurdles raised by Kerr: First, the court found that the issue was ripe because the case presented "pure questions of law" and was the "only time that the Government [could] challenge the denial of its order." *Id.* at 604. Second, the court held that it had appellate jurisdiction under 28 U.S.C. § 1291 because Magistrate Judge Smith's denial of the application was a final order in that "denying or granting the order finally disposes of the proceeding." 724 F.3d at 605. The court found it unnecessary to decide whether Magistrate Judge Smith's use of judicial notice was improper, as the government claimed. *Id.* at 615 n.14.

23 *In re Application*, 724 F.3d at 606.

24 *Id.* at 607–08. The Third Circuit had held that the SCA gives magistrate judges discretion to require a warrant. *In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010).

25 *In re Application*, 724 F.3d at 607–08.

26 *Id.* at 608–09.

27 *Id.* at 610.

28 *Id.*

An individual doing business with third parties who "knowingly exposes his activities . . . surrenders Fourth Amendment protections."[29] As long as the third party has a legal right to control the records, the government may issue a warrantless demand to that third party for the records without implicating the Fourth Amendment.[30]

The court concluded that cell-site location data are unprotected business records because the records are created by the cell service provider,[31] the records memorialize transactions to which the provider is a party,[32] the government does not require or encourage the preparation or retention of such records,[33] and the user voluntarily conveys the data to the service provider.[34] According to the court, therefore, the protections afforded business records depend not primarily on the expectations of the user, but rather on the actions and policies of the service provider. The SCA, Judge Clement concluded, represents Congress's best attempt at "balancing . . . privacy and safety"[35] and any change in that balance must come from the legislature.[36]

Judge Dennis dissented, arguing that the court should have decided the appeal "by adhering to the Supreme Court's constitutional question avoidance doctrine," which would counsel in favor of a reading of the SCA obliging magistrate judges to require a warrant.[37]

The Fifth Circuit adopted too limited a role for itself by assuming that, in applying the business-records doctrine, it should conduct only a positive analysis focused on whether individuals do in fact have an expectation of privacy in their cell-site location data. Rather, Supreme Court jurisprudence counsels that, in certain cases, courts should also conduct a normative analysis, asking whether the data at issue *should* be protected by the Fourth Amendment. The Supreme Court's decision in *United States v. Jones*[38] and the Wireless Communication and Public Safety Act of 1999[39] (WCPSA) gave the Fifth Circuit two good reasons to think that a normative analysis was necessary and that cell-

---

[29] *Id.* (quoting Reporters Comm. for Freedom of the Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1043 (D.C. Cir 1978) (emphasis omitted)).

[30] *Id.* at 611.

[31] *Id.* at 611–12.

[32] *Id.* at 612 ("[T]hese are the providers' own records of transactions to which it is a party.").

[33] *Id.* (citing United States v. Jones, 132 S. Ct. 945, 961 (2012) (Alito, J., concurring in the judgment)).

[34] *Id.* at 613–14. *Contra In re* Application of the United States for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (holding that location data is not voluntarily conveyed); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 756–57 (S.D. Tex. 2005) (same).

[35] *In re Application*, 724 F.3d at 615.

[36] *Id.* at 614–15.

[37] *Id.* at 615 (Dennis, J., dissenting); *see id.* at 615–17.

[38] 132 S. Ct. 945.

[39] Pub. L. No. 106-81, 113 Stat. 1286 (codified as amended in scattered sections of 47 U.S.C.).

site location data falls within the Fourth Amendment's protections under such an analysis.

The Supreme Court's reasonable expectation of privacy jurisprudence has recognized that a normative inquiry may be necessary even if an individual lacks an actual expectation of privacy. Such an inquiry is necessary where, despite the mere fact of "interceptibility," communications ought nevertheless to be private.[40] In *Katz v. United States*,[41] the Supreme Court found warrantless wiretapping of a telephone booth to be a violation of the Fourth Amendment based on both positive and normative inquiries. The Court did not confine its reasoning to whether individuals did in fact expect privacy in a phone booth.[42] Rather, the Court took heed of the "vital role that the public telephone has come to play in private communication" to determine the scope of the Fourth Amendment's protections.[43] The Court recognized that a normative assessment — asking what expectations of privacy society ought to protect — was its crucial task.[44] Justice Harlan's concurrence, which first set out the two-pronged "reasonable expectation of privacy" doctrine, also stressed that the Fourth Amendment's scope would be tested not only against an "actual (subjective) expectation of privacy," but also against normative measures of what society deems worthy of privacy protections.[45]

In *Smith v. Maryland*,[46] the Supreme Court further developed the idea that limiting Fourth Amendment analysis to whether an individual has an actual expectation of privacy may lead to "inadequate" privacy protections, and that a normative inquiry may be necessary.[47]

---

[40] *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 28 (explaining how, at the time of *Katz v. United States*, 389 U.S. 347 (1967), it was well known that telephone communications were vulnerable to wiretapping — such that one might not have an actual expectation of privacy — but that such communications were deemed worthy of protection by the Court).

[41] 389 U.S. 347.

[42] *Id.* at 352 (holding that one using a phone booth is "surely entitled to assume" that his conversation will be private); *see also In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 845 (S.D. Tex. 2010) ("But the bare possibility of disclosure by a third party cannot by itself dispel all expectation of privacy. Otherwise, nothing would be left of *Katz,* because it was surely possible in 1967 for the phone company to wiretap and disclose a private conversation in a public phone booth.").

[43] *Katz*, 389 U.S. at 352.

[44] *See* Freiwald, *supra* note 40, ¶¶ 32–33, 40, 44 (explaining that *Katz* suggests a normative analysis that courts have improperly ignored).

[45] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[46] 442 U.S. 735 (1979).

[47] *Id.* at 740 n.5. For an example of the Court applying a normative analysis in the third-party context, see *United States v. Miller*, 425 U.S. 435 (1976), in which the Court held the Fourth Amendment did not apply, but only after "examin[ing] the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents," *id.* at 442.

The *Smith* Court recognized that there are situations in which individuals "might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects" because of "influences alien to well-recognized Fourth Amendment freedoms," but where a court's normative inquiry would reveal that the Fourth Amendment *should* apply nonetheless.[48] The Court recognized that cabining the Fourth Amendment to protect only expectations of privacy individuals actually hold would erode the Fourth Amendment's protections, as individuals' awareness of government searches and seizures would serve to legitimize those very same invasions.[49]

Ignoring these lessons from *Katz* and *Smith*, the Fifth Circuit declined to conduct a normative analysis. The court instead assumed that the positive question was dispositive; that is, because individuals knew that their location data was transmitted to the phone company, they could not reasonably expect privacy in that data.[50] Even assuming the Fifth Circuit correctly assessed actual expectations of privacy, which is an open question,[51] that assessment was insufficient. As *Katz* and *Smith* both show, the mere fact that an individual does not have a subjective expectation of privacy does not preclude Fourth Amendment protections. The court missed an opportunity to consider whether the *type* of information transmitted to a third party might affect the Fourth Amendment's reasonable expectation of privacy analysis in the third-party context.

The court had two good reasons to find that cell-site location data warrants protections, whether individuals actually expect privacy in that data or not. First, *Jones* highlights the particularly sensitive nature of location tracking. There, the Court considered the constitutionality of law enforcement attaching a Global Positioning System (GPS) device to the car of a criminal suspect without a valid warrant and the subsequent use of GPS to monitor the suspect's location.[52] The majority, though focused on the common law trespass committed against the suspect, nevertheless recognized that location tracking could be problematic, even absent such a physical trespass.[53] The reasoning of Justices Alito and Sotomayor, who each filed concurrences,

---

[48] *Smith*, 442 U.S. at 740 n.5.

[49] *See* Freiwald, *supra* note 40, ¶ 27 (noting the "impermissible shortcut" taken by post-*Katz* courts, which have relied on a "fact-of-interceptibility" analysis to refuse to find any reasonable expectation of privacy "unless the public views those communications as invulnerable to acquisition").

[50] *See In re Application*, 724 F.3d at 613.

[51] *See, e.g.*, *In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 844–45 (S.D. Tex. 2010) (noting that while "tech-savvy" users may know that cell phones transfer location data to providers, *id.* at 845, nevertheless location data is not "'knowingly exposed' or 'voluntarily conveyed' . . . as those phrases are ordinarily understood," *id.*).

[52] United States v. Jones, 132 S. Ct. 945, 948 (2012).

[53] *Id.* at 953–54.

illustrates the normative assessment that there are situations in which location data ought to be private; Justice Scalia, writing for the majority, did not dismiss this possibility.[54] Justice Scalia noted that "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to" the reasonable expectation of privacy test established in *Katz*[55] and might be "an unconstitutional invasion of privacy."[56] Justice Sotomayor also explained that location-based tracking has uniquely pernicious effects[57] and suggested that the third-party doctrine may be "ill suited to the digital age."[58] The Fifth Circuit too quickly dismissed *Jones* in its analysis, assuming that *Jones* was distinguishable because it addressed government-initiated surveillance and not records subpoenaed from a third party.[59] The Fifth Circuit missed the opportunity to consider whether, according to the reasoning of *Jones*, Fourth Amendment protections should apply to cell-site location data, even though they are collected by a third party.

Second, Congress signaled in the WCPSA that cell-site location data are not normal business records.[60] In relevant part, the WCPSA establishes that "a customer shall not be considered to have approved the use or disclosure of or access to" cell phone location data,[61] and bars cell-service providers from disclosing "individually identifiable customer proprietary network information" except as required by law or with customer approval.[62] The WCPSA thus suggests that Congress intended that individuals' privacy interest in location data be given particular weight in privacy assessments.[63] Whereas the SCA speaks of communications records generally, it does not specifically address location data;[64] the WCPSA, enacted subsequently, does.[65] Moreover, the language of the WCPSA, which establishes that custom-

---

54 At least five Justices accepted that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* at 955 (Sotomayor, J., concurring) (quoting *id.* at 964 (Alito, J., concurring in the judgment)) (internal quotation marks omitted). Even Justice Scalia acknowledged this possibility. *See id.* at 953–54 (majority opinion).

55 *Id.* at 953.

56 *Id.* at 954.

57 *See, e.g.*, *id.* at 956 (Sotomayor, J., concurring) ("[T]he Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.").

58 *Id.* at 957.

59 *In re Application*, 724 F.3d at 609–10.

60 *See In re* Application of the United States for Historical Cell Site Data, 747 F. Supp. 2d 827, 841–42 (S.D. Tex. 2010) (noting that the WCPSA establishes that cell-site data is "not a proprietary business record subject to unfettered corporate control," *id.* at 841).

61 47 U.S.C. § 222(f) (2006 & Supp. V 2011).

62 *Id.* § 222(c)(1). This information includes location data. *See id.* § 222(h)(1).

63 *See In re Application*, 747 F. Supp. 2d at 842 ("[A]n act of Congress affecting [a] proprietary interest in a thing is undeniably relevant to the legitimate-expectation-of-privacy inquiry.").

64 *See* 18 U.S.C. § 2703(b)–(c) (2012) (referring to content and noncontent communications records, but making no mention of location data).

65 *See* 47 U.S.C. § 222(f).

ers "shall not be considered to have approved" disclosure of location data,[66] suggests courts cannot apply standard third-party analysis, which depends on assuming customers *have* consented to disclosure.

Thus, given the protections the WCPSA affords to cell-site location data, it could have informed a normative analysis had the Fifth Circuit conducted one. Using the WCPSA as a basis for such a normative analysis would hardly be novel: the Supreme Court has previously looked to acts of Congress to inform normative analyses of just the kind the Fifth Circuit avoided.[67] Moreover, other courts already have recognized that the WCPSA sends a strong signal to protect cell phone location data.[68] The Fifth Circuit should have recognized the possibility that, by designating cell-site location records as particularly sensitive, Congress signaled that individuals ought to be able to expect privacy in their cell-site data.

The court unnecessarily assumed that individuals' voluntary submission of cell location data to third parties, demonstrating no *subjective* expectation of privacy in that information, was conclusive. Supreme Court jurisprudence suggests the third-party doctrine may not always by itself resolve the application of the Fourth Amendment to sensitive information. Rather, courts must engage in a more difficult task, asking whether government intrusion "alter[s] the relationship between citizen and government in a way that is inimical to democratic society."[69] The Fifth Circuit missed an opportunity to modulate the breadth of the business-records doctrine, which, in the face of technological change, will have to give or else swallow privacy whole.[70]

---

[66] *Id.*

[67] *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 123 (1984) (looking to congressional treatment of cocaine possession to determine the legitimacy of an individual's privacy interest in a substance suspected to be cocaine); United States v. Miller, 425 U.S. 435, 442–43 (1976) (looking to a law related to bank secrecy to determine the legitimacy of expectations of privacy in bank records).

[68] *See, e.g.*, *In re* Application of the United States for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 552 (D. Md. 2011) (finding WCPSA counseled in favor of requiring probable cause before allowing government access to prospective cell phone location data); *In re* Application for Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 757 (S.D. Tex. 2005) ("Based on [the WCPSA], a cell phone user may very well have an objectively reasonable expectation of privacy in his call location information.").

[69] United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)) (internal quotation marks omitted).

[70] *See* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461 (2000) (discussing the ubiquity of public and private surveillance and its implications for privacy); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002) (noting the increasing detail available in "digital dossiers" created privately and the implications for government surveillance). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561 (2009).