FOURTH AMENDMENT — THIRD-PARTY DOCTRINE — FOURTH CIRCUIT HOLDS THAT GOVERNMENT ACQUISITION OF HISTORICAL CELL-SITE LOCATION INFORMATION IS NOT A SEARCH. — *United States v. Graham*, 824 F.3d 421 (4th Cir. 2016) (en banc).

The Supreme Court has held that people cannot reasonably expect privacy in information they willingly disclose to third parties and, thus, that government intrusions on such information are not Fourth Amendment searches.[1] Lower courts have also held that historical cell-site location information (CSLI) — a carrier's records of the cell tower used to route a user's calls and messages (typically the tower closest to the user)[2] — is such information willingly disclosed to third parties.[3] Recently, in *United States v. Graham*,[4] the Fourth Circuit upheld that rule, finding that two defendants could not reasonably expect privacy in CSLI that police used to place them at the crime scene. That holding shows the third-party doctrine's flaw: in its focus on categorizing behavior, it does not accurately estimate what society today would consider reasonable. Courts should update the doctrine to reflect our complex and changing relationship with technology.

Aaron Graham and Eric Jordan were prosecuted for six armed robberies in Baltimore that occurred over the course of several weeks in early 2011.[5] The fifth and sixth robberies took place on the same afternoon. Based on eyewitness testimony, the police arrested Graham and Jordan; they then acquired physical evidence connecting the defendants to two of the earlier robberies.[6] While investigating those robberies, an officer seized (under warrant) two phones from Graham's car, linking them to the phone numbers Graham and Jordan gave at arrest.[7] The police sought court orders through the Stored Communications Act[8] (SCA), under which the government may compel disclosure of certain records under a standard lower than probable cause.[9] They demanded that Sprint/Nextel (the defendants' phone carrier) provide the historical CSLI associated with the defendants' phones for a total of 221 days over seven months, collecting over 28,000 CSLI data points for each defendant.[10] Prosecutors used CSLI to place the defendants at most of the crime scenes.[11]

---

1 *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
2 United States v. Graham, 796 F.3d 332, 343 (4th Cir. 2015).
3 *See, e.g.*, United States v. Carpenter, 819 F.3d 880, 887–89 (6th Cir. 2016).
4 824 F.3d 421 (4th Cir. 2016) (en banc).
5 *Graham*, 796 F.3d at 338–39.
6 *See id.* at 340–41.
7 *Id.* at 340.
8 18 U.S.C. §§ 2701–2712 (2012).
9 United States v. Graham, 846 F. Supp. 2d 384, 396 (D. Md. 2012) (citing 18 U.S.C. § 2703(d)).
10 *Graham*, 796 F.3d at 341, 350.
11 *Id.* at 342–43.

Graham and Jordan brought a motion to suppress the CSLI as the fruit of an unconstitutional search.[12] The district court concluded that the defendants could not legitimately expect privacy in their historical CSLI records as they voluntarily conveyed that information to Sprint/Nextel; the third-party doctrine thus applied.[13] In the alternative, the court held that because the government had relied on the SCA orders in good faith, it could use the CSLI without triggering the exclusionary rule.[14] Accordingly, the court rejected the motion, and the defendants were then convicted following a jury trial. They appealed, arguing that the government, by obtaining the CSLI, had violated their Fourth Amendment rights.[15]

A panel of the Fourth Circuit agreed. Writing for the panel, Senior Judge Davis[16] held that the government invades an individual's reasonable expectation of privacy (and thus conducts a Fourth Amendment search) when it examines historical CSLI for an extended period of time.[17] Judge Davis rejected the government's claim that the carrier's privacy policy showed that the defendants did not expect privacy in their CSLI, as the policy said that the company *collects*, rather than discloses, information; users also rarely read those policies.[18] He next held that the third-party doctrine cannot apply to CSLI.[19] Users, he wrote, do not *voluntarily* convey location information to phone carriers.[20] Judge Davis also rejected the argument that CSLI is noncontent, or merely the information necessary to get content from point A to B,[21] which has traditionally merited less Fourth Amendment protection.[22] CSLI is more than the basic routing information that has been deemed digital noncontent; rather, it connects location to time.[23] However, the court's ruling that the Fourth Amendment applies to

---

[12] *Id.* at 341. When the government rested, the defendants made several motions based on evidentiary insufficiency; the court denied all but one, which was granted with respect to Jordan. *Id.* at 341–42.

[13] *Graham*, 846 F. Supp. 2d at 389, 400.

[14] *Id.* at 405–06.

[15] *Graham*, 796 F.3d at 342–43. They also contested the court's admission of certain lay testimony. *Id.* at 363. Jordan argued that the court should not have restricted his testimony, denied his severance motion, or excluded Graham's out-of-court statements. He also made arguments based on insufficiency of the evidence. *Id.* at 342. The panel rejected these arguments, *id.* at 364, 366, 369–70, 372–73, and the en banc court adopted those holdings, *Graham*, 824 F.3d at 424 n.1.

[16] Judge Davis was joined by Judge Thacker, who wrote separately to underscore privacy's importance in an "era of rapid technological development." *Graham*, 796 F.3d at 377 (Thacker, J., concurring).

[17] *Id.* at 344–45 (majority opinion).

[18] *Id.* at 345.

[19] *Id.* at 353.

[20] *Id.* at 352–54.

[21] *See* United States v. Carpenter, 819 F.3d 880, 886 (6th Cir. 2016) (defining noncontent).

[22] *Graham*, 824 F.3d at 433–34, 433 n.12.

[23] *Graham*, 796 F.3d at 358.

CSLI did not lead it to exclude the evidence — it affirmed Jordan's and Graham's convictions under the exclusionary rule's good faith exception.[24] Judge Motz dissented in part, concluding that the defendants voluntarily shared their CSLI with third parties and therefore could not reasonably expect privacy in it.[25]

Sitting en banc, the Fourth Circuit reversed the panel's Fourth Amendment holding.[26] Now in the majority, Judge Motz[27] first wrote that the third-party doctrine applies even to information conveyed for limited purposes.[28] She then observed that the state activity in question was not direct surveillance, but rather government acquisition of data that a carrier "created and maintained in the normal course of [its] business."[29] By using their phones, the defendants "assumed the risk" that the carrier would transmit that information to the government.[30] Judge Motz next rejected the defendants' argument that the information was not "voluntarily conveyed."[31] Cell users are aware that location matters because location determines reception, she wrote. By choosing to use cell phones despite that knowledge, she argued, users voluntarily convey to carriers their location information.[32]

Judge Motz then noted that courts have never attached significance to whether an individual has actively chosen to share her information; those courts upheld warrantless "trap and trace" devices, which allow the government to record the phone numbers of unsolicited incoming calls.[33] Users also cannot have an expectation of privacy in noncontent information, she wrote, citing non-CSLI cases that relied on the fact that defendants had used third-party equipment.[34] Judge Motz then rejected the defendants' argument that not using a phone requires someone to "opt out of modern society";[35] dissenters in other landmark third-party doctrine cases had raised similar arguments that the Supreme Court rejected.[36] Judge Motz distinguished the defendants' ar-

---

[24] *Id.* at 362.

[25] *Id.* at 378 (Motz, J., dissenting in part and concurring in the judgment).

[26] *Graham*, 824 F.3d at 424. The en banc court also ultimately affirmed the convictions. *Id.*

[27] Judge Motz was joined by then–Chief Judge Traxler and Judges Wilkinson, Niemeyer, King, Gregory, Shedd, Duncan, Agee, Keenan, Diaz, and Harris.

[28] *Graham*, 824 F.3d at 425 (citing United States v. Miller, 425 U.S. 435, 443 (1976)).

[29] *Id.*

[30] *Id.* at 427 (quoting Smith v. Maryland, 442 U.S. 735, 744 (1979)).

[31] *Id.* (quoting *Smith*, 442 U.S. at 744).

[32] *Id.* at 430.

[33] *Id.* at 431.

[34] *Id.* at 432 (citing United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008) (holding that internet users have no reasonable expectation of privacy in the IP addresses of websites they visit)).

[35] *Id.* (quoting Defendants'/Appellants' Supplemental En Banc Brief at 11, *Graham*, 824 F.3d 421 (No. 12-4659)).

[36] *Id.* at 433 (citing United States v. Miller, 425 U.S. 435, 451 (1976) (Brennan, J., dissenting); *Smith*, 442 U.S. at 750 (Marshall, J., dissenting)).

gument as relying on cases establishing restrictions on *content*, whereas CSLI is noncontent information meriting less protection.[37] Judge Motz next addressed the "mosaic theory"[38] argument that while small acquisitions of CSLI might not cross the "search" threshold, large-scale acquisitions often do. That analysis, she wrote, misunderstood *United States v. Jones*[39] and its two concurrences. In *Jones*, Justices Alito and Sotomayor seemed open to the mosaic theory.[40] But Judge Motz distinguished *Jones* as it involved *direct* surveillance.[41] People expect more privacy when government uses technology to do what it cannot otherwise do directly than they expect in the business records of third parties.[42] A person's expectation of privacy in the material she shares with third parties does not change because she has shared a lot of it.[43] Judge Motz sympathized with the idea that technology has changed society's expectations of privacy but felt bound by the Supreme Court; only the Court or Congress, she concluded, could reverse course.[44]

Judge Wilkinson concurred, writing that decisions regarding the Fourth Amendment's privacy protections should be left to Congress.[45] Judge Wynn[46] dissented in part, arguing that cell phone users do not truly "voluntarily convey[]" their CSLI to third parties.[47] He saw two commonalities in the cases establishing the third-party doctrine: in each, the defendant had *known* he was transmitting the information and had *acted* to submit it.[48] Both elements, he found, are missing in the case of CSLI. Cell phone users do not know about the CSLI shared by their phones, and they take no discrete action in order to convey it (aside from mere use).[49] Judge Wynn concluded that the size of the acquisition decided the case.[50] Although CSLI is less precise than GPS data, the government had acquired a large enough set of data to detect patterns, meriting constitutional protection.[51]

---

[37] *Id.*

[38] Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) (describing the mosaic theory).

[39] 132 S. Ct. 945 (2012).

[40] *See id.* at 964 (Alito, J., concurring in the judgment); *id.* at 955 (Sotomayor, J., concurring).

[41] *Graham*, 824 F.3d at 435. *Jones* involved a GPS tracker that officers warrantlessly installed on the defendant's car. 132 S. Ct. at 948.

[42] *Graham*, 824 F.3d at 435.

[43] *Id.* at 436.

[44] *Id.* at 436–37.

[45] *See id.* at 438 (Wilkinson, J., concurring).

[46] Judge Wynn was joined by Judges Floyd and Thacker.

[47] *Graham*, 824 F.3d at 442 (Wynn, J., dissenting in part and concurring in the judgment).

[48] *Id.* at 443.

[49] *Id.* at 444–45.

[50] *Id.* at 447.

[51] *Id.* at 447 & n.12. He also criticized the majority's overbroad holding, *see id.* at 448–49, but concurred in the judgment under the good faith exception to the exclusionary rule, *id.* at 441 n.1.

Graham is consistent with recent applications of the third-party doctrine: the defendants disclosed information to third parties, so they get no privacy protections.[52] But *Graham* shows that courts have shifted from trying to estimate what society really would consider reasonable, as they did in the cases establishing the third-party doctrine, to substituting a doctrinally constructed determination of reasonableness through the third-party doctrine. There is a space between that doctrinal expectation and what society would consider reasonable in a world of emerging technology, and courts ought to update the doctrine to reflect that.

The approach courts took in the earliest third-party doctrine cases came closer to an attempted estimate of society's real expectations. In *United States v. Miller*,[53] a seminal third-party doctrine case, the government subpoenaed copies of the defendant's checks and deposit slips.[54] The Court rejected Miller's claim that as he had disclosed those bank records only for the bank's use, he had retained his reasonable expectation of privacy in them.[55] But the Court did not reject his claims by mechanically labeling his information as third-party records. Rather, it examined "the nature of the particular documents sought to be protected" to determine whether Miller could have reasonably expected privacy in them.[56] In the Court's analysis, that nature *mattered*. The Court found it significant that the documents in question were not sensitive in nature or shared with the intent that they stay private; rather, they were commercial instruments any employee could see.[57] That, rather than their third-party nature, was why Miller — and by extension society — could not legitimately expect privacy in them.[58]

Graham also relied on *Smith v. Maryland*,[59] in which the Court established the third-party doctrine as a per se rule and thus took one step further from *Miller*'s more measured approach. But even once it applied the doctrine, the Court still explained why society would not recognize the defendant's expectation as reasonable. As Rebecca Lipman has argued, *Smith*'s conclusion was "narrower" than its categorical rule, depending instead on a fact-intensive analysis.[60] The

---

[52] *See, e.g.*, United States v. Davis, 785 F.3d 498, 511–12 (11th Cir. 2015) (en banc).

[53] 425 U.S. 435 (1976).

[54] *Id.* at 442. Miller was convicted of running an illegal distillery and of tax fraud. *See id.* at 436.

[55] *Id.* at 442.

[56] *Id.*

[57] *See id.*

[58] *See id.* at 442–43; *see also* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681, 734–35 (2011) (arguing that it was the "nature of the records themselves," *id.* at 734, that defeated Miller's privacy expectations).

[59] 442 U.S. 735 (1979).

[60] *Compare* Rebecca Lipman, Note, *The Third Party Exception: Reshaping an Imperfect Doctrine for the Digital Age*, 8 HARV. L. & POL'Y REV. 471, 475 (2014), *with Smith*, 442 U.S. at 743–44.

Court noted that the only difference between the defendant reading phone numbers to an operator, which he conceded was not private, and him dialing the numbers himself was automation.[61] In both *Miller* and *Smith*, that the records were disclosed to third parties was the beginning, not the end, of the Court's analysis.[62] The *Graham* court simply argued that the defendants had assumed a risk through transmitting information to third parties; it did not ask *why* society would agree.

That lack of analysis matters, as society *does* expect privacy in some third-party records, especially sensitive data (like CSLI) shared with technology companies. Studies show that people do not expect less privacy in third-party records as a class: rather, "the important variable appears to be the nature of the record, not who or what institution possesses it."[63] CSLI is that kind of uniquely invasive data; as Professor Susan Freiwald puts it, "[b]etween the availability of duration and registration data and the possibility that location data will be recorded when cell phone users send text messages or browse the Internet, it seems clear that [CSLI] creates a much more detailed picture of a person's movements" than police ever had before.[64] CSLI is more sensitive, in fact, than the noncontent, or "envelope," information that courts have traditionally protected less.[65] Consider this: The outside of an envelope tells police the zip code where the sender was located on one day. In effect, historical CSLI tells police not only that the sender was in one zip code on one day, but also at what mailbox and at what time. And it does that not just for one letter, but for many letters over long time spans. Some argue that the third-party doctrine has always been out of step with society's expectations of privacy.[66] But the fact is that we don't think of cell phones the way we thought of letters and papers. As the Court recently observed, new technologies raise vitally different questions than do facially similar analogues.[67] And like the GPS data in *Jones*, CSLI tells police an extraordinary amount about a person.

---

[61] *Smith*, 442 U.S. at 744–45.

[62] *See* Lipman, *supra* note 60, at 479 (arguing that courts today oversimplify these holdings, ignoring "the work the Court did in *Smith* and *Miller* [to] minimiz[e] the significance of the records attained by law enforcement").

[63] CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 184 (2007).

[64] Freiwald, *supra* note 58, at 709.

[65] Scholars argue that the content/noncontent distinction is increasingly outdated. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 398–99 (2014); Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2135–36 (2009) (arguing noncontent that reveals underlying content should be protected).

[66] *See, e.g.*, Stephen E. Henderson, *After* United States v. Jones*, After the Fourth Amendment Third Party Doctrine*, 14 N.C. J.L. & TECH. 431, 453–54 (2013).

[67] *See* Riley v. California, 134 S. Ct. 2473, 2493–95 (2014) ("Is an e-mail equivalent to a letter? Is a voicemail equivalent to a phone message slip?" *Id.* at 2493.).

Graham's facts illustrate the point. To link the defendants to robberies that took place over a period of weeks, the government obtained over seven months' worth of CSLI that could allow it to make inferences about the defendants' most intimate moments — taking place months before they were alleged to have committed crimes. Indeed, when the Court in *Jones* found that the government's GPS surveillance was an unconstitutional search,[68] the government sought to use CSLI at retrial to prove the same pattern of movements that they had originally proven with GPS.[69] To hold that Jones had a reasonable expectation of privacy in a pattern of movements that he then lost because of the means through which the government accessed them seems an absurd result.[70] Justice Sotomayor recognized this in *Jones* when she observed that the third-party doctrine's approach is "ill suited to the digital age."[71] But more instructive is her own approach. Rather than applying a per se rule that police could obtain information through technology if they could do so through physical surveillance, she would "ask whether people reasonably expect that their movements will be recorded" in a way that allows the government to infer the intimate details of their lives.[72] That is, she would use a contextual approach.

Though a criticism of that approach might be that it lacks the "simplicity and administrability" of the third-party doctrine,[73] courts in other areas of law conduct individualized analyses all the time. One example is medical records. In *Ferguson v. City of Charleston*,[74] the Court held that police needed a warrant to access pregnant women's drug tests, although those tests were conducted and retained by a third-

---

[68] United States v. Jones, 132 S. Ct. 945, 949 (2012).

[69] *See* Michael T.E. Kalis, Staff Article, *Ill Suited to the Digital Age: Fourth Amendment Exceptions and Cell Site Location Information Surveillance*, PITT. J. TECH. L. & POL'Y, Spring 2013, at 1, 14–15. The district court admitted the evidence. *See* United States v. Jones, 908 F. Supp. 2d 203, 214–16 (D.D.C. 2012). After a mistrial, defendant Antoine Jones pleaded out. *See* United States v. Jones, No. 05-0386-01 (ESH), 2014 WL 3538084, at *1 (D.D.C. July 14, 2014).

[70] The *Jones* majority reached that result by analyzing the GPS search as a physical trespass. *Jones*, 132 S. Ct. at 952–53. CSLI would seemingly fail that test. But the concurring Justices in *Jones* criticized that approach, arguing that the reasonable expectation of privacy test supplanted the trespass test. *Id.* at 959–61 (Alito, J., concurring in the judgment). Justice Sotomayor noted that many methods of surveillance that once would have required a physical trespass now can be accomplished through technology. *Id.* at 955 (Sotomayor, J., concurring). As the government's strategy at retrial shows, CSLI does exactly that — it does by electronic means what the government once had to rely on physical trespass to accomplish.

[71] *Id.* at 957 (Sotomayor, J., concurring) (observing that the Court may need to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"); *see also Graham*, 824 F.3d at 437 (noting that the "*per se* rule" of the third-party doctrine "seems unmoored from current understandings of privacy").

[72] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

[73] Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985, 985 (2016).

[74] 532 U.S. 67 (2001).

party state hospital.[75] But the Court did not apply any per se rule to make that determination, although it could have applied the third-party doctrine on the facts.[76] Rather, it applied a "balancing test" that weighed the women's privacy interests against the government's interest in preventing drug abuse.[77] It found: "The reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with non-medical personnel without her consent."[78] Similarly, the Third Circuit (citing *Ferguson*) refused to apply the third-party doctrine to a blood sample submitted as part of a rape kit.[79] Looking instead to the disclosure's nature, the court held that because the appellant "did nothing to forfeit [an] expectation" of privacy in her blood, she had retained her privacy interest although she shared the sample with a third party.[80]

These cases show the feasibility of a contextual approach to privacy expectations. Had the *Ferguson* Court and the Third Circuit applied the third-party doctrine, they would have classified the women as having lost their expectations of privacy just by disclosing information to third parties — without ever reaching the privacy questions. Those questions exist in CSLI. Relying on *Ferguson*, a district court judge in California writing on CSLI found that "a cell phone user's reasonable expectation of privacy in her location at virtually all times is not destroyed simply because law enforcement would have to obtain the records" from third parties.[81] Courts are entirely competent to conduct this kind of individualized analysis for CSLI — some already do so.

As Justice Alito observed, Congress could impose greater protections for CSLI.[82] After *Miller*, Congress passed a law that offered bank customers some privacy protections from police.[83] It could also do so here. And even if courts were to address the question, they could still find warrantless acquisition of CSLI constitutional.[84] But in failing to consider society's real expectations of privacy, courts rob themselves of an opportunity to fashion a doctrine that does what it says: track society's reasonable expectations of privacy.

---

[75] *See id.* at 76, 86.

[76] *See* Henderson, *supra* note 66, at 440 ("[*Ferguson*] is inconsistent with a robust third party doctrine.").

[77] *Ferguson*, 532 U.S. at 78.

[78] *Id.*

[79] *See* Reedy v. Evanson, 615 F.3d 197, 228–30 (3d Cir. 2010).

[80] *Id.* at 230.

[81] *In re* Application for Tel. Info. Needed for a Criminal Investigation, 119 F. Supp. 3d 1011, 1030 (N.D. Cal. 2015).

[82] *See* United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring in the judgment).

[83] *See* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2012).

[84] *See* Issacharoff & Wirshba, *supra* note 73, at 1025–28 (arguing that the Fourth Amendment's reasonableness doctrine might be a better fit for third-party information).