KeyCite Yellow Flag - Negative Treatment
Declined to Extend by United States v. Lambis, S.D.N.Y., July 12, 2016

824 F.3d 421
United States Court of Appeals,
Fourth Circuit.

United States of America, Plaintiff–Appellee,
v.
Aaron Graham, Defendant–Appellant.
Electronic Frontier Foundation; National Association of Criminal Defense Lawyers; American Civil Liberties Union Foundation of Maryland; Center for Democracy & Technology; American Civil Liberties Union Foundation; Downsizedc.org; Downsize DC Foundation; Gun Owners Foundation; Gun Owners of America, Inc.; Institute on the Constitution; Reporters Committee for Freedom of the Press; United States Justice Foundation; Conservative Legal Defense and Education Fund, Amici Supporting Appellant.
United States of America, Plaintiff–Appellee,
v.
Eric Jordan, Defendant–Appellant.
Electronic Frontier Foundation; National Association of Criminal Defense Lawyers; American Civil Liberties Union Foundation of Maryland; Center for Democracy & Technology; American Civil Liberties Union Foundation; Conservative Legal Defense and Education Fund; Downsizedc.org; Downsize DC Foundation; Gun Owners Of America, Inc.; Gun Owners Foundation; Institute on the Constitution; Reporters Committee for Freedom of the Press; United States Justice Foundation, Amici Supporting Appellant.

No. 12-4659, No. 12-4825
|
Argued: March 23, 2016
|
Decided: May 31, 2016

Synopsis

Background: Following denial of their motion to suppress, 846 F.Supp.2d 384, defendants were convicted in the United States District Court for the District of Maryland, Richard D. Bennett, J., of being felon in possession of firearm, Hobbs Act robbery, conspiracy to commit Hobbs Act robbery, and brandishing firearm, and they appealed. The Court of Appeals for the Fourth Circuit, 796 F.3d 332, affirmed the convictions, but held that the government violated defendants' Fourth Amendment rights in obtaining historical cell-site location information from defendants' cell phone provider without a warrant. Government moved for rehearing en banc, which was granted.

[Holding:] The Court of Appeals, en banc, Diana Gribbon Motz, Circuit Judge, held that government did not violate Fourth Amendment by obtaining historical cell-site location information from cell phone provider without warrant.

Affirmed.

Wilkinson, Circuit Judge, filed concurring opinion.

Wynn, Circuit Judge, filed opinion, concurring in the judgment, and dissenting in part, with which Floyd, and Thacker, Circuit Judges, joined.

West Headnotes (8)

[1] **Searches and Seizures**
What Constitutes Search or Seizure

A Fourth Amendment "search" occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable. U.S. Const. Amend. 4.

Cases that cite this headnote

[2] **Searches and Seizures**
Use of electronic devices; tracking devices or 'beepers.'

Government did not violate defendants' Fourth Amendment rights in obtaining historical cell-site location information from defendants' cell phone provider without a warrant in order to deduce defendants' approximate locations at times that crimes took place; defendants had no

reasonable expectation of privacy in that historical location information, as they voluntarily conveyed such information to cell phone provider by making and receiving calls and texts on their phones, the data was non-content routing information, and government obtained court order directing provider to disclose the information, pursuant to the Stored Communications Act (SCA). U.S. Const. Amend. 4; 18 U.S.C.A. § 2703(c), (d).

7 Cases that cite this headnote

[3] **Searches and Seizures**
What Constitutes Search or Seizure

In assessing whether a Fourth Amendment search has occurred, it is important to begin by specifying precisely the nature of the state activity that is challenged. U.S. Const. Amend. 4.

Cases that cite this headnote

[4] **Searches and Seizures**
Abandoned, surrendered, or disclaimed items

Under the "third-party doctrine" applicable to Fourth Amendment searches, an individual can claim no legitimate expectation of privacy in information that he has voluntarily turned over to a third party. U.S. Const. Amend. 4.

2 Cases that cite this headnote

[5] **Searches and Seizures**
Expectation of privacy

The Fourth Amendment does not protect information voluntarily disclosed to a third party because even a subjective expectation of privacy in such information is not one that society is prepared to recognize as reasonable. U.S. Const. Amend. 4.

Cases that cite this headnote

[6] **Searches and Seizures**
Taking items abandoned, voluntarily surrendered, or sold

The government does not engage in a Fourth Amendment "search" when it acquires information from a third party that a suspect has voluntarily disclosed to the third party. U.S. Const. Amend. 4.

Cases that cite this headnote

[7] **Searches and Seizures**
Abandoned, surrendered, or disclaimed items

The third-party doctrine, pursuant to which an individual can claim no reasonable expectation of privacy under the Fourth Amendment to information that he voluntarily discloses to a third party, even covers information that is considered highly private, like financial records. U.S. Const. Amend. 4.

3 Cases that cite this headnote

[8] **Searches and Seizures**
Expectation of privacy

In the face of rapidly advancing technology, courts must assure preservation of that degree of privacy against government intrusion that existed when the Fourth Amendment was adopted. U.S. Const. Amend. 4.

Cases that cite this headnote

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

***423** Appeals from the United States District Court for the District of Maryland, at Baltimore. Richard D. Bennett, District Judge. (1:11-cr-00094-RDB-1; 1:11-cr-00094-RDB-2)

Attorneys and Law Firms

ARGUED: Meghan Suzanne Skelton, Office of the Federal Public Defender, Greenbelt, Maryland, for Appellants. Rod J. Rosenstein, Office of the United States Attorney, Baltimore, Maryland, for Appellee. ON BRIEF: James Wyda, Federal Public Defender, Office of the Federal Public Defender, Baltimore, Maryland, for Appellant Aaron Graham; Ruth Vernet, Ruth J. Vernet, Esq., LLC, Rockville, Maryland, for Appellant Eric Jordan. Nathan Judish, Computer Crime & Intellectual Property Section, United States Department of Justice, Washington, D.C.; Sujit Raman, Chief of Appeals, Greenbelt, Maryland, Benjamin M. Block, Assistant United States Attorney, Office of the United States Attorney, Baltimore, Maryland, for Appellee. Nathan Freed Wessler, Catherine Crump, Ben Wizner, American Civil Liberties Union Foundation, New York, New York; David R. Rocah, American Civil Liberties Union Foundation of Maryland, Baltimore, Maryland; Kevin S. Bankston, Gregory T. Nojeim, Center for Democracy & Technology, Washington, D.C.; Thomas K. Maher, Vice–Chair, 4th Circuit Amicus Committee, National Association of Criminal Defense Lawyers, Durham, North Carolina; Hanni Fakhoury, ***424** Electronic Frontier Foundation, San Francisco, California, for Amici American Civil Liberties Union Foundation, American Civil Liberties Union Foundation of Maryland, Center for Democracy & Technology, Electronic Frontier Foundation, and National Association of Criminal Defense Lawyers. Michael Connelly, Ramona, California, for Amicus United States Justice Foundation; Robert J. Olson, Herbert W. Titus, William J. Olson, Jeremiah L. Morgan, William J. Olson, P.C., Vienna, Virginia, for Amici DownsizeDC.org, Downsize DC Foundation, United States Justice Foundation, Gun Owners of America, Inc., Gun Owners Foundation, Conservative Legal Defense and Education Fund, and Institute on the Constitution. Bruce D. Brown, Gregg Leslie, Hannah Bloch–Wehba, Reporters Committee for Freedom of the Press, Washington, D.C., for Amicus Reporters Committee for Freedom of the Press.

Before TRAXLER, Chief Judge, and WILKINSON, NIEMEYER, MOTZ, KING, GREGORY, SHEDD, DUNCAN, AGEE, KEENAN, WYNN, DIAZ, FLOYD, THACKER, and HARRIS, Circuit Judges.

Affirmed by published opinion. Judge Motz wrote the majority opinion, in which Chief Judge Traxler and Judges Wilkinson, Niemeyer, King, Gregory, Shedd, Duncan, Agee, Keenan, Diaz and Harris joined. Judge Wilkinson wrote a separate concurring opinion. Judge Wynn wrote a dissenting opinion in which Judges Floyd and Thacker joined.

ON REHEARING EN BANC

DIANA GRIBBON MOTZ, Circuit Judge:

In United States v. Graham, 796 F.3d 332 (4th Cir. 2015), a panel of this court affirmed the convictions of Defendants Aaron Graham and Eric Jordan arising from their participation in a series of armed robberies. The panel opinion sets out the facts of this case in great detail. Id. at 339–43. The only facts now relevant concern the portion of the Government's investigation during which it obtained historical cell-site location information (CSLI) from Defendants' cell phone provider. This historical CSLI indicated which cell tower—usually the one closest to the cell phone—transmitted a signal when the Defendants used their cell phones to make and receive calls and texts. The Government used the historical CSLI at Defendants' trial to place them in the vicinity of the armed robberies when the robberies had occurred.

A majority of the panel held that, although the Government acted in good faith in doing so, it had violated Defendants' Fourth Amendment rights when it obtained the CSLI without a warrant. The majority directed that henceforth the Government must secure a warrant supported by probable cause before obtaining these records from cell phone providers. The Government moved for rehearing en banc, which we granted, vacating the panel opinion. See United States v. Graham, 624 Fed.Appx. 75 (4th Cir. 2015); 4th Cir. R. 35(c). We now hold that the Government's acquisition of historical CSLI from Defendants' cell phone provider did not violate the Fourth Amendment.[1]

***425** Supreme Court precedent mandates this conclusion. For the Court has long held that an individual enjoys no Fourth Amendment protection "in information he voluntarily turns over to [a] third part[y]." Smith v. Maryland, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979). This rule—the third-party doctrine—applies even when "the information is revealed" to a third party, as it assertedly was here, "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will

not be betrayed." United States v. Miller, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). All of our sister circuits to have considered the question have held, as we do today, that the government does not violate the Fourth Amendment when it obtains historical CSLI from a service provider without a warrant. In addition to disregarding precedent, Defendants' contrary arguments misunderstand the nature of CSLI, improperly attempt to redefine the third-party doctrine, and blur the critical distinction between content and non-content information.

The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case.

I.

[1]The Fourth Amendment ensures that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const. amend. IV. Broadly, "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable." Kyllo v. United States, 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). The issue that confronts us here is whether the Government's acquisition of the historical CSLI records constituted a Fourth Amendment search.

[2] [3]In assessing whether such a search has occurred, "it is important to begin by specifying precisely the nature of the state activity that is challenged." Smith, 442 U.S. at 741, 99 S.Ct. 2577 (emphasis added). Here, that "activity" is the Government's acquisition from a phone company, Sprint/Nextel, of historical CSLI records—i.e., the records of the phone company that identify which cell towers it used to route Defendants' calls and messages. The Government did not surreptitiously view, listen to, record, or in any other way engage in direct surveillance of Defendants to obtain this information. Rather, as the Sprint/Nextel custodian of the CSLI records testified at trial, CSLI is created and maintained in the normal course of Sprint/Nextel's business. Defendants themselves acknowledge that service providers, like Sprint/Nextel, maintain CSLI records "[b]y technical and practical ***426** necessity." Defendants' Br. at 13.[2]

Moreover, to obtain the CSLI from Sprint/Nextel, the Government had to apply to a federal court for an order directing the company to disclose the records. The Stored Communications Act (SCA or the Act) provides that, to gain access to even these non-content records, the Government must demonstrate either probable cause for a warrant or "specific and articulable facts showing that there are reasonable grounds to believe that ... the records ... are relevant and material to an ongoing criminal investigation" for a court order. 18 U.S.C. § 2703(c), (d) (2012). The Government followed the second route and Defendants do not contend that in doing so it failed to meet the requirements of the Act. What Defendants do contend is that in permitting the Government to obtain the Sprint/Nextel records in this way, the Act violates the Fourth Amendment. According to Defendants, the statute permits the Government to unconstitutionally collect their private information.

This argument ignores the nature of the governmental activity here, which critically distinguishes this case from those in which the government did unconstitutionally collect private information. In United States v. Karo, 468 U.S. 705, 714–15, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984), for instance, the Drug Enforcement Agency placed a beeper within a can of ether and received tracking information from the beeper while the can was inside a private residence. Similarly, in Kyllo, 533 U.S. at 34–35, 121 S.Ct. 2038, the Department of the Interior used a thermal imager to gather "information regarding the interior of the home." And in United States v. Jones, ––U.S. ––––, 132 S.Ct. 945, 948–49, 954, 181 L.Ed.2d 911 (2012), the FBI and local law enforcement secretly installed a GPS tracking device on a suspect's vehicle and monitored the vehicle's movements for four weeks.[3]

On the basis of these cases, Defendants contend that the government always invades an individual's reasonable expectation of privacy when it employs technological devices to track an individual's moves. Perhaps so. But that question is not before us. No government tracking is at issue here. Rather, the question before us is whether the government invades an individual's reasonable expectation of privacy when it obtains, from a third party, the third party's records, which permit the government to deduce location information. Karo, Kyllo, and Jones, all of which involve direct government surveillance activity, tell us nothing about the answer to that question.[4]

[4] [5] [6] ***427** Instead, the cases that establish the third-party doctrine provide the answer. Under the third-party doctrine, an individual can claim "no legitimate expectation of privacy" in information that he has voluntarily turned over to a third party. Smith, 442 U.S. at 743–44, 99 S.Ct. 2577. The Supreme Court has reasoned that, by "revealing his affairs to another," an individual "takes the risk ... that the information will be

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

conveyed by that person to the Government." Miller, 425 U.S. at 443, 96 S.Ct. 1619. The Fourth Amendment does not protect information voluntarily disclosed to a third party because even a subjective expectation of privacy in such information is "not one that society is prepared to recognize as 'reasonable.' " Smith, 442 U.S. at 743, 99 S.Ct. 2577 (internal quotation marks and citation omitted). The government therefore does not engage in a Fourth Amendment "search" when it acquires such information from a third party.[5]

Applying the third-party doctrine to the facts of this case, we hold that Defendants did not have a reasonable expectation of privacy in the historical CSLI. The Supreme Court's reasoning in Smith controls. There, the defendant challenged the government's use of a pen register—a device that could record the outgoing phone numbers dialed from his home telephone. Id. at 737, 99 S.Ct. 2577. The Court held that the defendant could "claim no legitimate expectation of privacy" in the numbers he had dialed because he had "voluntarily conveyed" those numbers to the phone company by " 'expos[ing]' that information to" the phone company's "equipment in the ordinary course of business." Id. at 744, 99 S.Ct. 2577. The defendant thereby "assumed the risk that the company would reveal to police the numbers he dialed." Id.

Here, as in Smith, Defendants unquestionably "exposed" the information at issue to the phone company's "equipment in the ordinary course of business." Id. Each time Defendants made or received a call, or sent or received a text message—activities well within the "ordinary course" of cell phone ownership—Sprint/Nextel generated a record of the cell towers used. The CSLI that Sprint/Nextel recorded was necessary to route Defendants' cell phone calls and texts, just as the dialed numbers recorded by the pen register in Smith were necessary to route the defendant's landline calls. Having "exposed" the CSLI to Sprint/Nextel, Defendants here, like the defendant in Smith, "assumed the risk" ***428** that the phone company would disclose their information to the government. Id. at 744, 99 S.Ct. 2577. For these reasons, the Government's acquisition of that information (historical CSLI) pursuant to § 2703(d) orders, rather than warrants, did not violate the Fourth Amendment.

This holding accords with that of every other federal appellate court that has considered the Fourth Amendment question before us. Not one has adopted the Defendants' theory.

Three of our sister courts have expressly held, as we do today, that individuals do not have a reasonable expectation of privacy in historical CSLI records that the government obtains from cell phone service providers through a § 2703(d) order. See United States v. Carpenter, 819 F.3d 880, 887–89 (6th Cir.2016) (holding that "for the same reasons that Smith had no expectation of privacy in the numerical information at issue [in Smith], the defendants have no such expectation in the [CSLI] locational information here"); United States v. Davis, 785 F.3d 498, 511–13 (11th Cir.) (en banc) (holding that defendant has no "objective[ly] reasonable expectation of privacy in MetroPCS's business records showing the cell tower locations that wirelessly connected his calls"), cert. denied, —— U.S. ——, 136 S.Ct. 479, 193 L.Ed.2d 349 (2015); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (In re Application (Fifth Circuit)) (holding that the government can use "[s]ection 2703(d) orders to obtain historical cell site information" without implicating the Fourth Amendment (emphasis omitted)). And although the fourth of our sister courts opined that "[a] cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way," it held that "CSLI from cell phone calls is obtainable under a § 2703(d) order," which "does not require the traditional probable cause determination" necessary for a warrant. In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 313, 317 (3d Cir. 2010) (In re Application (Third Circuit)).

Moreover, even in the absence of binding circuit precedent, the vast majority of federal district court judges have reached the same conclusion.[6] Defendants are ***429** forced to rely on four inapposite state cases that either interpret broader state constitutional provisions instead of the Fourth Amendment, or do not consider historical CSLI records, or both.[7] In sum, the Defendants' preferred holding lacks support from all relevant authority and would place us in conflict with the Supreme Court and every other federal appellate court to consider the question.

II.

[7]Despite the lack of support for their position, Defendants insist that the third-party doctrine does not apply here. They argue that "[a] cell phone user does not even possess the CSLI to voluntarily convey," and that even assuming users do convey such information, "revealing this information is compelled, not voluntary."[8] Defendants' En Banc Br. at 10-11. These arguments

misapprehend the nature of CSLI, improperly attempt to redefine the third-party doctrine, and rest on a long-rejected factual argument and the constitutional protection afforded a communication's content.

A.

Defendants maintain that cell phone users do not convey CSLI to phone providers, voluntarily or otherwise. We reject that contention. With respect to the nature of CSLI, there can be little question that cell phone users "convey" CSLI to their service providers. After all, if they do not, then who does?

Perhaps Defendants believe that because a service provider generates a record of CSLI, the provider just conveys CSLI to itself. But before the provider can create such a record, it must receive information indicating that a cell phone user is relying on a particular cell tower. The provider only receives that information when a cell phone user's phone exchanges signals with the nearest available cell tower. A cell phone user therefore "conveys" the location of the cell towers his phone connects with to his provider whenever he uses the provider's network.

***430** There is similarly little question that cell phone users convey CSLI to their service providers "voluntarily." See Davis, 785 F.3d at 512 n.12 ("Cell phone users voluntarily convey cell tower location information to telephone companies in the course of making and receiving calls on their cell phones."). This is so, as the Fifth Circuit explained, even though a cell phone user "does not directly inform his service provider of the location of the nearest cell phone tower." In re Application (Fifth Circuit), 724 F.3d at 614; see also Carpenter, 819 F.3d at 887–88.

Logic compels this conclusion. When an individual purchases a cell phone and chooses a service provider, he expects the provider will, at a minimum, route outgoing and incoming calls and text messages. As most cell phone users know all too well, proximity to a cell tower is necessary to complete these tasks. Anyone who has stepped outside to "get a signal," or has warned a caller of a potential loss of service before entering an elevator, understands, on some level, that location matters. See In re Application (Fifth Circuit), 724 F.3d at 613 ("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.").

A cell phone user voluntarily enters an arrangement with his service provider in which he knows that he must maintain proximity to the provider's cell towers in order for his phone to function. See Carpenter, 819 F.3d at 887–88 ("[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."). Whenever he expects his phone to work, he is permitting—indeed, requesting—his service provider to establish a connection between his phone and a nearby cell tower. A cell phone user thus voluntarily conveys the information necessary for his service provider to identify the CSLI for his calls and texts. And whether the service provider actually "elects to make a ... record" of this information "does not ... make any constitutional difference." Smith, 442 U.S. at 745, 99 S.Ct. 2577.

To be sure, some cell phone users may not recognize, in the moment, that they are "conveying" CSLI to their service provider. See In re Application (Third Circuit), 620 F.3d at 317. But the Supreme Court's use of the word "voluntarily" in Smith and Miller does not require contemporaneous recognition of every detail an individual conveys to a third party.[9] Rather, ***431** these cases make clear that the third-party doctrine does not apply when an individual involuntarily conveys information—as when the government conducts surreptitious surveillance or when a third party steals private information.

Thus, this would be a different case if Sprint/Nextel had misused its access to Defendants' phones and secretly recorded, at the Government's behest, information unnecessary to the provision of cell service. Defendants did not assume that risk when they made calls or sent messages. But like the defendant in Smith, 442 U.S. at 745, 99 S.Ct. 2577, Defendants here did "assume the risk" that the phone company would make a record of the information necessary to accomplish the very tasks they paid the phone company to perform. They cannot now protest that providing this essential information was involuntary.

B.

In their efforts to avoid the third-party doctrine, Defendants attempt to redefine it. They maintain that the third-party doctrine does not apply to historical CSLI because a cell phone user does not "actively choose[ ] to share" his location information. Defendants' Br. at 30. Such a rule is nowhere to be found in either Miller or Smith. Moreover, this purported requirement cannot be squared with the myriad of federal cases that permit the

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

government to acquire third-party records, even when individuals do not "actively choose to share" the information contained in those records.

For example, courts have attached no constitutional significance to the distinction between records of incoming versus outgoing phone calls. The technology the police used in Smith—a pen register—recorded only the numbers dialed by a suspect's phone. It did not (and could not) record any information about incoming calls. To capture that information, police routinely use a "trap and trace" device. If Defendants were correct that the third-party doctrine applies just when an individual "actively chooses to share" information, then any effort to acquire records of incoming phone calls would constitute a search protected by the Fourth Amendment. After all, the phone customer never "actively chooses to share" with the phone company the numbers from incoming telephone calls. Only the user on the other end of the line, who actually dials the numbers, does so.

But federal courts have not required a warrant supported by probable cause to obtain such information. Rather, they routinely permit the government to install "trap and trace" devices without demonstrating probable cause. See, e.g., United States v. Reed, 575 F.3d 900, 914–17 (9th Cir. 2009); United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990).[10] And recently we held that police "did not violate the Fourth Amendment" when obtaining a defendant's "cellular phone records," even ***432** though the records included "basic information regarding incoming and outgoing calls on that phone line." United States v. Clenney, 631 F.3d 658, 666–67 (4th Cir. 2011) (emphasis added).[11]

Moreover, outside the context of phone records, we have held that third-party information relating to the sending and routing of electronic communications does not receive Fourth Amendment protection. United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). In Bynum, we explained that it "would not be objectively reasonable" for a defendant to expect privacy in his phone and Internet subscriber records, including "his name, email address, telephone number, and physical address." Id. Although we had no occasion in Bynum to consider whether an individual has a protected privacy interest in his Internet Protocol (IP) address, id. at 164 n.2, several of our sister circuits have concluded that no such interest exists. See United States v. Suing, 712 F.3d 1209, 1213 (8th Cir. 2013); United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010).

Similarly, the Ninth Circuit has held that "e-mail and Internet users have no expectation of privacy in ... the IP addresses of the websites they visit." United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008). The Forrester court also held that there is no reasonable expectation of privacy in either the to/from addresses of a user's emails or the "total amount of data transmitted to or from [a user's] account." Id. at 510–11. The court found the government's acquisition of this information "constitutionally indistinguishable from the use of a pen register that the Court approved in Smith," in part because "e-mail and Internet users, like the telephone users in Smith, rely on third-party equipment in order to engage in communication." Id. at 510.

Of course, computer users do "actively choose to share" some of the information discussed in the above cases, like the "to" address in an email and the subscriber information conveyed when signing up for Internet service. But users do not "actively choose to share" other pieces of information, like an IP address or the amount of data transmitted to their account. Internet service providers automatically generate that information. See Christie, 624 F.3d at 563; cf. Forrester, 512 F.3d at 511. Thus, the redefinition of the third-party doctrine that Defendants advocate not only conflicts with Supreme Court doctrine and all the CSLI cases from our sister circuits, but is also at odds with other established circuit precedent.

C.

In another attempt to avoid the third-party doctrine, Defendants rely on a factual argument long rejected by the Supreme Court and a series of cases involving the content of communications to support their assertion that historical CSLI is protected by the Fourth Amendment.

First, Defendants emphasize that cell phone use is so ubiquitous in our society today that individuals must risk producing CSLI or "opt out of modern society." Defendants' En Banc Br. at 11. Defendants ***433** contend that such widespread use shields CSLI from the consequences of the third-party doctrine and renders any conveyance of CSLI "not voluntary," for "[l]iving off the grid ... is not a prerequisite to enjoying the protection of the Fourth Amendment." Id.

But the dissenting justices in Miller and Smith unsuccessfully advanced nearly identical concerns. Dissenting in Miller, Justice Brennan contended that "the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

contemporary society without maintaining a bank account." 425 U.S. at 451, 96 S.Ct. 1619 (Brennan, J., dissenting) (internal quotation marks and citation omitted). And dissenting in Smith, Justice Marshall warned that "unless a person is prepared to forgo use of what for many has become a personal or professional necessity," i.e., a telephone, "he cannot help but accept the risk of surveillance." 442 U.S. at 750, 99 S.Ct. 2577 (Marshall, J., dissenting). It was, in Justice Marshall's view, "idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." Id. The Supreme Court has thus twice rejected Defendants' theory. Until the Court says otherwise, these holdings bind us.

Second, Defendants rely on cases that afford Fourth Amendment protection to the content of communications to suggest that CSLI warrants the same protection. See Ex parte Jackson, 96 U.S. 727, 733, 24 L.Ed. 877 (1877) (content of letters and packages); Katz v. United States, 389 U.S. 347, 353, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (content of telephone calls); United States v. Warshak, 631 F.3d 266, 287–88 (6th Cir. 2010) (content of emails). What Defendants fail to recognize is that for each medium of communication these cases address, there is also a case expressly withholding Fourth Amendment protection from non-content information, i.e., information involving addresses and routing. See Jackson, 96 U.S. at 733 (no warrant needed to examine the outside of letters and packages); Smith, 442 U.S. at 743–44, 99 S.Ct. 2577 (no reasonable expectation of privacy in phone numbers dialed); Forrester, 512 F.3d at 510 (no reasonable expectation of privacy in the to/from addresses of emails); accord Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring) (noting the Fourth Amendment does not currently protect "phone numbers" disclosed to phone companies and "e-mail addresses" disclosed to Internet service providers).

The Supreme Court has thus forged a clear distinction between the contents of communications and the non-content information that enables communications providers to transmit the content.[12] CSLI, which identifies the equipment used to route calls and texts, undeniably belongs in the non-content category. As the Sixth Circuit recently recognized, CSLI is non-content information because "cell-site data—like mailing addresses, phone numbers, and IP addresses—are information that facilitate personal communications, rather than part of the content of those communications themselves." Carpenter, 819 F.3d at 887–88.

Defendants disagree with this conclusion. They contend that CSLI should be treated "as content" because it "record[s] a ***434** person's movements over a prolonged period," implicating "serious ... privacy concerns." Defendants' Br. at 33. But all routing information "records" some form of potentially sensitive activity when aggregated over time. For example, a pen register records every call a person makes and allows the government to know precisely when he is at home and who he is calling and credit card records track a consumer's purchases, including the location of the stores where he made them. Of course, CSLI is not identical to either of these other forms of routing information, just as cell phones are not identical to other modes of communication. It blinks at reality, however, to hold that CSLI, which contains no content, somehow constitutes a communication of content for Fourth Amendment purposes.

Defendants' attempts to blur this clear distinction[13] further illustrate the extent to which their proposed holding would be a constitutional outlier—untenable in the abstract and bizarre in practice. Case in point: Under Defendants' theory, the Government could legally obtain, without a warrant, all data in the Sprint/Nextel records admitted into evidence here, except the CSLI. If that is so, then the line between a Fourth Amendment "search" and "not a search" would be the literal line that, moving left to right across the Sprint/Nextel spreadsheets, separates the seventh column from the eighth. The records to the left of that line list the source of a call, the number dialed, the date and time of the call, and the call's duration—all of which the government can acquire without triggering Fourth Amendment protection. The records to the right of that line list the cell phone towers used at the start and end of each call—information Defendants' contend is protected by the Fourth Amendment. Constitutional distinctions are made of sturdier stuff.

III.

Technology has enabled cell phone companies, like Sprint/Nextel, to collect a vast amount of information about their customers. The quantity of data at issue in this case—seven months' worth of cell phone records, spanning nearly 30,000 calls and texts for each defendant—unquestionably implicates weighty privacy interests.

Outrage at the amount of information the Government obtained, rather than concern for any legal principle, seems to be at the heart of Defendants' arguments. Thus they repeatedly emphasize the amount of CSLI obtained here and rely on authority suggesting that the government

can obtain a limited amount of CSLI without a warrant. In response, the panel majority expressly held that the government can acquire some amount of CSLI "before its inspection rises to the level of a Fourth ***435** Amendment search." Graham, 796 F.3d at 350 n.8. But, if as Defendants maintain, every bit of CSLI has the potential to "show when a particular individual is home," and no CSLI is voluntarily conveyed, Defendants' Br. at 19-20, then why would only large quantities of CSLI be protected by the Fourth Amendment?[14]

Defendants' answer appears to rest on a misunderstanding of the analysis embraced in the two concurring opinions in Jones. There, the concurring justices recognized a line between "short-term monitoring of a person's movements on public streets," which would not infringe a reasonable expectation of privacy, and "longer term GPS monitoring," which would. Jones, 132 S.Ct. at 964 (Alito, J., concurring in the judgment); see also id. at 955 (Sotomayor, J., concurring). But Jones involved government surveillance of an individual, not an individual's voluntary disclosure of information to a third party. And determining when government surveillance infringes on an individual's reasonable expectation of privacy requires a very different analysis.

In considering the legality of the government surveillance at issue in Jones, Justice Alito looked to what a hypothetical law enforcement officer, engaged in visual surveillance, could reasonably have learned about the defendant. He concluded that four weeks of GPS monitoring by the government constituted a Fourth Amendment "search" because "society's expectation" had always been "that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue" an individual's movements in public for very long. Id. at 964 (Alito, J., concurring in the judgment) (emphasis added). In other words, direct surveillance by the government using technological means may, at some point, be limited by the government's capacity to accomplish such surveillance by physical means.[15]

However, society has no analogous expectations about the capacity of third parties to maintain business records. Indeed, we expect that our banks, doctors, credit card companies, and countless other third parties will record and keep information about our relationships with them, and will do so for the entirety of those relationships—be it several weeks or many years. Third parties can even retain their records about us after our relationships with them end; it is their prerogative, and many business-related reasons exist for doing so. This is true even when, in the aggregate, these records reveal sensitive information similar to what could be revealed by direct surveillance. For this reason, Justice Alito's concern in Jones is simply inapposite to the third-party doctrine and to the instant case.

Here, Defendants voluntarily disclosed all the CSLI at issue to Sprint/Nextel. And the very act of disclosure negated any reasonable expectation of privacy, regardless of how frequently that disclosure occurred or how long the third party ***436** maintained records of the disclosures. Defendants ignore these critical facts, attempting to apply the same constitutional requirements for location information acquired directly through GPS tracking by the government to historical CSLI disclosed to and maintained by a third party.

We recognize the appeal—if we were writing on a clean slate—in holding that individuals always have a reasonable expectation of privacy in large quantities of location information, even if they have shared that information with a phone company. But the third-party doctrine does not afford us that option. Intrinsic to the doctrine is an assumption that the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy.

Although third parties have access to much more information now than they did when the Supreme Court decided Smith, the Court was certainly then aware of the privacy implications of the third-party doctrine. Justice Stewart warned the Smith majority that "broadcast[ing] to the world a list of the local or long distance numbers" a person has called could "reveal the most intimate details of [that] person's life." Smith, 442 U.S. at 748, 99 S.Ct. 2577 (Stewart, J., dissenting). That is, in essence, the very concern that Defendants raise. But the Supreme Court was unmoved by the argument then, and it is not our place to credit it now. If individuals lack any legitimate expectation of privacy in information they share with a third party, then sharing more non-private information with that third party cannot change the calculus.

[8]Of course, in the face of rapidly advancing technology, courts must "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." Kyllo, 533 U.S. at 34, 121 S.Ct. 2038. The Supreme Court has long concluded that the third-party doctrine does this. Thus the Court has never held that routing information, like CSLI, shared with third parties to allow them to deliver a message or provide a service is protected under the Fourth Amendment. Perhaps this is implicit acknowledgment that the privacy-erosion argument has a flip-side:

technological advances also do not give individuals a Fourth Amendment right to conceal information that otherwise would not have been private.[16]

Moreover, application of the third-party doctrine does not render privacy an unavoidable casualty of technological progress—Congress remains free to require greater privacy protection if it believes that desirable. The legislative branch is far better positioned to respond to changes in technology than are the courts. See Jones, 132 S.Ct. at 964 (Alito, J., concurring in the judgment) ("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."); see also In re Application (Fifth Circuit), 724 F.3d at 615 (explaining that that the proper "recourse" ***437** for those seeking increased privacy is often "in the market or the political process").

The very statute at issue here, the Stored Communications Act (SCA), demonstrates that Congress can—and does—make these judgments. The SCA requires the government to meet a higher burden when acquiring "the contents of a wire or electronic communication" from "a provider of electronic communication service" than when obtaining "a record ... pertaining to a subscriber ... or customer" from the provider. 18 U.S.C. § 2703(a), (c) (emphasis added). It requires the executive to obtain judicial approval, as the Government did here, before acquiring even non-content information. Id. § 2703(c), (d). And the SCA is part of a broader statute, the Electronic Communications Privacy Act of 1986 (ECPA), which Congress enacted in the wake of Smith. See Pub. L. No. 99-508, 100 Stat. 1848. In the ECPA, Congress responded directly to the holding in Smith by requiring the government to obtain a court order (albeit not one supported by probable cause) before installing a pen register or "trap and trace" device. See 18 U.S.C. § 3121(a) (2012). Although Congress could undoubtedly do more, it has not been asleep at the switch.[17]

Ultimately, of course, the Supreme Court may decide to revisit the third-party doctrine. Justice Sotomayor has suggested that the doctrine 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." Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring). Indeed, although the Court formulated the third-party doctrine as an articulation of the reasonable-expectation-of-privacy inquiry, it increasingly feels like an exception. A per se rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy. But Justice Sotomayor also made clear that tailoring the Fourth Amendment to "the digital age" would require the Supreme Court itself to "reconsider" the third-party doctrine. Id.

The landscape would be different "if our Fourth Amendment jurisprudence cease [d] to treat secrecy as a prerequisite for privacy." Id. But unless and until the Supreme Court so holds, we are bound by the contours of the third-party doctrine as articulated by the Court. See, e.g., Agostini v. Felton, 521 U.S. 203, 237, 117 S.Ct. 1997, 138 L.Ed.2d 391 (1997) (reversing the Second Circuit but noting that it had correctly applied then-governing law, explaining that "if a precedent of this Court has direct application in a case, yet appears to rest on reasons rejected in some other line of decisions, the Court of Appeals should follow the case which directly controls" (internal quotation marks, alteration, and citation omitted)). Applying the third-party doctrine, consistent with controlling precedent, ***438** we can only conclude that the Fourth Amendment did not protect Sprint/Nextel's records of Defendants' CSLI. Accordingly, we hold that the Government legally acquired those records through § 2703(d) orders.

IV.

For the reasons set forth above, we affirm in all respects the judgment of the district court.

AFFIRMED

WILKINSON, Circuit Judge, concurring:

I am pleased to concur in Judge Motz's fine opinion. The court rightly holds that obtaining historical cell site location information (CSLI) from a third party cell phone provider is not a search under the Fourth Amendment. Any result to the contrary would be at odds with the Supreme Court and decisions from our sister circuits. I write separately to emphasize my concern that requiring probable cause and a warrant in circumstances such as these needlessly supplants the considered efforts of Congress with an ill-considered standard of our own.

Appellants appear to think that the Framers drafted the Constitution with the judiciary alone in mind. I do not deny that the judiciary has an important, indeed critical, role to play in interpreting the Fourth Amendment. But I fear that by effectively rewriting portions of a federal

statute under the guise of reasonableness review courts run the risk of boxing the democratic branches out of the constitutional dialogue. For good reason, developing constitutional meaning has always been a collaborative enterprise among the three departments of government. The present case offers a perfect example of why that is so.

I.

In enacting Title II of the Electronic Communications Privacy Act of 1986, popularly known as the Stored Communications Act (SCA), 18 U.S.C. § 2701 et seq., Congress did not behave in a flippant or haphazard fashion. Instead, it crafted a thorough statutory framework limiting the government's ability to gather wire and electronic communication data from communications service providers (here, Sprint/Nextel). The SCA's "comprehensive remedial scheme," Kelley v. Fed. Bureau of Investigation, 67 F.Supp.3d 240, 271 (D.D.C. 2014), "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." Sams v. Yahoo! Inc., 713 F.3d 1175, 1179 (9th Cir. 2013) (quoting Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1212 (2004)).

At the heart of the SCA lies § 2703. That provision establishes a calibrated set of procedural safeguards based on the type and amount of information sought and the length of time the records are stored. For instance, "only pursuant to a warrant," 18 U.S.C. § 2703(a), can the government obtain the contents of a communication that is in electronic storage with a service provider for 180 days or less. Alternatively, the government has a number of options for compelling the disclosure of non-content customer records, or the contents of communications in electronic storage for more than 180 days: "obtain[ ] a warrant," id. §§ 2703(b)(1)(A), (c)(1)(A), "use [ ] an administrative subpoena ... or trial subpoena," id. § 2703(b)(1)(B)(i), or "obtain[ ] a court order." Id. §§ 2703(b)(1)(B)(ii), (c)(1)(B).

***439** Here, the government secured a court order for the disclosure of non-content communication records (specifically, CSLI) pursuant to § 2703(c)(1)(B). Congress set forth the requirements for a valid court order in § 2703(d), which mandates that the government supply "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). In other words, § 2703(d) "is essentially a reasonable suspicion standard." In re U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 287 (4th Cir. 2013).

I see no reason to depart from Congress's carefully tailored scheme. As the majority points out, the SCA in fact exceeds the constitutional floor established by the Supreme Court, whose decisions hold that the Fourth Amendment does not apply to information voluntarily conveyed to third parties. Ante at 426 – 27; see, e.g., Smith v. Maryland, 442 U.S. 735, 743–44, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979); United States v. Miller, 425 U.S. 435, 443, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976). Although appellants would insert their own impressions of the Fourth Amendment into § 2703(d) by way of a warrant and probable cause requirement, that approach not only aspires to overturn Supreme Court rulings but to scuttle the laborious efforts of the Congress to balance privacy and law enforcement interests in a responsible way.

II.

It has long been the case that developing constitutional meaning is not a responsibility that rests solely on the shoulders of the judiciary. It has instead been "a power and duty shared by all three branches, and its shared nature suggests that it ought not be fulfilled by each branch acting independently within its sphere of authority." Dawn E. Johnsen, Functional Departmentalism and Nonjudicial Interpretation: Who Determines Constitutional Meaning?, 67 Law & Contemp. Probs. 105, 121 (2004). Formulation of constitutional guidance, in other words, is a collaborative enterprise, "with each branch encouraged to recognize its own institutional limitations and to respect the superior competencies of the others." Id. at 120.*

This principle applies with special force where Congress has weighed in on the Fourth Amendment's requirement of "reasonableness." That term, of course, "is not capable of precise definition or mechanical application." Bell v. Wolfish, 441 U.S. 520, 559, 99 S.Ct. 1861, 60 L.Ed.2d 447 (1979). Faced with a term literally crying out for balance between the competing interests of individual privacy and societal security, it is appropriate to accord some degree of deference to legislation weighing the utility of a particular investigative method against the degree of intrusion on individuals' privacy interests. See ***440** United States v. Jones, —— U.S. ——, 132 S.Ct.

945, 963–64, 181 L.Ed.2d 911 (2012) (Alito, J., concurring).

In this setting, Congress brings several cards to the table. First, it enjoys a relatively greater degree of access than courts to expert opinion generally and to the expertise of the executive branch in particular. Trial courts, of course, hear expert testimony all the time, but they are to a considerable extent at the mercy of the parties whose witnesses may be called to serve a narrow set of interests rather than the interests of the public at large. Appellate amicus briefs and arguments are helpful to be sure, but not enough, I think, to close the expertise gap or compensate for the large differences in size between congressional and judicial staffs. The more technical the issue (as the one before us surely is), the more salient the expertise differential may prove to be. It is not surprising, then, that "[t]hroughout our history ... it has been Congress that has taken the lead in ... balanc[ing] the need for a new investigatory technique against the undesirable consequences of any intrusion on constitutionally protected interests in privacy." Dalia v. United States, 441 U.S. 238, 264, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979) (Stevens, J., dissenting). That tradition is a sound one, for it not only reflects an understanding of our own institutional limitations, but the value of having democratic backing behind Fourth Amendment balancing.

Second, Congress is often better positioned to achieve legal consistency. Abandoning Congress's comprehensive effort for particularized and improvised judicial standards invites confusion into what has been a relatively stable area of the law. See ante at 426 – 28. The SCA—which remains "the primary vehicle by which to address violations of privacy interests in the communication field," Adams v. City of Battle Creek, 250 F.3d 980, 986 (6th Cir. 2001)—promotes uniformity by focusing the courts' inquiry on a prescribed set of conditions that must be satisfied before disclosure will be compelled. See, e.g., 18 U.S.C. § 2703(d). Detailed statutory standards have at least as fair a chance of achieving clear guidance and consistency as court developed rules. Congress's aim of consistency would be imperiled, however, if courts become willing to strike this or that portion of the statute to accommodate what may be their unique privacy policy views. In my judgment, uniform national standards rather than regional variations among the courts has merit where Congress has comprehensively legislated in a particular field.

Finally, Congress imparts the considerable power of democratic legitimacy to a high stakes and highly controversial area. The emergence of advanced communication technologies has set off a race between criminal enterprises on the one hand and law enforcement efforts on the other. Modern communication devices—even as they abet the government's indigenous tendencies to intrude upon our privacy—also assist criminal syndicates and terrorist cells in inflicting large-scale damage upon civilian populations. Appellants' strict standard of probable cause and a warrant even for non-content information held by third parties thus risks an imbalance of the most dangerous sort, for it allows criminals to utilize the latest in technological development to commit crime and hamstrings the ability of law enforcement to capitalize upon those same developments to prevent crime. The fact that the appellants in this case were convicted of Hobbs Act violations and brandishing offenses cannot obscure the implications of their proposed standards for much more serious threats down the road.

In my view, striking a balance in an area rife with the potential for mass casualty ***441** cannot leave democracy out in the cold. Courts must continue to play a vital role in Fourth Amendment interpretation, but in large matters of life and death the people's representatives must also play their part. See, e.g., Donovan v. Dewey, 452 U.S. 594, 603, 101 S.Ct. 2534, 69 L.Ed.2d 262 (1981) (Congress's authorization of warrantless inspections of surface and underground mines deemed constitutional under the Fourth Amendment in light of the "notorious history of serious accidents" causing large loss of life in the mining industry). It is naive, I think, for the judicial branch to assume insensitivity to privacy concerns on the part of our elected brethren. Just last year, for example, a bipartisan Congress terminated the National Security Agency's collection of bulk phone records. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 (USA Freedom Act), Pub. L. No. 114-23, 129 Stat. 268. Other statutes make Congress's privacy concerns abundantly clear. See, e.g., Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (2012)); Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. § 2510 et seq. (2012)).

It is human nature, I recognize, to want it all. But a world of total privacy and perfect security no longer exists, if indeed it ever did. We face a future of hard tradeoffs and compromises, as life and privacy come simultaneously under siege. How sad, near the very inception of this journey, for appellants to adopt the most stringent of Fourth Amendment standards, to discard the great values of democratic compromise, and to displace altogether the legislative role.

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

WYNN, Circuit Judge, with whom FLOYD and THACKER, Circuit Judges, join, dissenting in part and concurring in the judgment:[1]

A customer buys a cell phone. She turns it on and puts it in her pocket. With those acts, says the majority, she has "voluntarily conveyed" an unbounded set of personal location data to her service provider, all of which is unprotected by the Fourth Amendment. Here, that included 221 days' worth of information, amounting to roughly 29,000 location-identifying data points for each Defendant.

The majority further claims that "Supreme Court precedent mandates this conclusion," that "[l]ogic compels" it. Ante, at 425, 430. But those contentions are difficult to square with the array of concurring and dissenting opinions that have already been issued by federal appellate judges on this subject.[2] With respect for the differing ***442** view of my colleagues in the majority, this is not an easy issue. Not only that, but a close reading of the Supreme Court's third-party doctrine demonstrates that cell site location information (CSLI) is not "voluntarily conveyed" by cell phone users. It is therefore not beyond the Fourth Amendment's reach.

I.

A.

The third-party doctrine operates to bar Fourth Amendment protection only for information that has been "voluntarily conveyed" by an individual to a third party. The majority does not dispute this limitation, see ante, at 426–27, 429–30, nor could it. That phrase, or some slight variation of it, appears without exception as a necessary analytical component in each of the Supreme Court's founding third-party doctrine cases. Smith v. Maryland, 442 U.S. 735, 744, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) ("When he used his phone, petitioner voluntarily conveyed numerical information to the telephone company...." (emphasis added)); id. at 745, 99 S.Ct. 2577 ("[P]etitioner voluntarily conveyed to [the phone company] information that it had facilities for recording...." (emphasis added)); United States v. Miller, 425 U.S. 435, 442, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) ("All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks...." (emphasis added)); Hoffa v. United States, 385 U.S. 293, 302, 87 S.Ct. 408, 17 L.Ed.2d 374 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it." (emphasis added)); Lewis v. United States, 385 U.S. 206, 212, 87 S.Ct. 424, 17 L.Ed.2d 312 (1966) ("[This case] presents no question of the invasion of the privacy of a dwelling; the only statements repeated were those that were willingly made to the agent and the only things taken were the packets of marihuana voluntarily transferred to him." (emphasis added)); see also United States v. White, 401 U.S. 745, 749, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971) (no Fourth Amendment protection where an individual "voluntarily confides his wrongdoing" to another (quoting Hoffa, 385 U.S. at 302, 87 S.Ct. 408)).

The Supreme Court, then, has intentionally employed the "voluntary conveyance" concept in every relevant case to limit the reach of an otherwise sweeping per se rule that denies Fourth Amendment protection. It seems therefore crucial here to ask: what, precisely, did the Court mean when it chose those words, in the context of those cases?

Here is what those various defendants actually did to "voluntarily convey" information. One used his finger to dial, one by one, the numerical digits of a telephone number. Smith, 442 U.S. at 741, 99 S.Ct. 2577 (highlighting that pen registers disclose "only the telephone numbers that have been dialed" (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977))). Another submitted multiple checks and deposit slips— ***443** each presumably bearing a date, a dollar amount, a recipient name, and a personal signature. Miller, 425 U.S. at 442, 96 S.Ct. 1619. The others actually spoke. White, 401 U.S. at 746–47, 91 S.Ct. 1122 (conversations with a bugged government informant related to narcotics transactions); Hoffa, 385 U.S. at 296, 87 S.Ct. 408 (statements to an associate "disclosing endeavors to bribe [jury] members"); Lewis, 385 U.S. at 210, 87 S.Ct. 424 (conversations with an undercover law enforcement agent in the course of executing a narcotics sale).

In all of these cases—the only cases that can bind us here—"voluntary conveyance" meant at least two things. First, it meant that the defendant knew he was communicating particular information. We can easily assume Miller knew how much money he was depositing, that Smith knew the numbers he was dialing, and that Hoffa, Lewis, and White knew about the misconduct they verbally described to another.

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

Second, "voluntary conveyance" meant that the defendant had acted in some way to submit the particular information he knew. Crucially, there was an action—depositing, dialing, speaking—corresponding to each piece of submitted information. And where many data pieces were compiled into records—financial records in Miller, phone records in Smith—there was presumptively a discrete action behind each piece of data. The Court never suggested that the simple act of signing up for a bank account, or a phone line, was enough to willingly turn over thousands of pages of personal data.

These two components of "voluntary conveyance"—knowledge of particular information and an action submitting that information—were thus present in every "Supreme Court precedent" that can "mandate[ ] [our] conclusion" here. Ante, at 425. Those features also characterize the vast majority of cases where the third-party doctrine has been applied by other federal courts.

When a credit card holder signs a receipt that includes the address of the vendor, the bill amount, and the time of the transaction, she both indicates her knowledge of that particular information and acts to submit it.[3] Thus, courts have held that the third-party doctrine applies to credit card records. E.g., United States v. Phibbs, 999 F.2d 1053, 1077–78 (6th Cir. 1993); see also United States v. Maturo, 982 F.2d 57, 59 (2d Cir. 1992) (credit card records admitted as evidence); United States v. Kragness, 830 F.2d 842, 865 (8th Cir. 1987) (same).

When someone types "his name, email address, telephone number, and physical address" into a form and then submits that information to a service provider in order ***444** to secure internet access, he not only has knowledge of the typed information but has affirmatively acted to communicate it. United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010). Thus, courts have held that the third-party doctrine applies to subscriber information. Id.; see also United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) (collecting cases).

When an internet user types a URL—which is uniquely linked to a single IP address[4]—into her web browser and hits the "Enter" key, she knows the web address and she actively submits it. Thus, although the law in this area is still unsettled, courts have generally concluded that the third-party doctrine applies to the IP addresses of visited websites. See, e.g., United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("Like telephone numbers ... e-mail to/from addresses and IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party's servers.").[5]

It follows that knowledge of particular information and a corresponding act transmitting that information have defined "voluntary conveyance" in virtually every case espousing or applying the third-party doctrine, and certainly in every case that can bind us here. Those features describe traditional bank records and phone records, hotel bills and airline miles statements, email addresses and social media profile information. This is a description—not a redefinition—of the third-party doctrine.[6]

B.

The foregoing discussion makes clear that CSLI is not "voluntarily conveyed" by a cell phone user, and therefore is not subject to the third-party doctrine.

First, consider how little a cell phone user likely knows about his CSLI. Unlike ***445** the deposit amounts in Miller and the phone numbers in Smith, which were at various points made obvious to the user "in the ordinary course of business," Smith, 442 U.S. at 744, 99 S.Ct. 2577, there is no reason to think that a cell phone user is aware of his CSLI, or that he is conveying it. He does not write it down on a piece of paper, like the dollar amount on a deposit slip, or enter it into a device, as he does a phone number before placing a call. Nor does CSLI subsequently appear on a cell phone customer's statement, as the relevant information did for the banking customer in Miller and the phone caller in Smith. See Smith, 442 U.S. at 742, 99 S.Ct. 2577 ("All subscribers realize ... that the phone company has facilities for making permanent records of the numbers they dial, [because] they see a list of their ... calls on their monthly bills."). Consequently, "it is unlikely that cell phone customers are aware that their cell phone providers collect and store [CSLI]." In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 317 (3d Cir. 2010) (In re Application (Third Circuit)). And even if cell phone customers have a vague awareness that their location affects the number of "bars" on their phone, see ante, at 430, they surely do not know which cell phone tower their call will be routed through, a fact even the government concedes. Appellee's Br. at 53 ("[T]he location of the cell phone tower handling a customer's call is generated internally by the phone company and is not typically known by the customer."). User knowledge, the first component of "voluntary conveyance," is therefore

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

essentially absent.[7]

Second, consider what the cell phone user does—or does not do—to transmit CSLI. As a general matter, "CSLI is purely a function and product of cellular telephone technology, created by the provider's system network at the time that a cellular telephone call connects to a cell site." Commonwealth v. Augustine, 4 N.E.3d 846, 862, 467 Mass. 230 (2014). In some instances, CSLI is produced when a user places an outgoing call, an action that arguably corresponds with the generated information (even if the user remains unaware of that information). However, CSLI is also generated when a phone simply receives a call, even if the user does not answer. In these instances, CSLI is automatically generated by the service provider's network, without any user participation at all. See In re Application (Third Circuit), 620 F.3d at 317–18 ("[W]hen a cell phone user receives a call, he hasn't voluntarily exposed anything at all.").[8]

***446** In sum, because a cell phone customer neither possesses knowledge of his CSLI nor acts to disclose it, I agree with the Third Circuit that he "has not 'voluntarily' shared his location information with a cellular provider in any meaningful way." Id. at 317; accord Augustine, 4 N.E.3d at 862; Tracey v. State, 152 So.3d 504, 525 (Fla. 2014).[9]

II.

Because CSLI is not voluntarily conveyed to service providers, the third-party doctrine alone cannot resolve whether the government here conducted a Fourth Amendment "search." In other words, there must be an independent evaluation of whether "the government violates a subjective expectation of privacy that society recognizes as reasonable" by acquiring large amounts of CSLI. Kyllo v. United States, 533 U.S. 27, 33, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001) (citing Katz v. United States, 389 U.S. 347, 361, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (Harlan, J., concurring)). To answer that question, an examination is warranted of both the quality and quantity of the information the government here acquired.

The government obtained 221 days of CSLI for each Defendant.[10] That amounted ***447** to 29,659 location data points for Graham (an average of 134 data location points per day) and 28,410 location data points for Jordan (an average of 129 location points per day). Each piece of data revealed not only the particular cell tower through which the relevant call was routed, but also a particular 120-degree sector—or one-third "slice"—within that cell tower's range. The record indicates that the cell sites at issue in this case covered a circular area with a radius no larger than two miles. But given the density of cell sites in urban areas like Baltimore, where Sprint/Nextel operates 79 cell sites within the city limits and many more in Baltimore County, the relevant cell site area was likely far more precise for much of the location data obtained. The records reveal extensive details about Defendants' locations and movements throughout the seven months-long period. For Graham, over two thousand calls were initiated and terminated in different cell site sectors, indicating movement during the call. Some days offer particularly telling data. For example, during one 38-hour period in October 2010, Graham made and received 209 calls located in 55 different cell site sectors.

In United States v. Jones, —— U.S. ——, 132 S.Ct. 945, 181 L.Ed.2d 911 (2012), the Supreme Court unanimously held that the government's installation of a GPS device on a suspect's vehicle and its use of that device to track the vehicle's movements over a 28-day period violated the Fourth Amendment. See id. at 949, 954; id. at 964 (Alito, J., concurring in the judgment). A majority of the Court agreed that "longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." Id. at 955 (Sotomayor, J., concurring); id. at 964 (Alito, J., concurring in the judgment).[11] That conclusion was rooted in concerns about the government's ability to capture data describing an individual's movements and aggregate that data "to ascertain, more or less at will," private information about an individual, such as her "political and religious beliefs, sexual habits, and so on." Id. at 956 (Sotomayor, J., concurring). While the Justices left it an open question how long location surveillance could occur before triggering Fourth Amendment protection, Justice Alito clarified that "the line was surely crossed before the 4–week mark." Id. at 964.

Here, we confront a locational data set that is on the whole more invasive than the one considered in Jones. Admittedly, the CSLI acquired here, which could trace an individual to a neighborhood even if not to a specific address, was less precise than the GPS tracking information in Jones. "But precision is not the only variable with legal significance." United States v. Carpenter, 819 F.3d 880, 894–95 (6th Cir.2016) (Stranch, J., concurring). Quantity matters, too. And in my view, the sheer volume of data the government acquired here decides this case.[12]

***448** Whereas the Supreme Court deemed the government's collection of 28 days of location data unconstitutional, the data challenged here spans 221 days—nearly eight times the surveillance period

evaluated in Jones. The Eleventh Circuit concluded that a 67-day set of CSLI could "[w]ithout question ... when closely analyzed, reveal certain patterns with regard to [the defendant's] physical location in the general vicinity of his home, work, and indeed the robbery locations." United States v. Davis, 785 F.3d 498, 516 (11th Cir. 2015) (en banc). I have little trouble concluding that the close analysis of a 221-day CSLI set would reveal much more, potentially "enabl[ing] the Government to ascertain, more or less at will, [an individual's] political and religious beliefs, sexual habits, and so on." Jones, 132 S.Ct. at 956 (Sotomayor, J., concurring).

By acquiring vast quantities of Defendants' location information, spanning months, without Defendants' consent, the government infringed their reasonable expectations of privacy and thereby engaged in a search. Because that search was warrantless, it violated the Fourth Amendment.[13]

III.

Even more disquieting to me than the result the majority has reached today is the path it has chosen to reach it.

The majority does not decide, for instance, as did the Third Circuit, that the CSLI employed here was too imprecise or too discontinuous to infringe Defendants' privacy. See In re Application (Third Circuit), 620 F.3d at 312–13. That narrower holding would have allowed this Court to grapple, in the future, with the effect of rapidly changing phone technology, like the increasing "proliferation of smaller and smaller [cell sites] such as microcells, picocells, and femtocells—which cover a very specific area, such as one floor of a building, the waiting room of an office, or a single home," In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F.Supp.3d 1011, 1023 (N.D. Cal. 2015), or the advent of smartphone "pinging," whereby location data can be generated almost continuously, see, e.g., In re Application of U.S. for an Order Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F.Supp.2d 526, 534 (D. Md. 2011). Rather, the majority concedes what follows unavoidably from its holding: "the applicability of the Fourth Amendment [does not] hinge[ ] on the precision of CSLI," ante, at 426 n. 3, or on its quantity, ante, at 435–36. The Supreme Court has cautioned that "[w]hile the technology used in the present case [may be] relatively crude, the rule we adopt must take account of more sophisticated systems that are already ***449** in use or in development." Kyllo, 533 U.S. at 36, 121 S.Ct. 2038. Suppose the same case arises in two years, now featuring months of GPS-pinpointed location data, down to the second. Apply the majority's rule. Same result.

Neither does the majority hold, as the Eleventh Circuit did in the alternative, that the court order required by 18 U.S.C. § 2703(d), though less than a warrant backed by probable cause, nevertheless satisfied the Fourth Amendment's reasonableness "touchstone." See Davis, 785 F.3d at 516–18; id. at 521–24 (Jordan, J., concurring). That holding would have at least preserved a modicum of Fourth Amendment protection for the location data at issue here, requiring an evaluation of the relevant statutory provision that "assess[es], on the one hand, the degree to which [the search] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests." Id. at 517 (quoting Wyoming v. Houghton, 526 U.S. 295, 300, 119 S.Ct. 1297, 143 L.Ed.2d 408 (1999)). If that were the Court's holding, then the majority's token assurances that "Congress ... has not been asleep at the switch," ante, at 437, and my concurring colleague's laudatory musings about Congress's "striking a balance in an area rife with the potential for mass casualty," ante, at 440, might do more than salve our judicial consciences: they would actually be doctrinally relevant.[14] But as it is, Congress could repeal the SCA and the ECPA tomorrow. Apply the majority's rule. Same result.

What this elucidates is the extraordinary breadth of the majority's decision today. It is not bounded by the relative precision of location data, by the frequency with which it is collected, or by the statutory safeguards Congress has thought it prudent to enact. The majority's holding, under the guise of humble service to Supreme Court precedent, markedly advances the frontlines of the third-party doctrine. The Fourth Amendment, necessarily, is in retreat.

IV.

Only time will tell whether our society will prove capable of preserving age-old privacy protections in this increasingly networked era. But one thing is sure: this ***450** Court's decision today will do nothing to advance that effort. I dissent.

All Citations

824 F.3d 421

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

Footnotes

1 We reinstate the affirmance of Defendants' convictions and sentences and adopt the panel opinion with respect to all issues not addressed in this opinion. We note that, after en banc oral argument, Defendants moved to file supplemental briefing on a new claim, based on Johnson v. United States, ––– U.S. ––––, 135 S.Ct. 2551, 2554, 192 L.Ed.2d 569 (2015). Defendants argued, for the first time, that Johnson' s holding rendering 18 U.S.C. § 924(e) void for vagueness also renders void different language in § 924(c). We denied the motion as untimely. Even if we were to consider Defendants' late claim, however, it would not survive plain error review. United States v. Carthorne, 726 F.3d 503, 516 (4th Cir. 2013) ("An error is plain 'if the settled law of the Supreme Court or this circuit establishes that an error has occurred.' "). This court has not yet addressed this claim, and our sister circuits have divided on the issue. Compare United States v. Vivas–Ceja, 808 F.3d 719, 723 (7th Cir. 2015) (applying Johnson to find language identical to § 924(c) void for vagueness), and Dimaya v. Lynch, 803 F.3d 1110, 1120 (9th Cir. 2015) (same), with United States v. Taylor, 814 F.3d 340, 375–79 (6th Cir. 2016) (declining to find § 924(c) void for vagueness after Johnson).

2 As the Sixth Circuit explained, "[c]arriers necessarily track their customers' phones across different cell-site sectors to connect and maintain their customers' calls," and keep CSLI records "to find weak spots in their network and to determine whether roaming charges apply, among other purposes." United States v. Carpenter, 819 F.3d 880, 887 (6th Cir.2016).

3 Contrary to Defendants' suggestion, and unlike the information in Karo and Jones, the CSLI obtained here does not enable the government to "place an individual" at home or at other private locations. The historical CSLI at issue here does not provide location information anywhere near that specific. Rather, the record evidence establishes that each of the cell sites at issue here covers an area with a radius of up to two miles, and each data point of CSLI corresponds to a roughly 120-degree sector of a cell site's coverage area. That means the CSLI could only determine the four-square-mile area within which a person used his cell phone. Although we do not think the applicability of the Fourth Amendment hinges on the precision of CSLI, it is premature to equate CSLI with the surveillance information obtained in Karo and Jones.

4 Like these instances of government surveillance, when the government uses cell-site simulators (often called "stingrays") to directly intercept CSLI instead of obtaining CSLI records from phone companies, the Department of Justice requires a warrant. See Dep't of Justice, Department of Justice Policy Guidance: Use of Cell-Site Simulators 3 (2015), available at https://www.justice.gov/opa/file/767321/download.

5 Defendants argue that "[t]he government, not the cellular service providers, surveilled [them]." Defendants' En Banc Br. at 7. This is assertedly so because (1) the Communications Assistance For Law Enforcement Act, 47 U.S.C. § 1002 (2012) (CALEA), requires service providers to have the capacity to allow law enforcement to access CSLI, and (2) service providers use CSLI in the aggregate, while law enforcement analyzes individuals' CSLI to infer their location. Neither argument is sound. Miller involved a federal statute that similarly required a service provider (there, a bank) to create and maintain customer records, and the Supreme Court expressly held that the statute did not affect the applicability of the third-party doctrine. See Miller, 425 U.S. at 436, 440–44, 96 S.Ct. 1619. Moreover, the third-party doctrine does not require the government to use the third party's records in the same way the third party does. Third parties maintain records in the ordinary course of their own business. See Smith, 442 U.S. at 744, 99 S.Ct. 2577. That business is usually not crime-fighting. See, e.g., id. Thus, law enforcement will almost always use the accessed information for a different purpose and in a different way than the third party.

6 See, e.g., United States v. Wheeler, No. 15–216, ––F.Supp.3d ––––, ––––, 2016 WL 1048989, at *11–13 (E.D. Wis. Mar. 14, 2016) (Pepper, J.); United States v. Chavez, No. 3:14–185, 2016 WL 740246, at *2–4 (D. Conn. Feb. 24, 2016) (Meyer, J.); United States v. Epstein, No. 14–287, 2015 WL 1646838, at *4 (D.N.J. Apr. 14, 2015) (Wolfson, J.); United States v. Dorsey, No. 14–328, 2015 WL 847395, at *8 (C.D. Cal. Feb. 23, 2015) (Snyder, J.); United States v. Lang, No. 14–390, 78 F.Supp.3d 830, 834–37, at *3–4 (N.D. Ill. Jan. 23, 2015) (St. Eve, J.); United

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

States v. Shah, No. 13–328, 2015 WL 72118, at *7–9 (E.D.N.C. Jan. 6, 2015) (Flanagan, J.); United States v. Martinez, No. 13–3560, 2014 WL 5480686, at *3–5 (S.D. Cal. Oct. 28, 2014) (Hayes, J.); United States v. Rogers, 71 F.Supp.3d 745, 748–50 (N.D. Ill. 2014)(Kocoras, J.); United States v. Giddins, 57 F.Supp.3d 481, 491–94 (D. Md. 2014) (Quarles, J.); United States v. Banks, 52 F.Supp.3d 1201, 1204–06 (D. Kan. 2014) (Crabtree, J.); United States v. Serrano, No. 13–58, 2014 WL 2696569, at *6–7 (S.D.N.Y. June 10, 2014) (Forrest, J.); United States v. Moreno–Nevarez, No. 13–0841, 2013 WL 5631017, at *1–2 (S.D. Cal. Oct. 2, 2013) (Benitez, J.); United States v. Rigmaiden, No. 08–814, 2013 WL 1932800, at *14 (D. Ariz. May 8, 2013) (Campbell, J.); United States v. Gordon, No. 09–153–02, 2012 WL 8499876, at *2 (D.D.C. Feb. 6, 2012) (Urbina, J.); United States v. Benford, No. 09–86, 2010 WL 1266507, at *2–3 (N.D. Ind. Mar. 26, 2010) (Moody, J.); In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code Section 2703(d), 509 F.Supp.2d 76, 79–82 (D. Mass. 2007) (Stearns, J.). But see In re Application for Tel. Info. Needed for a Criminal Investigation, 119 F.Supp.3d 1011, 1024 (N.D. Cal. 2015) (Koh, J.); In re Application of U.S. for an Order Authorizing Release of Historical Cell–Site Info., 809 F.Supp.2d 113, 120–27 (E.D.N.Y. 2011) (Garaufis, J.).

7 Three of the state cases interpret broader state constitutional protections than the Fourth Amendment. See Commonwealth v. Augustine, 4 N.E.3d 846, 858, 467 Mass. 230 (2014) (finding "no need to wade into the [ ] Fourth Amendment waters" when the court could rely on article 14 of the Massachusetts Declaration of Rights); State v. Earls, 214 N.J. 564, 70 A.3d 630, 641–42 (2013) (explaining that New Jersey has "departed" from Smithand Millerand does not recognize the third-party doctrine); People v. Weaver, 12 N.Y.3d 433, 882 N.Y.S.2d 357, 909 N.E.2d 1195, 1201–02 (2009) ("[W]e premise our ruling on our State Constitution alone."). In addition to interpreting only the state constitution, the third case dealt with direct GPS surveillance by police, not CSLI records procured from a phone company. Weaver, 882 N.Y.S.2d 357, 909 N.E.2d at 1201–02. And the court in the fourth state case repeatedly pointed out that it was not considering "historical cell site location records"—like those at issue here—but "real time cell site location information," which had been obtained not through a § 2703(d) order, but under an order that had authorized only a "pen register" and "trap and trace device." Tracey v. State, 152 So.3d 504, 506–08, 515–16, 526 (Fla. 2014).

8 Defendants also emphasize the "highly private" nature of location information. Defendants' En Banc Br. at 13. But to the extent they do so to argue that the third-party doctrine does not apply to CSLI, they are mistaken. The third-party doctrine clearly covers information that is also considered "highly private," like financial records, Miller, 425 U.S. at 441–43, 96 S.Ct. 1619, phone records, Smith, 442 U.S. at 743–745, 99 S.Ct. 2577, and secrets shared with confidants, United States v. White, 401 U.S. 745, 749, 91 S.Ct. 1122, 28 L.Ed.2d 453 (1971).

9 If it were otherwise, courts would frequently need to parse business records for indicia of what an individual knew he conveyed to a third party. For example, when a person hands his credit card to the cashier at a grocery store, he may not pause to consider that he is also "conveying" to his credit card company the date and time of his purchase or the store's street address. But he would hardly be able to use that as an excuse to claim an expectation of privacy if those pieces of information appear in the credit card company's resulting records of the transaction. Cf. United States v. Phibbs, 999 F.2d 1053, 1077–78 (6th Cir. 1993) (Defendant "did not have both an actual and a justifiable privacy interest in ... his credit card statements.").

> Our dissenting colleagues similarly argue that the third-party doctrine requires specific "knowledge" on the part of the phone user about what information is being conveyed at the time. Because phone users usually do not "know[ ]" their own CSLI, the dissent argues, they cannot convey it. But the dissent cannot have it both ways: Accepting its premise as true for purposes of argument, we fail to see how a phone user could have a reasonable expectation of privacy in something he does not know. Indeed, the dissent rightly questions "whether anyone could credibly assert the infringement of a legitimate expectation of privacy" in "numbers dialed by someone else." The same logic would also apply to CSLI, which is created "by someone else"—and of which phone users, according to the dissent, are not even "aware."

10 Our dissenting colleagues posit that perhaps records of incoming calls have just not been challenged in court. They have been. See, e.g., In re Application of F.B.I., No. BR 14–01, 2014 WL 5463097, at *4 (Foreign Intel. Surv. Ct. Mar. 20, 2014) (listing courts that "have relied on Smith in concluding that the Fourth Amendment does not apply to ... incoming calls"); Reed, 575 F.3d at 914 (noting that there is "no Fourth Amendment expectation of privacy" in "call origination"

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

data); Sun Kin Chan v. State, 78 Md.App. 287, 300–01, 552 A.2d 1351 (Md. App. 1989) ("There is no constitutional distinction between the questions of 1) whom you call and 2) who calls you.").

11 Nor has this court ever suggested that other information typically contained in phone records—the date, time, and duration of each call, for example—merits constitutional protection. Yet a phone customer never "actively chooses to share" this information either. Rather, this information is passively generated and recorded by the phone company without overt intervention that might be detected by the target user. If individuals "voluntarily convey," all of this information to their phone companies, we see no basis for drawing the line at the CSLI at issue here. We note that this case deals with only 2010- and 2011-era historical CSLI, generated by texts and phone calls made and received by a cell phone.

12 In addition to being firmly grounded in the case law, the content/non-content distinction makes good doctrinal sense. The intended recipient of the content of communication is not the third party who transmits it, but the person called, written, emailed, or texted. The routing and addressing information, by contrast, is intended for the third parties who facilitate such transmissions.

13 Related concerns about a general "erosion of privacy" with respect to cell phones rest on a similar misapprehension of this distinction. These concerns revolve around protecting the large quantity of information stored on modern cell phones and on remote servers like the "cloud." See, e.g., Davis, 785 F.3d at 536 (Martin, J., dissenting). If all that information were indeed at risk of disclosure, we would share this concern. But documents stored on phones and remote servers are protected, as "content," in the same way that the contents of text messages or documents and effects stored in a rented storage unit or office are protected. See, e.g., United States v. Johns, 851 F.2d 1131, 1136 (9th Cir. 1988) (finding that a person renting a storage unit has a reasonable expectation of privacy in its contents); United States v. Speights, 557 F.2d 362, 363 (3d Cir. 1977) (finding reasonable expectation of privacy in secured locker at place of employment). These are clear limiting principles. Our holding today, that the Government may acquire with a court order, but without a warrant, non-content routing information (including historical CSLI), does not disturb those principles.

14 The lack of a bright line between permissible and impermissible amounts of CSLI also stands at odds with the Supreme Court's "general preference to provide clear guidance to law enforcement through categorical rules." Riley v. California, —— U.S. ——, 134 S.Ct. 2473, 2491, 189 L.Ed.2d 430 (2014).

15 We note, though, that such a rule would be unprecedented in rendering unconstitutional—because of some later action—conduct that was undoubtedly constitutional at the time it was undertaken. See United States v. Sparks, 750 F.Supp.2d 384, 392 (D. Mass. 2010), aff'd, 711 F.3d 58 (1st Cir. 2013) (recognizing the aggregation theory as "unworkable" because "conduct that is initially constitutionally sound could later be deemed impermissible if it becomes part of the aggregate").

16 For example, the Smith Court noted that, because a phone user who "had placed his calls through an operator ... could claim no legitimate expectation of privacy" in routing information exposed to that operator, "a different constitutional result" did not follow simply "because the telephone company has decided to automate." Smith, 442 U.S. at 744–45, 99 S.Ct. 2577. Similarly here, "a different constitutional result" does not follow because the telephone company has decided to make its phones mobile. Cf. United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012) ("Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system.").

17 Indeed, Congress has been actively considering changes to the ECPA in recent years based on advances in technology. See Jared P. Cole & Richard M. Thompson II, Congressional Research Service, Stored Communications Act: Reform of the Electronic Communications Privacy Act (ECPA), 8-10 (2015) (describing various proposed congressional amendments to the ECPA); Scott A. Fraser, Making Sense of New Technologies and Old Law: A New Proposal for Historical Cell–Site Location Jurisprudence, 52 Santa Clara L. Rev. 572, 576 (2012) (describing congressional fact-finding hearings on possible changes to the SCA). And some state legislatures have recently enacted warrant requirements for state agencies acquiring historical CSLI. See, e.g., Utah Code Ann. § 77-23c-102 (West 2015), amended by 2016 Utah Laws H.B. 369; N.H.

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

Rev. Stat. Ann. § 644-A:2-A:3 (West 2015). Legislatures manifestly can and are responding to changes in the intersection of privacy and technology.

*

My dissenting friend rightly lauds the function of judicial review, see Marbury v. Madison, 5 U.S. 137, 178, 1 Cranch 137, 2 L.Ed. 60 (1803), but effectively dismisses respect for Congress's efforts as one component of that review. See post at 449 n. 14. This, of course, envisions a process where the judiciary speaks only to itself, a curiously monologic exercise at odds with the constitutional structure of American government.

> Not to worry, says the dissent. All it is doing is "eliminating a single line of statutory text, specifically 18 U.S.C. § 2703(c)(1)(B)." Id. But "eliminating" a critical option Congress has provided in favor of the dissent's idea of what is best for us is the kind of constitutional club that ends the conversation and severely limits opportunities for legislative reforms and responses in what is a rapidly evolving field.

In accordance with the practice of my colleague, see United States v. Graham, 796 F.3d 332, 378 n.1 (4th Cir. 2015) (Motz, J., dissenting in part and concurring in the judgment), I have styled this opinion as a partial dissent. Even though I would affirm the Defendants' convictions under the exclusionary rule's good-faith exception, I take issue with the majority's determination that there was no Fourth Amendment violation, a conclusion which "will have profound consequences in future cases in the Fourth Circuit." *Id.*

2

Four other federal appellate courts have issued five decisions considering as a matter of first impression the applicability of the Fourth Amendment to CSLI, and those decisions generated seven concurring or dissenting opinions. See United States v. Carpenter, 819 F.3d 880, 884 (6th Cir.2016) (majority opinion); id. at 893–94 (Stranch, J., concurring); United States v. Davis, 785 F.3d 498, 500 (11th Cir. 2015) (en banc) (majority opinion); id. at 519 (W. Pryor, J., concurring); id. at 521 (Jordan, J., concurring); id. at 524 (Rosenbaum, J., concurring); id. at 533 (Martin, J., dissenting); United States v. Davis, 754 F.3d 1205 (11th Cir.) (unanimous), vacated, reh'g en banc granted, 573 Fed.Appx. 925 (11th Cir. 2014); In re Application of the U.S. for Historical Cell Site Data, 724 F.3d 600, 602 (5th Cir. 2013) (In re Application (Fifth Circuit)) (majority opinion); id. at 615 (Dennis, J., dissenting); In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to Gov't, 620 F.3d 304, 305 (3d Cir. 2010) (In re Application (Third Circuit)) (majority opinion); id. at 319 (Tashima, J., concurring). The only unanimous panel held that the government's warrantless acquisition of CSLI constituted a Fourth Amendment violation. Davis, 754 F.3d at 1215. No doubt, when the votes are tallied, more now support the majority's position. But that should not decide this case.

3

The majority argues that reading "voluntary conveyance" to require user knowledge would require courts "frequently ... to parse business records [such as credit card records] for indicia of what an individual knew he conveyed to a third party." Ante, at 430 n. 9. That argument is a bogeyman. Courts would not need to "parse" credit card records to determine whether the cardholder at a grocery knew he was conveying "the date and time of his purchase or the store's street address," id. any more than the Supreme Court had to "parse" Miller's bank records to determine whether he knew he was conveying the date, amount, or recipient name that appeared on the checks he himself had endorsed. That much was obvious from the nature of the record and the transactions it reflected. Where user knowledge cannot be easily ascertained in this manner, however, I would not force an ill-fitting presumption of voluntariness in order to strip Fourth Amendment protection from a defendant. See Ohio v. Robinette, 519 U.S. 33, 40, 117 S.Ct. 417, 136 L.Ed.2d 347 (1996) ("[V]oluntariness is a question of fact to be determined from all the circumstances." (quoting Schneckloth v. Bustamonte, 412 U.S. 218, 248–49, 93 S.Ct. 2041, 36 L.Ed.2d 854 (1973))).

4

See United States v. Forrester, 512 F.3d 500, 510 n.5 (9th Cir. 2008) ("Every computer or server connected to the Internet has a unique IP address. A website typically has only one IP address even though it may contain hundreds or thousands of pages. For example, Google's IP address is 209.85.129.104 and the New York Times' website's IP address is 199.239.137.200.").

5

One category of generally admitted third-party information would not be "voluntarily conveyed" under my reading of that requirement: phone records of incoming calls. See ante, at 431 – 32. Perhaps one reason such information is routinely admitted is that it is rarely challenged by defendants, since it is outgoing call information that tends to be incriminating, as was the case in the sole authority from this circuit cited by the majority. See United States v. Clenney, 631 F.3d

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

658, 662 (4th Cir. 2011) (investigator "confirmed through phone records that [defendant's] phone number was the source of outgoing calls"). Regardless, it is an open question whether anyone could credibly assert the infringement of a legitimate expectation of privacy in the numbers dialed by someone else (as one can in her movements over time, see infra section II). In other words, my view of "voluntary conveyance" may not require excluding warrantlessly procured incoming call information. Even if it did, that would be a small price to pay for preserving the substance of a constitutionally mandated limitation on the third-party doctrine's scope.

6 Indeed, it is the majority who has "improperly attempt[ed] to redefine the third-party doctrine." Ante, at 425; see also ante, at 429, 431. The majority recasts the Supreme Court's "voluntary conveyance" language in a double negative, such that "the third-party doctrine does not apply when an individual in voluntarily conveys information." Ante, at 431 (first emphasis added). The upshot of this approach is that the protections of the Fourth Amendment are limited to situations where "the government conducts surreptitious surveillance or when a third party steals private information." Id. While the majority might prefer to preserve Fourth Amendment protection only for information that is not coercively seized, that is not the Supreme Court's standard, and it should not be ours.

7 The majority "fail[s] to see how a phone user could have a reasonable expectation of privacy in something he does not know." Ante, at 430 n. 9. I wonder: does the majority imagine that Danny Kyllo knew what levels of infrared radiation emanated from his home and were recorded with precision by the government's thermal imaging device? See Kyllo v. United States, 533 U.S. 27, 29–30, 121 S.Ct. 2038, 150 L.Ed.2d 94 (2001). The rule that one must "know" what one can reasonably expect to keep private is new to me, and I believe to Fourth Amendment doctrine as well. It is also yet another aspect of this Court's present decision with troubling future implications. I suppose we can also expect no privacy in data transmitted by networked devices such as the "Fitbit" bracelet, which "can track the steps you take in a day, calories burned, and minutes asleep"; the "Scanadu Scout," which can "measure your temperature, heart rate, and hemoglobin levels"; or the "Mimo Baby Monitor 'onesie' shirt," which can "monitor your baby's sleep habits, temperature, and breathing patterns." Scott R. Peppet, Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent, 93 Tex. L. Rev. 85, 88 (2014); see also infra note 8. Making knowledge requisite to privacy is inconsistent not only with Supreme Court precedent but with our basic societal norms.

8 The majority does not take seriously this idea—that information might be automatically generated without user involvement. See ante, at 429 ("[T]here can be little question that cell phone users 'convey' CSLI to their service providers. After all, if they do not, then who does?"); id. ("Perhaps Defendants believe that ... the [service] provider just conveys CSLI to itself."). But even in the era of Miller and Smith, human beings were not the only entities capable of collecting and conveying information. That is also surely the case now, and will only become increasingly relevant going forward. See, e.g., Neil M. Richards, The Dangers of Surveillance, 126 Harv. L. Rev. 1934, 1940 (2013) ("The incentives for the collection and distribution of private data are on the rise. The past fifteen years have seen the rise of an Internet in which personal computers and smartphones have been the dominant personal technologies. But the next fifteen will likely herald the 'Internet of Things,' in which networked controls, sensors, and data collectors will be increasingly built into our appliances, cars, electric power grid, and homes, enabling new conveniences but subjecting more and more previously unobservable activity to electronic measurement, observation, and control."); Peppet, supra note 7, at 88–89. Today, the majority saddles us with a rule that does not distinguish between information an individual himself conveys and information that computerized devices automatically record, generate, and transmit. In other words, the majority's expansive interpretation of Miller and Smith will, with time, gather momentum—with effects increasingly destructive of privacy.

9 Because CSLI is not voluntarily conveyed by cell phone users, I find it unnecessary to wade into the murky waters that separate "content" from "non-content" information. The point of the "content" designation, as recognized by the Supreme Court, is that even some information that is voluntarily conveyed to (or routed through) third parties is nevertheless protected by the Fourth Amendment. For example, even though one voluntarily conveys information by speaking into a public telephone receiver, "the contents of [those] communications" are protected. Smith, 442 U.S. at 741, 99 S.Ct. 2577. The voluntarily conveyed content contained in a letter, Ex parte Jackson, 96 U.S. 727, 733, 24 L.Ed. 877 (1877), or in the body of an e-mail, United States v.

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.

Warshak, 631 F.3d 266, 288 (6th Cir. 2010), is protected, too. But where the information in question was never voluntarily conveyed in the first place, the third-party doctrine should have no application, even if that information is deemed "non-content."

10 This CSLI acquisition far eclipses any a federal appellate court has previously approved. Cf. Carpenter, 819 F.3d at 885–86 (considering two CSLI acquisitions, for separate defendants, spanning 88 and 127 days); Davis, 785 F.3d at 515 (CSLI acquisition spanning 67 days); In re Application (Fifth Circuit), 724 F.3d at 608 n.9 (CSLI acquisition spanning 60 days).

11 That is, five Justices agreed that longer-term location monitoring could violate an individual's reasonable expectation of privacy. Although the majority opinion was grounded in a trespass-based rationale, see id. at 949, it made clear that "[s]ituations involving merely the transmission of electronic signals without trespass would remain subject to [reasonable expectation of privacy] analysis," id. at 953.

12 The majority wonders "why ... only large quantities of CSLI [would] be protected by the Fourth Amendment." Ante, at 435. That is a fair question to ask of Defendants, who maintain that even smaller amounts of CSLI can be used to peer "into the home." Appellants' Br. at 20. In my view, however, the CSLI utilized here was not precise enough to implicate an individual's privacy interest in the home's interior. See United States v. Karo, 468 U.S. 705, 714–16, 104 S.Ct. 3296, 82 L.Ed.2d 530 (1984). Consequently, I consider the main privacy expectation infringed here to be in Defendants' movements over an extended period of time, which necessarily requires examining the quantity of data obtained. Furthermore, I agree that "[i]ntrinsic to the [third-party] doctrine is an assumption that the quantity of information an individual shares ... does not affect whether that individual has a reasonable expectation of privacy." Ante, at 436. That is, in part, why the majority's holding is so troublingly broad. See infra section III. But having determined that CSLI is not voluntarily conveyed, and thus that the third-party doctrine does not decide this case, I must evaluate separately whether a reasonable expectation of privacy has been infringed. Because the basis for my decision is extrinsic to the third-party doctrine, it is natural that I would not be bound by an "intrinsic ... assumption" of that doctrine.

13 "[A]s a general matter, warrantless searches 'are per se unreasonable under the Fourth Amendment....' " City of Ontario, Cal. v. Quon, 560 U.S. 746, 760, 130 S.Ct. 2619, 177 L.Ed.2d 216 (2010) (quoting Katz, 389 U.S. at 357, 88 S.Ct. 507). In my view, none of the "few specifically established and well-delineated exceptions" to that rule apply here. Id.

14 My concurring colleague joins the majority based on his "fear that by effectively rewriting portions of a federal statute under the guise of reasonableness review courts run the risk of boxing the democratic branches out of the constitutional dialogue." Ante, at 438. If that is truly the grounds for his concurrence, I hope my friend understands that the majority's opinion today will be the last word spoken in that "dialogue." It is a conversation ender. Following today's decision, the judiciary will have absolutely no role in articulating what protections the Fourth Amendment requires for private information that is not either directly gathered by the government or secretively stolen by third parties. We have thus avoided "boxing out" the other branches, but only at the cost of boxing out ourselves. So much for a "collaborative enterprise among the three departments of government." Ante, at 438. By the way, the statutory "rewriting" my colleague fears would require eliminating a single line of statutory text, specifically 18 U.S.C. § 2703(c)(1)(B). The efficiency of that modification is possible because Congress, as my colleague recognizes, provided in its "carefully tailored scheme," ante, at 439, that the government could acquire non-content customer information by obtaining a warrant. 18 U.S.C. § 2703(c)(1)(A). One wonders whether Congress itself might have anticipated the potential for a contrary decision today. Finally, although I appreciate my colleague's civics lesson on the institutional competencies of Congress, I would remind him of one of our own: judicial review. See Marbury v. Madison, 5 U.S. 137, 178, 1 Cranch 137, 2 L.Ed. 60 (1803).

© 2016 Thomson Reuters. No claim to original U.S. Government Works.

 © 2016 Thomson Reuters. No claim to original U.S. Government Works.