The Supreme Court’s recent opinion in Carpenter v. United States has set a course for rethinking Fourth Amendment rights in the digital age. It is the third bright star in the last seven years, marking a welcome and long overdue departure from the so-called “third-party doctrine” that has limited privacy rights for the last four decades. In a 5-4 decision, the Court ruled that police must usually get a warrant to access historical “cell site location information” (CSLI) — geographic data held by a cellphone service provider about where a device has connected to its network. It is a major win for privacy rights and it shines the way forward for future Fourth Amendment challenges: digital is different.

The question becomes, different how? And how far might Carpenter extend?

The case involves 127 days’ worth of Timothy Carpenter’s historical CSLI, obtained without a warrant or probable cause, and used to convict him for a string of robberies. On one level, the Court’s decision to require a warrant for such long-term location tracking is not surprising. In United States v. Jones, the Court ruled that 28 days of GPS tracking required a warrant. In Riley v. California, the Court required a warrant to search a cellphone incident to arrest, signaling its sensitivity to the wealth of private data stored on digital devices, including historic location information. The big wrinkle in Carpenter is that the police obtained the CSLI directly from the cellphone service provider, a third-party, instead of searching the defendant’s phone or using a GPS tracker.

For the last 40 years, the involvement of a third party has triggered the “third-party doctrine,” a rule dictating that there can be no reasonable expectation of privacy in personal information voluntarily shared with a “third party.” The doctrine comes from two cases, United States v. Miller and Smith v. Maryland, involving access to bank deposit slips and landline phone call records, respectively. In both instances, the Court held that a warrant is not required because the defendant “assumed the risk” that such business records “would be divulged to police.”

The doctrine has faced mounting criticism in recent years as more of daily life moves online and into the hands of third parties, including internet and cellphone service providers. Indeed, as Justice Sotomayor concurred in Jones, the rule 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.”

But compelled to follow Miller and Smith, most lower courts to consider the question found no privacy interest in CSLI because it had been conveyed to a third party. The big question in Carpenter was whether the Court would continue to apply the third-party doctrine in the digital age or somehow limit its reach.

BY MICHAEL PRICE

WWW.NACDL.ORG

THE CHAMPION
Chief Justice Roberts, writing for the Court, declined to “mechanically” apply the third-party doctrine to CSLI, describing it as “qualitatively different” from the records in Smith and Miller, and “an entirely different species of business record.” Instead of operating as a binary switch, the Court instructs, the doctrine should take into account “the nature of the particular documents sought” to determine whether there is a legitimate “expectation of privacy” concerning their contents. Here, the Court found that obtaining more than six days of CSLI requires a warrant, absent fact-specific exceptions like exigency.

This is a big doctrinal shift away from how many courts have understood and applied the third-party rule to date. Far from considering the underlying contents or nature of the information at issue, the doctrine has usually worked as a complete bar to Fourth Amendment protection for information shared with third parties. As Justice Thomas says in his dissent, Smith and Miller “announced a categorical rule: Once you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have had in it.” “This is true,” says Justice Kennedy in a separate dissent, “even when the records contain personal and sensitive information.” Instead, Kennedy continues, the Court appears to “establish a balancing test” for each “qualitatively different category of information.”

The majority, however, says that they are simply “declining to extend Smith and Miller to cover these novel circumstances.” As a result, the third-party doctrine poses no obstacle to finding a privacy interest in 127 days of CSLI, an “all-encompassing record of the holder’s whereabouts.”

Relying on two concurrences in Jones, the Court finds CSLI to be intensely private information. It “provides an intimate window into a person’s life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations.” CSLI contains the “privacies of life” and present even greater concerns than the GPS tracking in Jones because, building on Riley, a cellphone is “almost a ‘feature of the human anatomy’” that follows its owner into “private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” It also allows the government to “travel back in time to retrace a person’s whereabouts,” giving the police “access to a category of information otherwise unknowable.” It is increasingly precise, “approaching GPS-level precision.” The result is “a detailed chronicle of a person’s physical presence compiled every day, every moment, over several years” that implicates privacy concerns far beyond those considered in Smith and Miller. Carpenter further distinguishes CSLI from the records in Smith and Miller by recognizing that CSLI “is not truly ‘shared’ as one normally understands the term.” Instead, the Court reasons, cellphones have become “indispensable to participation in modern society”; they create CSLI “without any affirmative act” but also with “[v]irtually any activity”; and there is “no way to avoid leaving behind a trail of location data” short of disconnecting the phone from the network. In sum, there is no alternative to creating and conveying CSLI; it is a reality of the digital age that should not be confused with “‘assum[ing] the risk’ of turning over a comprehensive dossier of [one’s] physical movements” to the police.

Of course, CSLI is far from the only type of pervasive, invasive third-party data that works this way. Today, third-party service providers keep records detailing cellphone use, web browsing history, and most online activities. Online retailers keep track of what a user has purchased or merely perused. App makers log how users interact with their programs, and often much more. Companies like Google, Apple, and Facebook host private files and photos in the “cloud” while maintaining a frighteningly detailed log of user activity, both on and off their sites. Emailing, tweeting, instant messaging, surfing, searching, liking, and downloading all create an inescapable trail of third-party records that may raise constitutional concerns on par with CSLI.

Justice Roberts calls CSLI “unique” and insists that the Court’s decision is a “narrow one,” declining to express a view on real-time CSLI or “tower dumps.” But as Justice Breyer quipped at oral argument, “This is an open box. We know not where we go.” CSLI may be a different “species” of third-party records, but like Darwin in the Galapagos, the Court may soon begin to discover other new species of protected data that implicate the same “basic Fourth Amendment concerns” as CSLI and demand a warrant.

Even the use of “conventional” surveillance tools, like security cameras, which Carpenter says it does not “call into question,” may be open to challenge if used in conjunction with other new technologies like real-time facial recognition or automatic license plate readers. Using such software on a dense network of cameras could raise the same privacy concerns around location tracking that motivated the majority in both Carpenter and Jones.

None of this was lost on the Court’s four dissenters, Justices Kennedy, Thomas, Alito, and Gorsuch. Justice Kennedy would have continued to apply Smith and Miller in full force, fearing “undue restrictions” on law enforcement. He writes that property law principles should form a “baseline” for determining reasonable expectations of privacy, and that CSLI belongs to cellphone service providers, not individual users. He also chides the majority for not “explain[ing] what makes something a different category of information.” According to Kennedy, Carpenter provides no principled way of telling whether credit card records, digital wallet data, or cellphone call details should receive the same treatment as CSLI. The same is true, he continues, for IP address information and website browsing history. Kennedy meant it as a warning, but it could easily double as a to-do list for defense lawyers and privacy advocates.

Justice Thomas looks beyond Smith and Miller and identifies the source of the problem as Katz v. United States, which gave rise to the reasonable expectation of privacy test. Katz is “a failed experiment” that the Court is “dutybound” to reconsider, Thomas writes, arguing that it strays from the text of the Fourth Amendment and has become unworkable. Like Justice Kennedy, Thomas would tie Fourth Amendment rights to property law. Thomas finds it telling that Carpenter “cites no property law in briefs to this Court” and “does not explain how he has a property right in the companies’ records under the law of any jurisdiction at any point in American history.”

Likewise, Justice Alito finds “no plausible ground” to maintain that CSLI qualifies as Carpenter’s “papers” or “effects” for Fourth Amendment purposes. He also sounds the alarm about a potential “upheaval” in the way grand jury subpoenas work. Carpenter is “revolutionary,” according to Alito, because it imposes a probable cause standard on the compulsory production of CSLI. And “nothing stops its logic from sweeping much further.” One possibility, Alito concludes, is that “all other orders compelling the production of documents will require a
demonstration of probable cause” if they contain sensitive personal information. Whether this is a warning or an invitation likely depends on one’s perspective.

Finally, Justice Gorsuch joins Justice Thomas in criticizing the Katz framework that gave rise to the third-party doctrine. But unlike the other dissenters, Gorsuch is hostile to the third-party doctrine and concerned about its implications in the digital age. Indeed, one might mistake the Gorsuch dissent for a concurrence. “What’s left of the Fourth Amendment?” Gorsuch asks, noting that “[e]ven our most private documents — those that, in other eras, we would have locked safely in a desk drawer or destroyed — now reside on third-party servers.”

Most immediately, it frees lower courts from the dead hand of Smith and Miller to protect data of comparable “depth, breadth, and comprehensive reach” to CSLI. Building on Jones and Riley, Carpenter also makes it clear that the Court is willing to reconsider old doctrines that do not fit with the realities of the digital age. In that sense, Carpenter caps a trinity of cases that may spell a welcome rebirth of Fourth Amendment rules for years to come.

Notes
3. Riley v. California, 134 S. Ct. 2473, 2490 (2014) (“Historic location information is a standard feature on many smartphones and can reconstruct someone’s specific movements down to the minute, not only around town but also within a particular building.”).
5. Smith, 442 U.S. at 745.
8. See United States v. Thompson, 866 F.3d 1149 (10th Cir. 2017); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (en banc); Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
10. Id. at *11.
11. Id. at *9, n.3; *15.
12. One notable exception is email. See United States v. Warshak, 631 F.3d 266, 285–286 (6th Cir. 2010) (email “is the technological scion of tangible mail” and it would “defy common sense to afford emails lesser Fourth Amendment protection.”).

About the Author
Michael Price is NACDL’s Senior Litigation Counsel.

Michael Price
NACDL
Washington, DC
202-465-7615
mprice@nacdl.org
www.nacdl.org
@NACDL