Spring 3-1-2019

Protecting Electronic Privacy

Erwin Chemerinsky
Berkeley Law

Recommended Citation
103 Judicature 76 (2019)

VOLUME 103 NUMBER 1 SPRING 2019
Judicature
Published by the Bolch Judicial Institute at Duke Law. Reprinted with permission.
judicialstudies.duke.edu/judicature

Protecting Electronic Privacy

BY ERWIN CHEMERINSKY

***Carpenter v. United States*, decided by the Supreme Court in June 2018, is one of the most important decisions applying the Fourth Amendment to the technology of the 21st century.**[1] The Court held that police may obtain significant cellular location information — information that can be used to determine where a person was at a particular time — only if there is a warrant based on probable cause or exigent circumstances. The ruling is a strong affirmation of the right to privacy under the Fourth Amendment. Yet the decision raises more questions than it answers, presenting issues that are now facing the lower courts and that ultimately will need to be resolved by the Supreme Court.

FACTS

Timothy Carpenter was suspected of committing a series of armed robberies. The FBI went to his cell phone provider and got the cell phone tower records — the cell site location information ("CSLI") — that revealed his location and his movements for 127 days. The FBI received this information without a warrant, though it had obtained a court order from a judge pursuant to the federal Stored Communications Act. The key difference is that probable cause — which is required for a warrant — is not needed under the Stored Communications Act. The cell tower information was crucial evidence used to convict Carpenter and sentence him to 116 years in prison.

Every time a cell phone sends and receives calls, texts, or emails or accesses the internet, it connects to cell towers. The resulting records — generated hundreds and sometimes thousands of times per day for a single phone — include the precise GPS coordinates of each tower as well as the day and time the phone tried to con-

nect to it. It is possible to determine a person's location and movements at almost any point in time with this information. The police constantly use this technology: In 2016, Verizon and AT&T alone received a total of about 125,000 requests for cellular information from law enforcement agencies.

The United States District Court for the Eastern District of Michigan denied Carpenter's suppression motion and allowed the cellular location records to be used as evidence against him. The United States Court of Appeals for the Sixth Circuit affirmed. The issue before the Supreme Court in *Carpenter v. United States* was whether the Fourth Amendment, which prohibits unreasonable searches and arrests, requires that the police obtain a warrant in order to access this information. The Court, in a 5-4 decision, reversed the lower courts and ruled in favor of Carpenter. Chief Justice John Roberts wrote the opinion for the Court, which was joined by Justices Ruth Bader Ginsburg, Stephen Breyer, Sonia Sotomayor, and Elena Kagan. Each of the four dissenters — Justices Anthony Kennedy, Clarence Thomas, Samuel Alito, and Neil Gorsuch — wrote a separate opinion.

THE OPINIONS

Chief Justice Roberts's opinion stressed that accessing a person's cellular location information for a long period of time seriously intrudes on privacy. He wrote: "Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's whereabouts. As with GPS information, the time-stamped data 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.' These location records hold for many Americans the 'privacies of life.'"[2]

The Court analogized this case to *Riley v. California*,[3] which had held a few years earlier that police cannot look at the content of a person's cell phone as part of a search incident to arrest without a warrant or unless emergency circumstances justify a warrantless search. In *Riley*, in an opinion also by Chief Justice Roberts, the Court emphasized the privacy interests that people have in the content of their cell phones. Virtually everyone has a cell phone on which we store deeply personal information.

The government's primary argument to the Court — and the reason the federal district court and the Sixth Circuit ruled against Carpenter — was that he had no reasonable expectation of privacy because he had voluntarily shared this information with a third party. The "third-party doctrine" provides that we have no privacy interest in information that we share with a third party. In 1979, the Court found in *Smith v. Maryland* that the phone company constituted a "third party" for purposes of this doctrine, holding that police do not need a warrant to obtain from the phone company a record of the numbers that we dial or receive calls from because we should not be able to expect that the third party — the phone company — will keep the information secret.[4] The Court has also used the third party doctrine to hold, in the 1976 case of *United States v. Miller*, that the police can obtain our banking information, such as records of our deposits and withdrawals, without a warrant because a third party — the bank — has the information.[5]

Justice Sotomayor has been very critical of the third-party doctrine, saying that it "is ill suited to the digital age."[6] She has explained that we live in an era "in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[7]

But the Court in *Carpenter* said that it was neither reconsidering the third-party doctrine nor applying the doctrine to stored cellular location information. Chief Justice Roberts wrote: "We decline to extend *Smith* and *Miller* to cover these novel circumstances. Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[8] The Court stressed the extensive information that could be learned from stored cellular location information as compared with the amount of information that could be obtained in the earlier cases and declared: "There is a world of difference between the limited types of personal information addressed in *Smith* and *Miller* and ▸

The "third-party doctrine" provides that we have no privacy interest in information that we share with a third party. . . . But the Court in *Carpenter* said that it was neither reconsidering the third-party doctrine nor applying the doctrine to stored cellular location information.

the exhaustive chronicle of location information casually collected by wireless carriers today. The Government thus is not asking for a straightforward application of the third-party doctrine, but instead a significant extension of it to a distinct category of information."[9] The Court thus concluded that because obtaining the information is a search, it requires a warrant based on probable cause unless there are emergency circumstances.

Each of the four dissenters objected on different grounds. Justice Kennedy stressed the third-party doctrine and the traditional power of the government to obtain information by compulsory process, rather than needing a warrant based on probable cause. He emphasized: "Cell-site records . . . are no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process. Customers like petitioner do not own, possess, control, or use the records, and for that reason have no reasonable expectation that they cannot be disclosed pursuant to lawful compulsory process."[10]

Justice Thomas, by contrast, expressed his view that the scope of the Fourth Amendment is determined by property rights. He strongly objected to approaching the Fourth Amendment based on the protection of the "reasonable expectation of privacy," which has been the law since *Katz v. United States* in 1967.[11] Justice Thomas described the *Katz* test as "a failed experiment" and did not see the Fourth Amendment as protecting privacy, including Carpenter's privacy.[12] For Thomas, there was a search under the Fourth Amendment only if there was an intrusion on constitutionally protected property interests.

Justice Alito emphasized that the Court's decision threatens to change the law in the myriad situations in which the government obtains information, even very private information, through court orders and subpoenas. He said these are not searches and should not be governed by the Fourth Amendment. He concluded his dissent by declaring: "The desire to make a statement about privacy in the digital age does not justify the consequences that today's decision is likely to produce."[13]

> The holding of *Carpenter* is clear: From now on, if police want to obtain significant stored cellular location information, there must be a warrant based on probable cause or exigent circumstances that justify an exception to the warrant requirement. But the decision raises many other questions that it does not answer.

Finally, Justice Gorsuch, like Justice Thomas, saw the Fourth Amendment as protecting property interests; he, too, found fault with the *Katz* test and the focus on a reasonable expectation of privacy. He criticized Carpenter for failing to present a claim based on intrusion into his property rights.

THE UNANSWERED QUESTIONS

The holding of *Carpenter* is clear: From now on, if police want to obtain significant stored cellular location information, there must be a warrant based on probable cause or exigent circumstances that justify an exception to the warrant requirement. But the decision raises many other questions that it does not answer.

First, what about all of the instances in which police obtained stored cellular location information without a warrant before June 22, 2018, the day *Carpenter* was decided? For cases in which decisions are final and no longer pending in the trial court or on appeal, *Carpenter* will have no effect. Rarely do Supreme Court decisions concerning criminal procedure apply retroactively, and never has the Court found a decision about the scope of the Fourth Amendment to apply retroactively.

Carpenter does apply to any cases pending in trial or appellate courts at the time it was decided. But practically speaking, *Carpenter* will not work to exclude the evidence in these cases, either. The Court has held that the exclusionary rule does not apply if police act in good faith; the exclusionary rule applies only if police intentionally or recklessly violate the Fourth Amendment.[14] Prior to *Carpenter*, police were acting in good faith in obtaining stored cellular location information without a warrant because the new rule did not yet exist, so there is no basis for excluding this evidence. Indeed, lower courts since *Carpenter* have come to this conclusion.[15]

Second, *Carpenter* leaves open the question of whether police access to other types of cellular tower information will require a warrant based on probable cause. Chief Justice Roberts, writing for the Court, stated: "Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or 'tower dumps' (a download of information

on all the devices that connected to a particular cell site during a particular interval)."[16] It remains unsettled if police will need a warrant if they want to obtain cellular location information for a short period of time, unlike the 127 days in *Carpenter*, including if they want to access it in "real time." While those scenarios still provide ample opportunity to learn private information about a person, they do not furnish law enforcement with as much information as would an extended period of time. Regardless, my sense is that the reasoning of *Carpenter* — that cellular location information reveals private information — will cause courts to extend it to all instances in which police are seeking to obtain these records.

"Tower dumps" pose a fascinating Fourth Amendment issue. Obtaining a "tower dump" means obtaining a list of all of the cellular devices that communicated to a cell tower at a particular time. For example, if used in the *Carpenter* case, police could obtain a list of all cell phones that communicated to the towers near each of the armed robberies. They then could see if any phone was near all of those towers at the times of all of the robberies. If, say, Carpenter's phone was near the locations of all of the robberies, could that fact be used as evidence against him? Obtaining a tower dump would likely indicate Carpenter's proximity to the crimes, as would obtaining his stored cellular location information. But a tower dump would *only* reveal that his phone was near the cell towers of the robberies when they happened — far less private information than revealed by stored cellular location information.

Third, what is the future of the third-party doctrine? The Court was careful to say that it was not overruling or changing the doctrine but did not offer a clear explanation as to why it did not apply, other than to make a distinction based on the amount of information that can be learned about a person from stored cellular location information. More generally, it is unclear when police will need a warrant based on probable cause, rather than a subpoena or a court order, to obtain other kinds of private information, such as medical records. This was a key point in the dissents of Justices Kennedy and Alito and is sure to lead to a great deal of litigation.

CONCLUSION

In 1928, in *Olmstead v. United States*, the Supreme Court held that wiretapping, essentially electronic eavesdropping, is a search requiring a warrant only if the police physically enter a person's property.[17]

It took almost 40 years, but the Court finally brought the Fourth Amendment into the 20th century in 1967 in *Katz v. United States*, when the Court found that the Fourth Amendment protects people — not property — and that there is a "search" if there is an infringement of the reasonable expectation of privacy.[18]

In recent decisions, including *Carpenter*, the Court has said that there is a search if there is an intrusion either on constitutionally protected property rights or on the reasonable expectation of privacy. Cases like *Carpenter* and *Riley* are important because they apply the Fourth Amendment to the technology of the 21st century. New technologies have given police enormously expanded power to monitor our movements and our communications. But they also raise profoundly difficult questions about balancing privacy rights and law enforcement needs. The one thing that can be said with certainty: Cases like *Carpenter* and *Riley* are just the beginning of the Court's applying the Fourth Amendment to modern technology.

ERWIN CHEMERINSKY is Dean and Jesse H. Choper Distinguished Professor of Law at the University of California, Berkeley School of Law. He frequently argues appellate cases, including in the United States Supreme Court. He is the author of eleven books, including leading casebooks and treatises about constitutional law, criminal procedure, and federal jurisdiction.

1 *Carpenter v. United States*, 138 S. Ct. 2206 (2018).

2 *Id.* at 2217.

3 *Riley v. California*, 134 S. Ct. 2473 (2014).

4 *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

5 *United States v. Miller*, 425 U.S. 435, 443 (1976).

6 *United States v. Jones*, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

7 *Id.*

8 *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018).

9 *Id.* at 2219.

10 *Id.* at 2224 (Kennedy, J., dissenting).

11 *Katz v. United States*, 389 U.S. 347 (1967).

12 *Carpenter*, 138 S. Ct. at 2246 (Thomas, J., dissenting).

13 *Id.* at 2261 (Alito, J., dissenting).

14 *Herring v. United States*, 555 U.S. 135, 147 (2009).

15 *See, e.g., United States v. Chavez*, 894 F.3d 593, 608 (4th Cir. 2018) (holding that good-faith exception to the exclusionary rule applied to investigators who obtained defendant's cell phone records without a warrant).

16 *Carpenter*, 138 S. Ct. at 2220.

17 *Olmstead v. United States*, 277 U.S. 438, 466 (1928).

18 *Katz v. United States*, 389 U.S. 347, 353 (1967).