How Private is Your Cellphone? The Next Fourth Amendment Challenge

By **Deanna Paul** | August 15, 2017

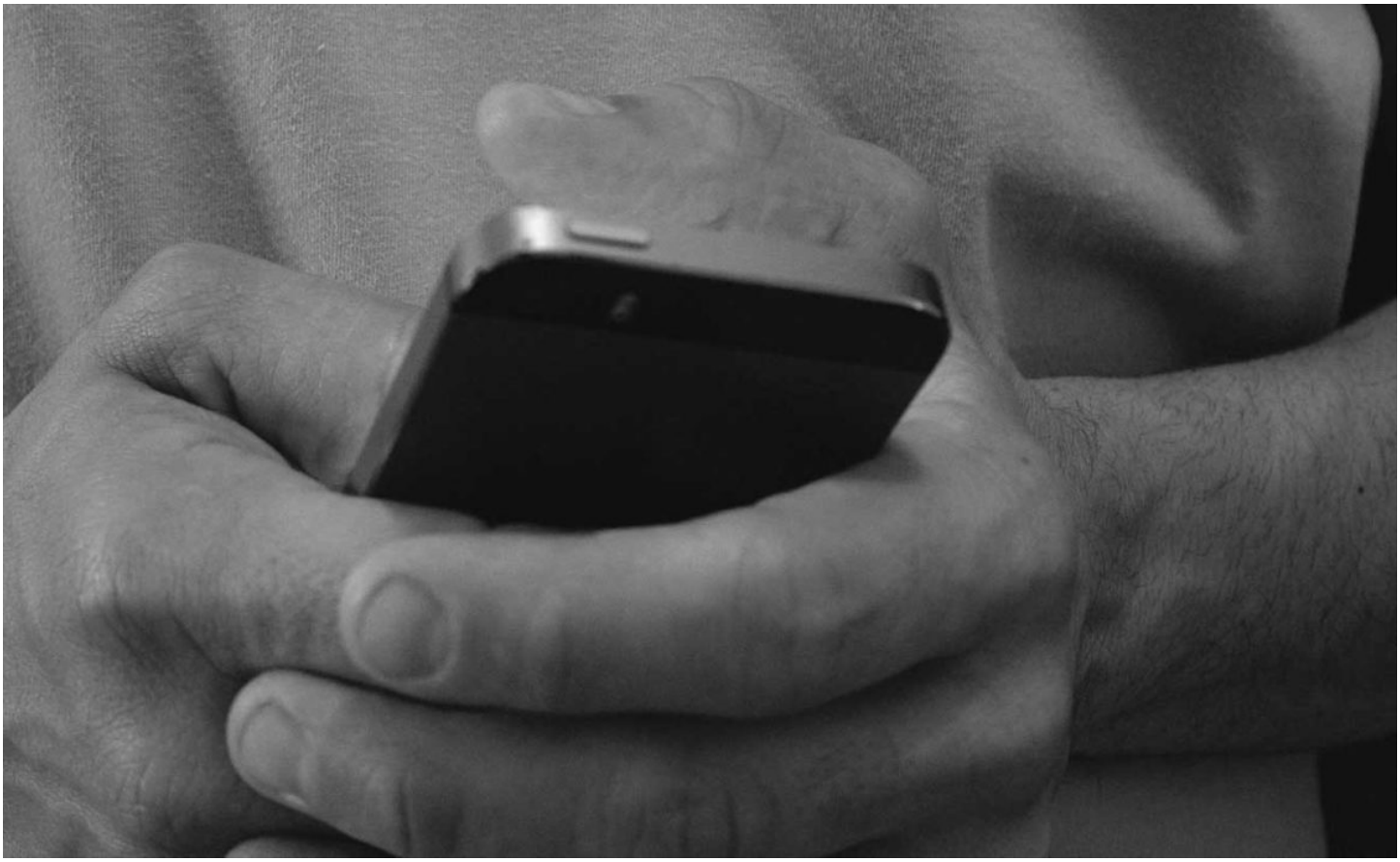

Photo by Victor via Flickr

Most people know that very little they do on the web is private. The terabytes of data held online contain personal information accessible not only to friends, relatives and would-be employers, but to private businesses, which frequently collect user information in order to deliver better services to customers.

Can the government see it too?

In 1979, the Supreme Court ruled in *Smith v. Maryland* (https://www.oyez.org/cases/1978/78-5374) that Fourth Amendment protections against warrantless searches do not cover such "third party" access to online data. In what has since been developed as the "Third Party Doctrine," the court ruled that an individual has no legitimate expectation of privacy for information voluntarily given to a third party—be it a person, bank, or phone carrier—information that is also then similarly available to government agencies.

But what are government agencies, such as law enforcement, constitutionally permitted to *do* with the data they collect? A case before the Court next month may help answer the question.

Carpenter v. United States (https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/05/supreme-court-agrees-to-hear-carpenter-v-united-states-the-fourth-amendment-historical-cell-site-case/?utm_term=.8c8ed9185780) has the potential to affect application of the Fourth Amendment's Third Party Doctrine in the digital age.

The case involves a string of robberies, allegedly organized by the defendant, Timothy Carpenter, which occurred over a two-year period. Police acquired cell site location information (CSLI) associated with the phone he used. Although no search warrant was ever obtained, a judge did sign a court order under the Stored Communications Act (https://www.law.cornell.edu/uscode/text/18/2701), a statute that requires reasonable suspicion, not probable cause.

The CSLI records revealed Carpenter's location and movements over 127 days and showed that during the five-month period his phone was in communication with cell towers near the crime scenes.

Although there is a tendency to read *Smith v. Maryland* as a blanket rule, where anything given to or accessed by a third party has no Fourth Amendment interest, it doesn't make sense to apply a doctrine created over 30 years ago to types of communications and data that were neither used at the time nor contemplated by the Court.

"Given how much [of] our data goes through third parties, if you take a strong reading of the Doctrine, it essentially wipes out Fourth Amendment protections for most modern communications," Michael Price, Senior Counsel for the Liberty and National Security Program at New York University's Brennan Center for Justice, told me. (https://www.brennancenter.org/)

"There is also nothing about location information in *Smith*. To rely on it, and say that location information should be accessible without a warrant, is reading the case far too broadly."

Price's point is an important one.

To analogize cases is to suggest they should be treated the same under the law and receive the same level of protection. Although the facts may specifically involve cell-site information, *Carpenter* is about more than just location privacy. Here, as is increasingly the case with Internet-of-Things-based prosecutions, a third-party server already had access to the sought after location data.

Deanna Paul

Carpenter presents the first chance for the Court to reconsider Fourth Amendment protections against warrantless searches and seizures of information generated and collected by the many modern technologies we use every day.

This is an opportunity at least one Supreme Court Justice has recognized.

In 2012, the Court resolved the issue of location privacy in *United States v. Jones* (https://www.law.cornell.edu/supremecourt/text/10-1259) , holding that installation of a Global Positioning System (GPS) tracking device on a vehicle and using it to monitor the vehicle's movements constitutes a search under the Fourth Amendment. In her concurrence, Justice Sonia Sotomayor wrote that the current approach to these cases 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"

She suggested it may need to be rethought in the future.

There are signs from recent cases, like *Jones,* that the Justices are aware of the importance of technology in contemporary life. They appear to recognize that technology is significantly different today than it was ten years ago, let alone when the Court was deciding cases like *Smith*.

Cellular phones have become essential to freedom of speech and First Amendment rights.

Riley v. California (http://www.scotusblog.com/case-files/cases/riley-v-california/) was the first time the Supreme Court identified the central role that cellphones have in today's society, holding that police need a warrant to search a smart phone belonging to a person who has been arrested. Writing for the majority in 2014, Chief Justice John Roberts said that cell phones have "such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."

The *Riley* Court went on to say that cellular phones have become essential to freedom of speech and First Amendment rights and, due to the volume and personal nature of the information that can be stored on a cellphone, the data should be presumptively protected by the First Amendment. The decision notes that a cell phone can double as a diary, camera, calendar, or newspaper, which makes the search of one fundamentally different from a physical search or even a search of business records.

"This is an important decision, in terms of First Amendment protections, showcasing the Supreme Court's comfort with new technology and that it is cognizant of the impact of digital information," said Andrew Ferguson of the David A. Clarke School of Law at the University of District Columbia, and a national expert on predictive policing and the Fourth Amendment,

See also: Digital Privacy Rights of Probationers (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3015480)

Similarly, earlier this year, the Court decided *Packingham v. North Carolina* (http://www.scotusblog.com/2017/06/opinion-analysis-court-invalidates-ban-social-media-sex-offenders/) , which addressed the prevalence and necessity of the internet and social media in a digitized society.

Riley embodies the idea that new technologies and the digital space are different, yet fails to view these devices for what they are rather than what they're most similar to. A cell phone is not a diary, calendar or any of the technologies cited by by the Court, and to draw a series of slightly-off-the-mark analogies and suggesting they should be treated the same, is not a solution.

In reviewing *Carpenter*, there are only a few scenarios for the Court—each of which will have lasting implications.

The Court might opt to temporarily put tape over the problem, hiding behind the Third Party Doctrine and wait for the next case to make its way up.

Or it could limit the Doctrine's application to CSLI and recognize that carrying a cellular phone does not, in and of itself, amount to consenting to location tracking.

"One of the difficulties the Court is confronted with is that the Doctrine, as it's been created, doesn't offer a nice neat answer," said Ferguson. "The Court may have to rethink their traditional approach to the Fourth Amendment in order to address this new technological threat to privacy and security.

"The other difficulty is: If *Carpenter* is really about the future of the Third Party Doctrine, it is about far more than just cell site records—it is about the future of a data-driven third party mediated age."

That is a huge question to answer. And, due to the far-reaching consequences any of the scenarios the Court may chose, the Court may also just decide to punt it to a future case.

There are few things we do online that aren't connected, in some way, to a third party. As smartphone technology continues to advance, more and more aspects of our lives will be recorded and stored on third-party servers. Lower courts across the country are only just beginning to consider how the Internet of Things will affect our expectations of privacy.

Carpenter is an opportunity for the Supreme Court to reconceive how privacy and security values can be protected in an era of increasingly sophisticated surveillance technologies that allow us to remotely control the lights and heat in our homes or monitor intruders.

Let's hope the Justices take it.

Deanna Paul (@thedeannapaul (https://www.twitter.com/thedeannapaul)) is a former New York City prosecutor and adjunct professor of trial advocacy at Fordham University School of Law. This fall she will begin attending Columbia University's graduate school of journalism. Her nonfiction work has been published by The Marshall Project*,* Rolling Stone*, and* WIRED.