10-3-2018

Privacy and the New Age of Technology

Odelia Nikfar
Cardozo Arts & Entertainment Law Journal

Privacy and the New Age of Technology

BY ODELIA NIKFAR/ ON OCTOBER 3, 2018

This past June, the Supreme Court decided the case *Carpenter v. United States*,[1] which some may call one of the most influential and important opinions of our time. This case calls into question the government's access to information provided by a device that is most probably within one foot of you right now. That's right – your cell phone. The issue presented in this case is whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements.[2]

In 2011, police officers arrested four men suspected of robbing a series of Radio Shack and T-Mobile stores in Detroit.[3] One of the men confessed to the crime and identified others who

had been accomplices, giving over their phone numbers to the FBI.[4] The FBI used this information to apply for court orders to obtain phone records for petitioner Timothy Carpenter, under the Stored Communications Act.[5] Federal Magistrate Judges issued the orders and the government was able to obtain the information they requested.[6] Carpenter moved to suppress the cell-site data provided by the phone carriers, arguing that his Fourth Amendment rights were violated when the Government seized his records.[7]

The Court of Appeals for the Sixth Circuit held that Carpenter lacked a reasonable expectation of privacy in the location information, because he shared that information with his wireless carriers.[8] In its reasoning, the Sixth Circuit essentially applied the third-party doctrine, which the government argued is controlling.[9] The third-party doctrine, which was decided in *Smith v. Maryland*[10] and *United States v. Miller,**[11]* dictates that a person does not have a reasonable expectation of privacy in information voluntary given to a third party.[12] Here, the Court correctly held that given the unique nature of cell phone location records, the third-party doctrine does not in itself overcome a person's Fourth Amendment protection.[13] The Court explained that this old doctrine does not apply to this new technology. The Court opined that there is a difference in the data at issue in this case and the data in the previous cases governed by the third-party doctrine. The type of data relevant in this case is much more intimate and sensitive than the information in earlier cases. The Court explained "when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."[14] This type of technology can allow the Government to track someone retrospectively, whereas if the Government wanted to track someone before, they would only be able to track him or her once a device was installed.[15]

Ultimately, the court did not overturn the third-party doctrine, but this decision weakens it. Technology has transformed our society into a very different world than the that of *Smith**[16]* and *Miller**[17]*. To say that a person voluntarily gives information to a third party through simply having a smartphone is using an old doctrine and mistakenly applying it to current times. In order to be an interactive member of today's society, a person does not have a meaningful choice in providing this information to wireless carriers. Whether it be through location tracking or any other type of information stored on a smartphone, it is an inappropriate extension of the third-party doctrine to claim that a person has no expectation of privacy because the information was shared with the wireless carrier, or other relevant third party.

The *Carpenter* decision is not limited to location data, but reaches farther to include any type of information collected by popular technologies.[18] Nathan Freed Wessler, a staff attorney at the ACLU who argued this case in front of the Supreme Court, explained, "[i]f the government had its way, virtually none of our sensitive information held by tech companies would enjoy the privacy rights guaranteed by the Constitution."[19] Imagine the consequences of this: anything posted on any social media site would be accessible to the Government. The information stored on your phone from your medical apps to your dating

apps, would all be accessible by the Government. The Supreme Court's decision in this case is the first step in protecting consumers from such a situation.

This case is especially relevant in wake of recent hearings lawmakers have had with leaders of tech companies regarding the need to strengthen online privacy. These hearings have highlighted the challenges of what legislation could entail especially for Internet companies who monetize the information they gather.[20] On the bright side, it appears that these hearings highlighted a bipartisan agreement on the same goal: to reach consensus on data privacy law.[21] This area of the law is relevant to anyone who owns a smartphone, and I am almost certain that that includes you.

Odelia Nikfar is a second-year law student at Benjamin N. Cardozo School of Law and a Staff Editor of the Cardozo Arts & Entertainment Law Journal. She will be a clinical legal intern on Cardozo's Tech Start-up Clinic in the spring semester and is interested in the nexus of technology and Constitutional Law.

[1] 138 S.Ct. 2206 (2018).

[2] *Id.* at 2211, 2216.

[3] *Id.* at 2212.

[4] *Id.*

[5] *Id.*; 18 U.S.C. § 2703 (2010).

[6] *Carpenter*, *supra* note 1 at 2212.

[7] *Id.*

[8] *Id.* at 2213.

[9] *Id.* at 2216-20.

[10] 442 U.S. 735, 752 (1979).

[11] 425 U.S. 435, 456 (1976).

[12] *Smith*, 442 U.S., at 743-744.

[13] *Carpenter*, 138 S.Ct. at 2217.

[14] *Id.* at 13.

[15] *Id.*

[16] *Supra* note 10.

[17] *Supra* note 11.

[18] Nathan Freed Wessler, *The Supreme Court's Groundbreaking Privacy Victory for the Digital Age*, ACLU (June 22, 2018, 2:30 PM) https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age.

[19] *Id.*

[20] John D. McKinnon & Douglas MacMillan,*Tech Executives Warn of Overregulation in Privacy Push*, The Wall Street Journal (Sept. 26, 2018, 2:49 PM) https://www.wsj.com/articles/tech-executives-warn-of-overregulation-in-privacy-push-1537987795?mod=searchresults&page=1&pos=3

[21] *Id.*