MERCATUS CENTER
George Mason University

TESTIMONY

# CLARIFYING THE LAW CAN HELP NEW HAMPSHIRE PROTECT ITS CITIZENS' PRIVACY

**Brent Skorup**
*Senior Research Fellow, Mercatus Center at George Mason University*

New Hampshire House of Representatives, Committee on Criminal Justice and Public Safety

March 10, 2021

Chair Abbas, Vice Chair Welch, and members of the committee, thank you for the opportunity to submit testimony today. My name is Brent Skorup, and I am a senior research fellow at the Mercatus Center at George Mason University. My research focuses on telecommunications and technology law.

Technology and telecommunications companies today collect large amounts of private and personal data, including geolocation information, home address, medical information, and financial information. So it is welcome news that New Hampshire legislators are assessing the state of new technology, privacy, and constitutional principles. Today I offer the following for the committee's consideration

1. Generally, this data collection is benign or necessary to provide important commercial services to users—such as sending an Uber driver to the right location, sending money via Venmo, or monitoring blood pressure or glucose levels via a Fitbit.
2. For communications common carriers, I hope the legislature will consider bringing clarity to the use of phone geolocation information and the use of warrantless purchases of consumer data by state law enforcement.

## BRING CLARITY TO COLLECTION OF PHONE GEOLOCATION INFORMATION

Communications common carriers such as wireless providers collect information about the approximate location of customers for business and for operational purposes, such as having a mobile call routed to customers' nearest cell towers.[1] Given the popularity of 5G and Wi-Fi technologies, which have much denser installations than traditional cell towers, cellular providers necessarily collect fairly precise geolocation and proximity information about users' phones.[2] The Supreme Court in *Carpenter v. United States* held that law enforcement collection of this cellular phone location information from a wireless carrier amounts to a search.[3] However, the decision was narrowed to the facts before it, and

1. Sarah Jensen, "Are Cell Phone Conversations Stored Somewhere and Are They Retrievable?," *Ask an Engineer*, November 5, 2013. This information may be accurate to the nearest quarter mile to the nearest few meters, depending on the technology used.
2. Carpenter v. United States, 138 S. Ct. 2206, 2218–19 (2018).
3. According to Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018), "The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."

For more information or to meet with the scholar, contact
Mercatus Outreach, 703-993-4930, mercatusoutreach@mercatus.gmu.edu
Mercatus Center at George Mason University, 3434 Washington Blvd., 4th Floor, Arlington, Virginia 22201

the decision did not expressly apply to law enforcement using real-time phone location information from common carriers or "tower dumps" of all users of a certain cell tower.[4] New Hampshire may wish to expressly add phone geolocation data, including cell triangulation data and tower dumps, to the examples of protected data to provide more protections to residents and to bring clarity to state law.

## CLARIFY WHETHER WARRANTLESS PURCHASES OF CONSUMER INFORMATION BY LAW ENFORCEMENT IS PERMITTED

According to recent news reports, some federal law enforcement agencies collect certain private or personal information by purchasing it from commercial data collection companies.[5] I am not aware of reports of common carriers such as wireless operators selling such information to New Hampshire (or federal) law enforcement. However, consumer data is regularly bought and sold for, say, advertising purposes, and these recent news reports suggest that such data are increasingly a tool of law enforcement. To protect against this practice in the future, New Hampshire may consider requiring a search warrant or other safeguards before using or purchasing such data from common carriers. As written, the current draft does not protect against these acquisitions of private or personal information because this information is acquired via a judicially recognized exception to a warrant requirement—the third-party doctrine.[6]

Thank you for the opportunity to submit testimony today about this important privacy legislation.

4. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).
5. For examples of several federal agencies purchasing users' information, see Byron Tau and Michelle Hackman, "How the U.S. Government Obtains and Uses Cellphone Location Data," *Wall Street Journal*, February 7, 2020; Joseph Cox, "How the U.S. Military Buys Location Data from Ordinary Apps," *Vice*, November 16, 2020.
6. Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).