MERCATUS CENTER
George Mason University

TESTIMONY

CONSIDERING A 21ST-CENTURY APPROACH TO WARRANT REQUIREMENTS FOR ELECTRONIC INFORMATION

Jennifer Huddleston
Research Fellow, Fourth Branch Project, Mercatus Center at George Mason University

New Hampshire House of Representatives, Judiciary Committee

January 22, 2020

Good morning, Chairwoman Marjorie Smith, Vice Chairwoman Sandra Keans, and distinguished members of the Judiciary Committee.

My name is Jennifer Huddleston and I am a research fellow with the Mercatus Center at George Mason University, where my research focuses on the intersection of law and technology, including issues related to data privacy and protection. Thank you for the opportunity to provide testimony today regarding my research and its relation to the regulation of search and seizures.

In my testimony today, I plan to cover three key points:

1. Clarifying requirements for government to obtain access to electronic information can be an appropriate role for states in protecting civil liberties.
2. Establishing statutory requirements for access by the government to electronic information reflects both the original intentions of protections from search and seizure and limits disruption of innovation by preventing abuses while still enabling justified uses of technology.
3. Avoiding potential spillover effects beyond the context of searches and seizures and avoiding unnecessarily burdening the government's use of widely available technologies are important goals.

STATES AND EXPANSION OF CIVIL LIBERTIES PROTECTIONS FOR DATA FROM WARRANTLESS SEARCH AND SEIZURE

States have an important role to play as laboratories of democracy. This can be true in a number of policy areas including technology policy, where they can serve both as a testing ground for new technologies as well as the policies that govern those technologies.[1] This is an appropriate role for states when there are few or no spillover effects beyond their borders; e.g., in transportation innovation or the creation of sandboxes for financial technologies.

In some cases, state policies can have potentially dire consequences for innovation by the creation of a disruptive patchwork. In the case of data privacy or other data protection regulations, states like

1. Jennifer Huddleston, "What States and Cities Do Right to Promote Innovation," *The Bridge*, October 9, 2018.

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

California have chosen to pursue broad policies that have far-reaching and potentially devastating consequences and that are beyond their constitutional role.[2] Instead, policies that look to govern the state's use of or law enforcement's access to electronic data are reflective of a more appropriate state role in data protection. Such laws can clarify rights for citizens and responsibilities for both government actors and companies when making or complying with requests for electronic information.[3] Such laws only apply within the state and to the state's law enforcement, unlike broad consumer privacy laws, and they are less likely to have spillover effects and are likely to reflect the general trajectory and norms emerging surrounding government access to such data. While state data privacy laws such as the California Consumer Privacy Act constrain consumers' and private entities' choices and often have broad definitions that stretch beyond a state's borders, the decision to formally establish guidelines for when a warrant is required to access electronic information reflects both the federal government's and courts' expansions of the Fourth Amendment and serves as a restraint only on the states' own powers.

Such protections build on solid legal precedents and a proper understanding of the intentions behind protections from warrantless search and seizure. The Third-Party Doctrine allows the government to obtain information that has been shared with someone else without a warrant on the basis that there is no reasonable expectation of privacy when information has been shared.[4] This doctrine was initially developed in an analog era and utilized to obtain information that, for example, had been shared with a bank teller or phone company in the course of a transaction.[5]

There has been a gradual erosion of this doctrine to extend protections to various forms of communications and data. For example, on a federal level the Wiretap Act and Electronic Communications Privacy Act establish Fourth Amendment protections and warrant requirements for various communications that might have otherwise been obtainable under the broadest interpretation of the Third Party Doctrine.[6] More recently, the Supreme Court in *Carpenter v. United States* held that Cell Site Location Information (CSLI) could not be obtained using a request via the Third-Party Doctrine, but instead required a warrant.[7] Yet this ruling was narrowly tailored and only applies to that specific type of data, leaving open many questions about the Third-Party Doctrine and other technologies.[8]

Seeing the general trajectory of federal law, states are now considering clarifying the warrant requirements for access to different types of data beyond just CSLI. In 2019, Utah became the first state to establish warrant requirements for electronic data in general.[9] This approach is an acceleration in the direction the law appears to be heading at a federal level. It provides certainty and consistency while allowing protecting civil liberties, but also recognizes that there are cases where there is sufficient cause to support government access to such information via a warrant.[10] It also provides sufficient room for innovation to flourish. Such a solution provides the traditional balance between the reasonable need to access such information pursuant to a justified investigation and the protection of civil liberties.

---

2. Jennifer Huddleston, "The Problem of Patchwork Privacy," *Technology Liberation Front*, August 15, 2018; Jennifer Huddleston and Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations* (Washington, DC: Regulatory Transparency Project, 2019).
3. Molly Davis, "Utah Just Became a Leader in Digital Privacy," *Wired*, March 22, 2019.
4. John Villasenor, "What You Need to Know about the Third-Party Doctrine," *Atlantic*, December 30, 2013.
5. Villasenor, "What You Need to Know."
6. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–23 (2018).
7. Carpenter v. United States, 138 S. Ct. 2206 (2018).
8. Jennifer Huddleston, "Come Back with a Warrant: The Potential Impact of Carpenter Beyond Cell Phones," *Plain Text*, July 27, 2018.
9. Davis, "Utah Just Became a Leader in Digital Privacy."
10. Anne Bolamperti and Patrick X. Fowler, "What Does the New Utah Electronic Data Privacy Law Do?," *S&W Cybersecurity and Data Privacy Law Blog*, May 1, 2019.

CLARITY FOR AN INCREASINGLY CONNECTED FUTURE

A variety of technologies including cell phones and email have already called into question if the Third-Party Doctrine reflects contemporary understandings of reasonable expectations of privacy and the Fourth Amendment. In providing certainty and clarity regarding the needs for a warrant requirement for access to electronic data, states can create a better framework based on principles that can evolve with increasingly connected technologies.

Carpenter was narrowly tailored to apply to only one type of data, so it leaves lingering questions about other location information and the Third-Party Doctrine. For example, internet of things devices and wearable fitness trackers as well as various cell phone apps have numerous benefits to consumers and can provide important information and evidence for government planning and law enforcement.[11] Transportation technologies such as dockless scooters and autonomous vehicles involve the incidental collection of location data to ensure the operation of the technology.[12] There are many benefits to these technologies and devices; there are also questions about the potential for violations of civil liberties, especially if such information may be obtained without a warrant.

Laws clarifying the requirements, such as first obtaining a warrant for such information, will increasingly become important in our connected future. Rather than drafting changes that establish or clarify the requirements for obtaining only one particular type of data, policymakers should consider an approach that is based on the original principles behind the protection from unnecessary government intrusion and can adapt to any range of technologies. In this way, an approach like Utah's that applies to all electronic information is more able to adapt in an era of rapidly moving technologies than the case-by-case, technology-by-technology approach taken by the Court's narrow decision in *Carpenter*. To avoid a constant need for amendments and updates, a principles-based, technology-neutral approach will provide greater certainty to consumers, innovators, and the government actors seeking the information.

AVOIDING UNINTENDED CONSEQUENCES

Laws addressing the warrant requirements for obtaining various types of electronic data are well-intentioned, seeking to strike a balance between preserving civil liberties and promoting innovation, but policymakers must be cautious in order avoid potential unintended consequences.

For example, policymakers should not prevent all government access or usage of a technology in most cases, but rather provide guardrails that will deter potential abuse; e.g, having a clear and easy-to-follow protocol for obtaining the electronic information requested via a warrant and having strict limits on real-time uses.[13] Such issues arise less in the context of electronic data but are of greater concern in the potential regulation or ban of other technologies, such as facial recognition, by government entities such as law enforcement.[14] Just as warrants can strike a balance between necessary access to prevent harm and traditional understandings of privacy from government intrusion, there are various ways other than bans that would better strike a balance when it comes to these technologies as well.[15]

Additionally, the language used in describing the principles and reasons for the requirements of a warrant for obtaining electronic data are also important. For example, referring to "owning your data"

11. Jennifer Huddleston and Anne Philpot, "Adapting 4th Amendment Standards to Connected Tech," *Law360*, November 14, 2019.
12. Jennifer Huddleston and Trace Mitchell, "Should Shared Mobility Services Share Your Data?," *The Bridge*, June 26, 2019.
13. Matthew Feeney, "Should Facial Recognition Be Banned?," *Cato at Liberty*, May 13, 2019.
14. Feeney, "Should Facial Recognition Be Banned?"; Adam Thierer, "The Great Facial Recognition Technopanic of 2019," *The Bridge*, May 17, 2019.
15. Feeney, "Should Facial Recognition Be Banned?"

is not accurate and can have consequences for innovation and choice in the consumer context.[16] Even if intended to apply only in law enforcement or other government action context, such terms or interpretations could get applied more generally by courts when considering common-law complaints and could cause confusion for consumers, especially in light of a growing patchwork of consumer privacy laws.[17]

CONCLUSION

Data privacy is a multifaceted issue. In many cases, the cross-border nature of data and associated issues will mean that a federal framework is necessary for issues such as consumer privacy. However, establishment of the framework for government access to electronic data, as with other issues in technology policy, is an opportunity for states to act as a leader and provide greater clarity for consumers, innovators, and government actors. States seeking to clarify such civil liberties protections have the opportunity to be early movers in reflecting the general legal trajectory on such issues.

16. Will Rinehart, "The Law & Economics of 'Owning Your Data,'" *Insight*, American Action Forum, April 10, 2018 (discussing the problems with "owning" one's data).
17. Huddleston, "The Problem of Patchwork Privacy."