MERCATUS CENTER
George Mason University

TESTIMONY

PENNSYLVANIA AND THE FUTURE OF DATA PRIVACY

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

Pennsylvania State Senate, Communications & Technology Committee

February 5, 2020

Good morning, Chair Kristin Phillips-Hill, Minority Chair Timothy Kearney, and distinguished members of the Communications & Technology 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 submit this statement today regarding potential considerations for policymakers regarding data privacy and protection at the state level.

In this statement I focus on three key points:

1. The current landscape of data protection policy, including how the less regulatory approach has enabled innovation and existing privacy regulations for more sensitive types of data
2. The potential problems arising from state-level actions regarding the regulation of data privacy, including the creation of a disruptive patchwork and potential constitutional concerns
3. Ways in which states can be a leader in data privacy while avoiding these potential pitfalls, such as clarifying warrant requirements for access to electronic data

THE CURRENT LANDSCAPE OF DATA PRIVACY

The past 18 months have seen increased discussions from policymakers at all levels regarding issues related to data protection and privacy. Much of this conversation has been driven by both the enactment of new regulations, such as the European Union's General Data Protection Rule (GDPR) and California's Consumer Privacy Act (CCPA), which establish many more requirements for the use and collection of data, and headlines related to various data breaches and concerns about the use of data such as the Cambridge Analytica incident.[1] While this increases the sense of urgency for policymakers at all levels to consider data protection legislation, the potential consequences of changes to the traditional American approach to data privacy and protection need to be carefully considered as well.

1. The Cambridge Analytica incident (involving a researcher exploiting access to individuals' data by selling data to a private firm obtained through a quiz in violation of Facebook's terms for researchers) and other privacy incidents were the subject of the recent Facebook-FTC consent decree. Alvin Chang, "The Facebook and Cambridge Analytica Scandal, Explained with One Diagram," *Vox*, May 2, 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

In general, the United States has approached the regulation of information technology from a "permissionless" framework that presumes a technology should be allowed free of regulatory intervention except in cases where there is a high probability of tangible, potentially irreversible or catastrophic harm.[2] This approach is in contrast to the "precautionary" approach taken by many European countries that requires technology innovators to show that potential negative consequences, even if unlikely, have been fully considered and avoided before the innovation is allowed on the market.[3] The results of these different policy approaches is apparent when examining the fact that most of the current tech giants have emerged from the United States, while few of the most innovative companies are found in Europe and other more regulated regions.[4]

When it comes to data privacy, the United States is not necessarily the Wild West it is portrayed to be. In fact, many of the already-considered most sensitive areas of data such as healthcare and financial information are already subject to industry-specific regulations at a federal level.[5] Similarly, many concerns about privacy are actually concerns about data security or data breach. While the current 50-state data breach notification patchwork is not ideal and illustrates some potential consequences of a state-by-state approach, it does insure that affected consumers in each state should receive some form of notification if the covered data is compromised.[6]

Over the past year, there have been many proposals for federal data privacy legislation and many Congressional hearings on the issue, yet no specific proposal seems to have gained sufficient traction to become law.[7] In the perceived void, some states, including California, Maine, and Nevada have chosen to pass their own legislation to address what they perceive as a pressing problem.[8] Yet such an approach is far from a second-best solution and may create far more problems than it solves.

PROBLEMS WITH A STATE-LEVEL APPROACH TO DATA PRIVACY REGULATION

States have been leaders in many areas of technology policy and provided an important laboratory of democracy for different approaches to regulation.[9] For example, Pennsylvania has an innovative approach to autonomous vehicle governance that allows it to be a leader in the field.[10] However, when it comes to issues surrounding data privacy, state actions could result in creating a disruptive regulatory patchwork that could undermine future innovation. Even if there were no concerns about the content of such regulations, state data privacy laws could be found unconstitutional.

State laws on data privacy could face three constitutional concerns. First, since data rarely obey borders and a single transaction can involve multiple states, state data privacy laws are likely to have significant out-of-state effects.[11] Therefore, it is possible that these laws could be found unconstitutional under the Dormant Commerce Clause, given the potential burdens on out-of-state consumers and firms with

2. Adam Thierer, *Permissionless Innovation: The Continuing Case for Comprehensive Technological Freedom* (Arlington, VA: Mercatus Center at George Mason University, 2016), 7–21, 34.
3. Thierer, *Permissionless Innovation*, 22–33.
4. Barry Jaruzelski, Volker Staack, and Robert Chwalik, "Will Stronger Borders Weaken Innovation," *Strategy+Business*, no. 89 (2017): 1–16.
5. Alan McQuinn, "Understanding Data Privacy," *RealClearPolicy*, October 25, 2018.
6. Jennifer Huddleston, "The State of State Data Laws, Part 1: Data Breach Notification Laws," *The Bridge*, July 31, 2019; Caleb Skeath and Brooke Kahn, "State Data Breach Notification Laws: 2018 in Review," *Inside Privacy*, December 31, 2018.
7. Jennifer Huddleston, "An Analysis of Recent Federal Data Privacy Legislation Proposals" (Mercatus Policy Brief, Mercatus Center at George Mason University, Arlington, VA, March 2019).
8. Jennifer Huddleston, "Should Congress be Concerned about California's Data Privacy Law," *The Hill*, December 3, 2019.
9. Jennifer Huddleston, "What States and Cities Do Right to Promote Innovation," *The Bridge*, October 9, 2018.
10. Jennifer Huddleston and Adam Thierer, "Pennsylvania's Innovative Approach to Regulating Innovation," *The Bridge*, September 5, 2018.
11. Jennifer Huddleston and Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations* (Washington, DC: Regulatory Transparency Project, 2019).

minimal measurable benefits for states' interests.[12] The courts, when considering potential Dormant Commerce Clause violations, will first look if the law is directly discriminatory against out-of-state actors; but even when it is not, the courts will examine whether it might indirectly discriminate against those actors and whether the burdens on such actors are disproportionate to the purported in-state benefits.[13] For example, in *Bibb v. Navajo Freight Lines,* the Supreme Court struck down as unconstitutional under the Dormant Commerce Clause a state law specifying a type of mudflap on trucks. The law could have resulted in truck drivers not being able to comply with laws in all 50 states and having to change their mudflaps at each border.[14] It would be even more difficult for today's online commerce and the data associated with it to stop at state borders. Additional constitutional concerns could also arise from state data privacy laws. For example, conflicts with the existing federal data privacy laws in other regulated areas such as financial and health information could render supposedly comprehensive laws at least partially preempted in these areas.[15] Additionally, regulations of data privacy at any level should carefully consider the potential impact on free expression from either deletion requirements or content-based distinctions in such regulations.[16]

Even if such laws are found to be constitutional, there are significant concerns of the negative effects a patchwork could have on consumer choice and innovation. In some cases, companies may find it easiest to comply with the most restrictive regulations rather than create state-specific products, meaning consumers would be limited to the choices allowed under the most restrictive state's regime.[17] But in some cases these laws might contradict one another, thereby balkanizing the internet and preventing the same products from being offered in all 50 states.[18] Not only would this result in consumers being unable to benefit from certain products, it could also create confusion regarding what rights individuals have and how companies should respond to certain requests.

While often well-intentioned, policymakers should also consider the other tradeoffs and costs that might be involved with a far more restrictive data regulation in the name of privacy. For example, the GDPR has resulted in decreased venture capital investment in small companies, making it more difficult for new players to emerge and even preventing the creation of new jobs by these companies.[19] The compliance costs of the CCPA for in-state firms is expected to be $55 billion by the state's own estimates and there is no doubt that at least some out-of-state firms will incur costs to comply as well.[20] But beyond the costs, privacy regulations can also fail to solve the problems they intend to; they may create incentives to respond rapidly to requests rather than focus on other privacy- or security-related measures, and as a result such regulation could lead to loopholes that could be exploited and exacerbate concerns about privacy and security.[21]

---

12. Huddleston and Adams, *Potential Constitutional Conflicts*.
13. Pike v. Bruce Church, 397 U.S. 137, 142 (1970).
14. Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520 (1959).
15. Huddleston and Adams, *Potential Constitutional Conflicts*; "Does the HIPAA Privacy Rule Preempt State Laws?," US Department of Health and Human Services, last reviewed July 26, 2013, https://www.hhs.gov/hipaa/for-professionals/faq/399/does-hipaa-preempt-state-laws/index.html (providing an example of when conflicts may be preempted).
16. Huddleston and Adams; Christopher Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases" (Public Interest Comment, Mercatus Center at George Mason University, Arlington, VA, October 27, 2017).
17. Jennifer Huddleston, "The Problem of Patchwork Privacy," *Technology Liberation Front*, August 15, 2018.
18. Huddleston, "The Problem of Patchwork Privacy."
19. Jian Jia, Ginger Lin, and Liad Wagman, "The Short-Run Effects of GDPR on Technology Venture Capital Investment," *Vox* (Center for Economic Policy Research), January 7, 2019.
20. State of California Department of Justice, Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018*, August 2019.
21. Lorenzo Franceschi-Bicchierai, "Researchers Show How Europe's Data Protection Laws Can Dox People," *Motherboard*, *Vice*, August 8, 2019; Nick Statt, "Amazon Sent 1,700 Alexa Voice Recordings to the Wrong User Following Data Request," *Verge*, December 20, 2018.

When it comes to broad consumer privacy legislation, states may not be the appropriate actors for regulation.

WHAT STATES MIGHT CONSIDER DOING REGARDING DATA PRIVACY

While broad consumer data privacy regulations might not be an appropriate use of state power because of the potential patchwork and spillover effects, states can consider other ways to be a leader on data protection issues. These actions, however, should be reserved only to those data transactions that can be considered wholly intrastate rather than interstate. This means that, largely, such actions will not be restraints on the consumers interactions with companies, but rather restraints on the government's own use of data.

Some potential areas states might want to consider include clarifying the warrant requirements for access to electronic data. Last year, Utah became a leader by establishing warrant requirements for police access to electronic information, effectively ending the state's use of the Third-Party Doctrine.[22] The Third-Party Doctrine, which allows government access to various information shared with third parties such as numbers dialed or interactions with a bank teller without a warrant, has already come under question at the federal level, and in 2018 the Supreme Court established that cell site location information requires a warrant for access rather than being accessible under this doctrine.[23] The issue of when information has been sufficiently shared to waive a warrant requirement will be increasingly relevant for a variety of technologies, including wearable fitness trackers and connected transportation technologies.[24] Forward-thinking states can establish clear guidance that protects civil liberties without stymying government and law enforcement. By clarifying guidelines on this issue, states can provide increased certainty to government actors, citizens, and innovative companies without the spillover effects associated with broad consumer data privacy laws.

CONCLUSION

Data privacy is likely to continue to be a topic of discussion in the coming years. Policymakers at all levels should consider the potential tradeoffs associated with broad regulation as well as the potential for a patchwork to create more problems with few solutions. While states have often been leaders when comes to technology policy, the broader issue of consumer data privacy may be beyond their constitutional role in the federalist system.

22. Molly Davis, "Utah Just Became a Leader in Digital Privacy," *Wired*, March 22, 2019.
23. John Villasenor, "What You Need to Know about the Third-Party Doctrine," *Atlantic*, December 30, 2013; Carpenter v. United States, 138 S. Ct. 2206 (2018).
24. Jennifer Huddleston, "Come Back with a Warrant: The Potential Impact of Carpenter Beyond Cell Phones," *Plain Text*, July 27, 2018; Jennifer Huddleston and Anne Philpot, "Adapting 4th Amendment Standards to Connected Tech," *Law360*, November 14, 2019; Jennifer Huddleston and Trace Mitchell, "Should Shared Mobility Services Share Your Data?," *The Bridge*, June 26, 2019.