MERCATUS CENTER
George Mason University

TESTIMONY

CONSIDERATIONS FOR NORTH DAKOTA REGARDING CONSUMER DATA PRIVACY POLICY

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

North Dakota Legislature, Interim Commerce Committee

January 15, 2019

Good afternoon, Chairman Scott Louser, Vice Chairman Shawn Vedaa, and distinguished members of the Interim Commerce Committee.

My name is Jennifer Huddleston, and I am a research fellow at the Mercatus Center at George Mason University, where my research focuses primarily on the intersection of law and technology. This focus includes issues surrounding consumer data privacy. Thank you for this opportunity to discuss such policy matters in relation to the protections, enforcement, and remedies regarding consumers' personal data and the impact of actions taken by other states on this matter.

Within this context I would like to focus on three key points:

1. Existing laws regarding consumer data and the potential tradeoffs to other benefits, including free expression and innovation involved in further regulation of data privacy
2. Potential problems and constitutional concerns from state laws regarding data privacy, including issues under the Dormant Commerce Clause and creation of a disruptive patchwork, that result in the need for a single, federal standard
3. State policy regarding data privacy, which should focus only on the government's own actions or those actions that are solely intrastate

THE CURRENT DATA PRIVACY LANDSCAPE

The United States has traditionally embraced a "permissionless" approach to information technology issues, including issues related to consumer data privacy. The presumption in this approach is that new technology should be allowed to enter the market unless otherwise subject to existing regulation or if regulation would prevent harm or catastrophe that would clearly result from the introduction of the technology or its specific application. In contrast, Europe has taken a much more "precautionary" approach that presumes the potentially risky or harmful impact of technology and instead requires innovators and entrepreneurs to show that such potential risks have been eliminated or minimized. In the same time period, the United States has emerged as a leader in the digital economy, while more heavily regulated jurisdictions such as Europe have produced few tech giants. A shift away from this "permissionless" framework would likely result in tradeoffs that could change the traditional success and leadership the United States has experienced in the digital economy.

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

Even with this light-touch tradition, the United States is not a Wild West when it comes to data privacy. Instead, the approach has been to identify areas where data are particularly sensitive and where disclosure of information or other potential privacy breaches are likely to result in potential harm. As a result, many types of information, including financial information, healthcare records, educational records, and the data for children under 13 are already subject to additional federal regulations.[1] While these laws may result in tradeoffs that mean certain benefits are forgone or certain innovations are not pursued, the laws represent a much more specific approach, focused on areas where there is particular vulnerability or risk of harm. Additionally, in some cases, these laws also illustrate that even in areas where society highly values privacy, there can be problems and tradeoffs. For example, frustration can ensue when an institution favors privacy out of an abundance of caution for HIPAA requirements and a patient is thus unable to obtain his or her own records.[2] Because all regulation regarding data privacy should be designed to address harms, it should be considered if existing laws already address these harms or could merely be updated to do so.

Concerns are sometimes based less in the day-to-day usage of data and are based more on concerns about data breaches and data security than data privacy. In this area, it is important to note that all 50 states have some kind of data breach notification law, so consumers should receive notification when involved in such an incident.[3] While this state-by-state approach has resulted in notification in all states, the requirements and covered information vary and can create confusion for both consumers and innovators.[4]

This current approach has allowed the expression of a wide range of individual preference when it comes to privacy and data usage. It has also allowed many beneficial services and options for both individuals and society as a whole.[5] Changes to the American approach to data privacy could result in the loss of these benefits and substantially affect individuals, innovation, and the economy.[6]

STATE REGULATION OF CONSUMER DATA PRIVACY PRESENTS ADDITIONAL CONCERNS

Recent headlines and the actions by other jurisdictions, including the European Union's General Data Protection Rule (GDPR), have led American policymakers to question continuing the more hands-off approach to this issue. In the absence of federal legislation, some states have chosen to consider their own legislation rather than wait for a national standard. As of January 2020, California, Maine, and Nevada have enacted additional consumer data privacy regulations and more than 18 other states, including North Dakota, are studying or have considered similar regulation.[7] However, this state-by-state approach has additional innovation-disrupting consequences and raises concerns about potential constitutionality.

Consumer data and the interactions that generate it can involve many states and is difficult to confine to a single state's borders. Ian Adams and I previously noted that "Such reasoning is straight-forward: data transmissions do not obey borders and a single online action can involve multiple states even if it involves only a single individual."[8] As a result, such state laws can have an impact and burden on firms

[1] Alan McQuinn, "Understanding Data Privacy," *RealClear Policy*, October 25, 2018
[2] Judith Graham, "In Days of Data Galore, Patients Have Trouble Getting Their Own Records," *Kaiser Health News*, October 25, 2018.
[3] Caleb Skeath and Brooke Kahn, "State Data Breach Notification Laws: 2018 in Review," *Inside Privacy*, December 31, 2018.
[4] Jennifer Huddleston, "The State of State Data Laws, Part 1: Data Breach Notification Laws," *The Bridge*, July 31, 2019.
[5] John Raidt, "7 Great Ways Data Can Benefit Society," *U.S. Chamber of Commerce*, May 23, 2016.
[6] Alan McQuinn and Daniel Castro, *The Costs of an Unnecessarily Stringent Federal Data Privacy Law* (Washington, DC: Information Technology and Innovation Foundation, 2019).
[7] National Conference of State Legislatures, "Consumer Data Privacy Legislation," January 3, 2020, http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.
[8] Jennifer Huddleston and Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations* (Washington, DC: Regulatory Transparency Project, 2019).

beyond a state's borders. Given these burdens on nonresident firms and potentially nonresident consumers, these laws may be unconstitutional under the Dormant Commerce Clause.[9]

When analyzing an argument regarding the Dormant Commerce Clause, the courts examine if the state law directly discriminates against out-of-state actors or, if facially neutral with regard to out-of-state actors, indirectly discriminates against them. Current state consumer data privacy laws are not facially discriminatory against out-of-state actors.[10] Their likely effect on out-of-state businesses and consumers, however, raises constitutional issues under the Dormant Commerce Clause, which, among other things, considers whether the burdens on out-of-state parties are disproportionate to the purported in-state benefits.[11] This is where the constitutionality of state consumer data privacy laws could likely be called into question. In *Bibb v. Navajo Freight Lines*, the US Supreme Court struck down a state law that would require a specific type of mudflaps, which would likely result in truck drivers having to change their mudflaps at state borders, as an unconstitutional burden on interstate commerce even if it was not facially discriminatory.[12] Data and the internet are naturally an interstate interaction, and it would be even more difficult to expect a change in data handling to occur at a virtual border for each state's specific requirements.

The Dormant Commerce Clause is not the only potential constitutional concern such laws face. As mentioned earlier, federal regulations exist for certain areas of data. While some of these laws allow for additional state regulation in these areas, state laws could create conflicts that make compliance with both state and federal regulation difficult or incredibly burdensome.[13] The supremacy of federal law could mean that if policymakers do not carefully consider these potential conflicts, allegedly comprehensive privacy laws could be anything but comprehensive as certain sections are preempted by their conflicts with federal laws.[14]

State lawmakers as well as federal lawmakers must also consider the potential conflicts between consumer data privacy and other rights. This is perhaps most obvious in the context of potential burdens on speech that may result from consumer data privacy laws. State data privacy laws may be subject to a high level of scrutiny and found unconstitutional if they discriminate based on the content or purpose of the data.[15] In addition, consideration of requirements such as deletion or a right to be forgotten could silence speakers and impact the availability of important information.[16]

Even aside from these constitutional considerations, a state-by-state approach could have additional negative effects on innovation. Such laws could conflict with one another, interrupting the seamless nature of the internet and information and preventing the same product from being offered in all states. Additionally, this patchwork approach could create confusion for both consumers and companies who are uncertain about what rights they have or what information they should provide. When such uncertainty ensues, mistakes and frustrations may result.

To combat this confusion, innovators might merely choose to comply with the most restrictive requirements, even if other states have more market-friendly approach. For example, Microsoft

---

[9] Huddleston and Adams, *Potential Constitutional Conflicts*.
[10] Huddleston and Adams.
[11] Pike v. Bruce Church, 397 U.S. 137, 142 (1970).
[12] Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520 (1959).
[13] Huddleston and Adams, *Potential Constitutional Conflicts*; US Department of Health and Human Services, "Does the HIPAA Privacy Rule Preempt State Laws?," March 12, 2003, 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).
[14] Huddleston and Adams, *Potential Constitutional Conflicts*.
[15] Huddleston and Adams; 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).
[16] Huddleston and Adams; Koopman et al., "Informational Injury in FTC Privacy and Data Security Cases."

already stated it would apply the requirements of the California Consumer Privacy Act (CCPA) nationally.[17] Even if all 50 states passed identical or nearly identical legislation, differences in interpretation or enforcement could still result in issues that mean a single state's enforcement decision has an outsized impact.

Such regulations are not costless, and state policymakers should carefully consider the potential economic costs as well as the loss of innovation and investment. California's own study of the potential impact of its CCPA showed it would cost $55 billion to in-state companies. This figure does not include the costs borne by out-of-state companies that will almost certainly be subject to the law.[18] The GDPR also provides an example of the potential costs. One study suggests that, in its first year, the GDPR resulted in a 17.6 percent decrease in weekly venture capital investment and such deals contained less investment than in prior years.[19] As a result of this decreased investment, research suggests that the GDPR could have resulted in 29,000 fewer jobs—jobs that were not created by new innovative companies.[20]

Finally, regulations that prevent certain uses of data could actually deter innovation in privacy and security as well as undermine their end goal. For example, the quick turnaround time for delivering data to legitimate requests can result in mistakes, as seen with the GDPR, such as a fiancé being able to obtain personal information on his betrothed or sending Alexa voice recordings to the wrong recipient.[21] Policymakers should carefully consider whether proposed regulation risks creating new privacy concerns and what its potential effect on data security is.

Keeping these potential constitutional concerns and consequences in mind, in many cases the best action for state policymakers may be no take action at all.

POTENTIAL PROPER ROLE FOR STATES IN ADVANCING DATA PRIVACY

Although I have laid out the potential issues and concerns with state data privacy actions in the preceding sections, there are some actions that states might be able to take within their proper role in the federal system. Largely these will be policies that affect only data actions that the state itself undertakes or that are solely intrastate.

The most notable example of this is a recent Utah law requiring a warrant for various law enforcement access to data.[22] Such an approach is in line with recent Supreme Court precedent regarding the removal of warrantless access to cell service location information.[23] Such laws protect individuals' civil liberties but do not have the same impact beyond state borders as other laws. Such an approach still should recognize that, at times, data are useful and beneficial while also recognizing existing principles and protections from unnecessary government intrusion.

---

[17] Daniel A. Lyons, "State Net Neutrality" (Research Paper No. 514, Boston College Law School, Newton, MA, October 11, 2019) (discussing such in the context of State Net Neutrality laws).
[18] State of California Department of Justice, Office of the Attorney General, *Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018*, August 2019.
[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, https://voxeu.org/article/short-run-effects-gdpr-technology-venture-investment.
[20] Jia, Lin, and Wagman, "The Short-Run Effects."
[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.
[22] Molly Davis, "Utah Just Became a Leader in Digital Privacy," *Wired*, March 22, 2019,
[23] Jennifer Huddleston and Anne Philpot, "Adapting 4th Amendment Standards to Connected Technology," *Law 360*, November 14, 2019; Brent Skorup and Jennifer Huddleston Skees, "Bringing Constitutional Doctrine into the Digital Age," *Washington Times*, July 3, 2018.

Policies at a state or local level should focus only on those actions and data that occur within their borders. Another possible example would be regulations related to the governments' own collection and usage of data. These issues are distinct from the broad consumer privacy laws often proposed and should also reflect specific harms and legal standards.

CONCLUSION

What, if any, additional regulation or enforcement is needed regarding consumer data privacy continues to be a hotly debated issue. However, in many cases a federal framework will be needed rather than the potential disruption caused by a state patchwork. Still, states can play an important role in encouraging action at the federal level and continuing to preserve the benefits of the American approach to innovation. Rather than seeking broad consumer privacy actions, if states feel the need to act, they should look at potential restraints on their own actions or other similar intrastate issues.