Statement

of

Jennifer Huddleston

Technology Policy Research Fellow
Cato Institute

before the

Judiciary Committee
Maine State Legislature

October 17, 2023

RE: Data Privacy Legislation At a State and Local Level

Chairs Carney and Moonen and Members of the Judiciary Committee:

My name is Jennifer Huddleston and I am a technology policy research fellow at the Cato Institute. My research focuses on the intersection of law and technology, including issues related to data privacy. I thank you for the opportunity to provide informational testimony based on my work on this topic. This testimony should be considered for informational purposes and not in support of or opposition to the legislation under consideration.

Tradeoffs must be carefully considered when it comes to data privacy

Data privacy is a top concern for many consumers,[i] however, the precise preferences vary greatly. Data has had hugely beneficial applications in a wide array of services and industries for both consumers and businesses. These beneficial applications and the availability of choices should not be forgotten in the policy debate around data privacy.

It is easy to forget what our experiences online and offline were like before our data became rich. Data has allowed retailers and platforms to provide consumers with more customized experiences that many may find more enjoyable than the prior one-size-fits-all approach. For those who do not, privacy-centric options have also emerged such as ad-blockers, virtual private networks (VPNs), and even just changing settings on a particular app to ask it not to track data. Consumers make many choices around the use of their data on a daily basis and these actions may vary depending on the service and type of data at hand. Policymakers should be careful to presume that all consumers always want the most privacy-centric option, as many find different privacy preferences beneficial in different scenarios.[ii]

Privacy legislation is often static and, as such, is unlikely to evolve as quickly as technology. This means innovators may be unable to provide what may turn out to be better experiences or even more private or secure opportunities due to limitations of compliance. For example, blockchain technology and artificial intelligence both have enormous potential, but have come into friction with highly regulatory approaches to data privacy.[iii]

Beyond these individual preferences and tradeoffs that businesses and individuals may make, privacy as a right may come into friction with other rights and values. Data rarely belongs to just a single individual but is typically generated through various interactions. Additionally, access to data is often important for other rights, such as freedom of the press or free expression. More regulatory approaches to privacy may come into friction with these rights.[iv]

To minimize tradeoffs, policymakers should look at what specific harms they are seeking to address rather than regulating data more broadly. In considering these harms, they should also consider whether existing laws around issues like fraud or deception already cover the concerns and if the approach is adaptable in ways that allow for new industry best practices to be considered.

A growing patchwork of state level data privacy legislation is costly for consumers and businesses

A dozen states now have comprehensive consumer data privacy laws. Most of these laws have generally followed either California's heavily regulatory approach or a slightly more flexible approach seen in Virginia and Utah.[v] This growing patchwork of laws, however, is likely to increase confusion for consumers and increase costs for businesses.

A federal approach remains preferable to a state-by-state approach for both innovators and consumers. One study found a 50-state patchwork of laws could lead to out-of-state costs that exceed $1 trillion over 10 years with hundreds of millions of this cost borne by small businesses.[vi] Many of these costs may be passed on to the consumer at a time when consumers are already concerned about rising prices, but that is not the only potential negative effect on consumers. Some products may find that certain states are not worth the costs or compliance risk of a stringent privacy regime. For example, numerous services — from small games to the Los Angeles Times — pulled out of Europe when its privacy regulation went into effect five years ago.[vii] States, particularly those considered to be smaller markets, could find similar scenarios occurring. Furthermore, in many cases, it remains unclear whether privacy regulations have actually improved privacy or changed consumer choices or just introduced an increasingly frustrating level of friction to the use of services.[viii]

Many of these concerns will also exist if data privacy is decided at a federal level, but a state-by-state approach has its own unique risks. States could easily come into conflict with one another over certain defaults such as "opt-in" versus "opt-out" models, rendering it impossible for the same product defaults to comply with both. Additionally, such laws are likely to impact out-of-state firms and interstate commerce, raising potential dormant commerce clause concerns.[ix] For these reasons, if the United States were to consider comprehensive consumer privacy regulation, it should be handled by Congress and not a state-by-state approach.

Conclusion

Thank you for your time and consideration of this information. While data privacy is an important topic for many consumers, the exact nature of those concerns vary, as do individual preferences. As such, legislation should be careful not to dictate a set of preferences for consumers but, if needed, focus on responses to particular currently unaddressed harms. I welcome any questions related to my research on data privacy and my responses to these questions.

[i] *Most consumers want data privacy and will act to defend it. International Association of Privacy Professionals* (2023). Accessible at https://iapp.org/news/a/most-consumers-want-data-privacy-and-will-act-to-defend-it/.

[ii] Alec Stapp, *Against Privacy Fundamentalism in the United States*. Niskanen Center (2018). Accessible at https://www.niskanencenter.org/against-privacy-fundamentalism-in-the-united-states/.

[iii] Mani Karthik Suhas Suripeddi & Pradnya Purandare, *Blockchain and GDPR – A Study on Compatibility Issues of the Distributed Ledger Technology with GDPR Data Processing*. Journal of Physics: Conference Series (2021). Accessible at https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042005; David Meyer, *Italy bans ChatGPT until OpenAI makes the hit A.I. respect Europe's privacy laws*. Fortune (2023). Accessible at https://fortune.com/2023/03/31/italy-bans-chatgpt-gdpr-violations-privacy-ai/.

[iv] Nani Jansen Reventlow, *Can the GDPR and Freedom of Expression Coexist?* Cambridge Core (2020). Accessible at https://doi.org/10.1017/aju.2019.77.

[v] Jennifer Huddleston & Gent Salihu, *The Patchwork Strikes Back: State Data Privacy Laws after the 2022–2023 Legislative Session*. Cato Institute (2023). Accessible at https://cato.org/blog/patchwork-strikes-back-state-data-privacy-laws-after-2022-2023-legislative-session-0/.

[vi] Daniel Castro et al., *The Looming Cost of a Patchwork of State Privacy Laws*. Information Technology & Innovation Foundation (2022). Accessible at https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/.

[vii] *GDPR Graveyard.* Americans for Tax Reform. Accessible at https://www.digitalliberty.net/wp-content/uploads/2019/12/GDPR-Graveyard-.pdf.

[viii] Frederic Gerdon et al., *Did the GDPR increase trust in data collectors? Evidence from observational and experimental data*. Information Communication & Society 25(14) (2022). Accessible at https://www.tandfonline.com/doi/abs/10.1080/1369118X.2021.1927138?role=tab&scroll=top&needAccess=true; Yu Zhao et al., *Privacy Regulations and Online Search Friction: Evidence from GDPR*. National Bureau for Economic Research (2021). Accessible at https://conference.nber.org/conf_papers/f160434.pdf.

[ix] Jennifer Huddleston & Ian Adams, *Potential Constitutional Conflicts in State and Local Data Privacy Regulations*. Regulatory Transparency Project (2019). Accessible at https://rtp.fedsoc.org/paper/potential-constitutional-conflicts-in-state-and-local-data-privacy-regulations/.