Statement

of

Jennifer Huddleston

Technology Policy Senior Fellow
Cato Institute

before the

Subcommittee on Financial Institutions
Committee on Financial Services
United States House of Representatives

June 4, 2025

RE: "Framework for the Future: Reviewing Data Privacy in Today's Financial System"

Chair Barr, Vice-Chair Loudermilk, Ranking Member Foster, and distinguished members of the House Committee on Financial Services Subcommittee on Financial Institutions:

My name is Jennifer Huddleston, and I am a senior fellow in technology policy at the Cato Institute. My research focuses primarily on the intersection of law and technology, including issues related to data privacy. Therefore, I welcome the opportunity to testify regarding data privacy in today's financial system.

In this testimony, I will focus on three key points:

- First, data privacy in sensitive areas such as the financial services sector is already regulated by existing law;
- Second, as state or potential federal data privacy laws continue to emerge, careful attention should be paid to the way they may interact with or conflict with existing law in such regulated industries and what this patchwork might mean regarding the burden on small players, particularly if there are enforcement mechanisms such as private rights of action for statutory damages that could significantly raise the risk of costly litigation;
- Finally, any conversations around data privacy should consider the impact on innovation, consumer choice, and small players, as well as how such laws could interact with or hinder the deployment of better solutions.

Understanding Existing Data Privacy Law in the Financial Services Sector

Because of the lack of a comprehensive federal data privacy law, some have criticized the United States as a sort of wild west when it comes to data privacy. Instead, the United States' approach has been to respond with regulation for particularly vulnerable or sensitive data where consumers would be more likely to face harm should it be abused or insecure. These laws are more narrowly focused on the consumer data experience and data privacy or security within these areas or

industries.[1] The financial services sector, for example, already has consumer-focused data privacy laws, including the Graham-Leach-Bliley Act (GLBA) that regulates the personal data of consumers held by financial services firms and the Fair Credit Reporting Act (FCRA) that regulates consumer credit data from credit reporting agencies.

My testimony in this hearing will focus on consumer privacy; however, a number of laws and regulations, including the Bank Secrecy Act, require reporting from financial services firms and allow warrantless government access to information about individuals' financial transactions. My Cato colleagues in our Center for Monetary and Financial Alternatives have explored the need for reform to protect individuals' financial privacy from government surveillance and to ensure that individuals' Fourth Amendment rights are respected.[2]

Potential Interactions Between Comprehensive Data Privacy Laws in Financial Services

Consumer privacy in the financial sector has been regulated for several decades. Additional data privacy laws, however, could further add to a regulatory burden or conflict with existing laws. An emerging patchwork of laws that are both sector-specific and general in their applications will make it more difficult for smaller or more innovative players to navigate. To date, at least 19 states have passed comprehensive consumer privacy laws, with many more debating such legislation.[3] In addition, there is an ongoing effort to pass general federal consumer privacy legislation.[4] This is resulting in the emergence of a concerning patchwork that can be

[1] Alan McQuinn, "Understanding Data Privacy," *RealClearPolicy*, October 25, 2018.
[2] Norbert Michel, "Experts Agree That Financial Privacy Needs A Revamp," *Forbes*, September 16, 2024 and Jennifer Schulp, "Financial Privacy Is Under Fire — The Issue Should Draw the Attention of Both Parties," *The Hill*, August 26, 2024.
[3] Jennifer Schulp, "Financial Privacy Is Under Fire — The Issue Should Draw the Attention of Both Parties," *The Hill*, August 26, 2024.
[4] *See* Office of Chairman Brett Guthrie, "Chairman Guthrie and Vice Chairman Joyce Issue Request for Information to Explore Data Privacy and Security Framework," *House Energy and Commerce Committee*, February 21, 2025.

problematic and confusing for both consumers and regulated entities who are unsure of the requirements or rights when data inevitably involves interactions in multiple states.[5]

Even when such laws are modeled on one another, there could be significant differences that can cause potential conflicts. While most state consumer privacy laws have carve-outs for data already regulated under laws like the FCRA and GLBA, this does not mean that they do not potentially impact or create other conflicts for the financial services sector or financial data.[6] This can include the definitions of particularly sensitive data — including financial information — and the timelines and steps entities must take to respond to consumer requests or potential issues. These conflicts can be particularly felt by smaller or more innovative entities who will have to navigate various definitions.

Additionally, enforcement mechanisms around private rights of action for statutory damage could deter innovation, particularly in an already highly regulated and risk-averse sector. While not related to financial data, the Illinois Biometric Information Privacy Act has such a mechanism and is illustrative of the problems such enforcement can create, even in data considered particularly sensitive. Because of statutory damages and private right of action, the law has resulted in significant claims against companies based not on actual injury, but mere violation and recovery for the attorneys bringing such actions.[7] Additionally, this potential has

[5] *See* Jennifer Huddleston and Gent Salihu, "The Patchwork Strikes Back: State Data Privacy Laws after the 2022–2023 Legislative Session," *Cato at Liberty (blog)*, July 6, 2023.
[6] Consumer Financial Protection Bureau, *State Consumer Privacy Laws and the Monetization of Consumer Financial Data* (Consumer Financial Protection Bureau, November 2024).
[7] *See* U.S. Chamber of Commerce Institute for Legal Reform, *A Bad Match: Illinois and the Biometric Information Privacy Act* (U.S. Chamber of Commerce Institute for Legal Reform, October 2021).

deterred the launch of certain innovative products that might create positive consumer experiences or even improve security.[8]

How Privacy Law and Innovation Could Conflict

While recognizing the specific risks of economic harm and the sensitivity of financial data is logical, law is static and innovation is dynamic, yielding the potential need to review regulation to allow improvements in data privacy, security, and innovation as various technologies might provide alternatives that are more protective of privacy or provide better services to consumers who opt in but might not be able to comply. While consumers value privacy, they also enjoy the improvements and personalized services we have come to expect through data usage. This includes the financial services sector both for its ability to use data to improve consumer security through actions like fraud detection and to better serve its customers.

When it comes to the financial services industry, there are three ways existing data privacy regulation might deter innovation that I'd like to highlight. First, many data privacy laws were created with earlier technologies in mind. This may make it more difficult to use more secure technologies like blockchain or even cloud computing and could also create greater privacy risks through retention requirements than are truly necessary.[9] Second, enforcement mechanisms around private rights of action or the need for government approval could deter companies of all sizes from trying innovative ways to use or protect data. Finally, artificial intelligence may require us to rethink our existing frameworks around data usage, retention, and minimization.[10]

---

[8] Amy Korte, "A New Feature on Google's Arts & Culture App Is Not Available to Illinois Users Because of the State's Strict Biometric Privacy Law," *Illinois Policy*, January 23, 2018 and *see* Joseph J. Lazzarotti et al., "From Time Keeping to Dashcams, BIPA Litigation Continues," *JacksonLewis*, January 10, 2022.
[9] *See* Virginie Liebermann and Michel Molitor, "Blockchain vs. Data Protection," *International Network of Privacy Law Professionals*, July 30, 2024 (discussing such issues in the general context of GDPR).
[10] *See* Orly Lobel, "The Law of AI For Good," *Florida Law Review 75*, no. 6, January 26, 2023.

In regulated industries like financial services, many of the concerns regarding AI harms — like discrimination — are addressed by existing laws; however, data privacy laws and other regulations could potentially prevent some of the potential improvements for consumers and the industry that this disruptive technology could bring.[11]

Conclusion

Financial data and the financial services sector's use of data have long been considered more sensitive due to the potential economic impact on consumers and businesses from abuse or breach. It is still important to consider the burden that regulation may place on positive uses of data and how a growing patchwork of laws could deter innovation or create complexity and confusion. As the committee considers its existing laws and new challenges, it should consider not only how to respond to potential risks, but also how to minimize the impact on beneficial uses of data and new applications of technology. We should consider not only what might be possible today, but how the future may provide new and exciting opportunities and solutions that could improve and expand consumer experiences.

[11] *See* Jack Solowey and Jennifer Huddleston, "Words to Fear: I'm From the State Government, and I'm Here to Help with AI Risk," *Cato at Liberty (blog)*, June 10, 2024.