Statement

of

Jennifer Huddleston

Technology Policy Research Fellow
Cato Institute

before the

Judiciary Committee
Maine State Legislature

October 17, 2023

RE: Data Privacy Working Session

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 and will focus on five of the questions presented today.

(1) What are the benefits and drawbacks of including a private right of action in consumer data privacy legislation?

A private right of action risks bringing litigation that may particularly burden small firms and not actually improve the underlying concerns if there are not appropriate guardrails that ensure such litigation only responds to actual harm and benefits those truly impacted — not just certain attorneys. For this reason, a private right of action for mere statutory violations, one that encourages class actions and extends beyond actual damages, is likely to have significant drawbacks.

One of the key drawbacks of a private right of action is that the actual individuals who experience harm may not be the ones compensated or provided other forms of redress for that harm. Rather, it's the attorneys that bring the cases. For example, one analysis found that "plaintiffs' lawyers received an average settlement of $11.5 million per firm per case, while individuals received an average settlement of $506 per case in litigation under Illinois' Biometric Information Privacy Act."[i] Additionally, companies may be faced with pressure to settle or change practices even if they would have been successful in court due to the costs of litigation, particularly for startups and small companies. Given the risk of potential litigation even if no harm occurs, companies may be more hesitant to deploy certain technology that is beneficial if it is unclear that it meets specific statutory requirements.

As will also be discussed in answers to Question 2, this is not merely theoretical, as the Illinois Biometric Information Privacy Act (BIPA) has a private right of action. The consequences for Illinois residents and businesses have been significant. But these lawsuits have not only been limited to cases where residents' data has been leaked, but to statutory violations where no harm occurred. This is most notable in the case that was brought against Six Flags, where the Illinois court upheld that mere statutory violations, without injury or adverse effect, were sufficient for harm.[ii] Additionally, the total amount of litigation has risen significantly in light of large settlements and court decisions, often without a need to prove actual harm following such an interpretation.[iii] This includes cases against phototagging on popular websites like Facebook[iv] as well as more unexpected cases against trucking companies[v] and White Castle[vi].

(2) Should the Legislature enact standalone bills addressing biometric identifiers and health data in addition to enacting a comprehensive data privacy bill or should the Legislature address all types of consumer personal data in a single bill? Why?

As an individual cannot change certain features — like their iris or fingerprints — and certain information around health can be considered particularly sensitive, policymakers often want to provide additional protection for this information. However, overly broad definitions may cause problems, as can a failure to specifically define the harm that is sought to be addressed. In most cases, proposals only address the concerns about this information in the hands of private actors and do not consider potential abuse by the government of what is considered particularly sensitive information.

At a federal level, certain health information is already protected under the Health Insurance Portability and Accountability Act (HIPAA). As with any privacy law, proposals should be grounded in particular harms and have clear definitions. Health information could be considered so broadly that it could end up applying to a much wider range of apps than likely intended. For example, the resting heart rate on a fitness tracker, the purchase of special dietary requirement food at a grocery store, or a photo with a cigarette could be considered health information under broad definitions subjecting much more data and many more innovators to a law's requirements. Additionally, some of this same "sensitive" information can be helpful in empowering users to take control of their own health, such as apps that can send reminders for medication, track blood sugar, or provide information about what a pregnant woman could expect.

As biometric information such as fingerprints or voice prints cannot be changed, many advocate for additional privacy protection for such information. Washington, Texas, and Illinois have laws applying broadly to biometric information. Biometric information is also covered under some states' comprehensive privacy laws. While often viewed with a skeptical eye, biometric information can be beneficial both for consumers and improving cybersecurity. For example, for many of the same reasons behind the desire to keep the information more secure, biometric information can also be useful for securing access to certain areas or information in a way that improves cybersecurity. Additionally, this information can be used to help identify family and friends in photos or help identify who is at the door with a smart doorbell. Over-regulation might discourage further development of this technology or limit beneficial applications when faced with inflexible regulatory requirements. The result could be as seen in states that currently have these laws that certain features are unavailable.[vii]

(4) Are there particular approaches to consumer data privacy in other states that you consider particularly valuable or problematic?

A dozen states now have comprehensive consumer data privacy laws. As discussed in previous work, due to the nature of data, a federal approach is preferable to a state-by-state approach. Most of these laws have generally followed either California's heavily regulatory approach or a slightly more flexible approach seen in Virginia and Utah.[viii] Of note, Tennessee became the first state to create a safe harbor for compliance with National Institute of Science and Technology

Standards as part of their privacy law.[ix] Such an approach could lessen the burden of state specific compliance costs and be more flexible and adaptive with industry best practices.

A growing patchwork of laws is likely to increase confusion for consumers who will be unlikely to know their rights from state to state and to innovators who may not know how to respond to potentially conflicting requirements or what to do in certain scenarios. As such, it is a far from ideal solution. For example, there is currently a 50-state patchwork of data breach notification laws, but these laws vary in the type of information covered, what constitutes notification, the timelines for notification, and what consumers should be notified.[x] This will only be more pronounced in the case of more general data privacy laws.

A federal approach remains preferable to a state-by-state approach for both innovators and consumers. For example, one study found "the out-of-state costs from 50 such laws could exceed $1 trillion over 10 years, with at least $200 billion hitting small businesses."[xi] Many of these costs will likely be passed on to the consumer at a time when consumers are already concerned about rising prices.

(5) What existing federal laws protect consumer personal data in your industry (or the industry of concern to you) – what types of data do those laws protect (or not protect) and what types of companies do they regulate (or not regulate)?

Contrary to popular belief, the United States is not without any data privacy laws. Rather than take an overarching approach, the federal government (as well as states) have responded to concerns related to specific types of data that is considered more sensitive or to specific populations, such as children, that are considered more vulnerable or unable to properly consent.[xii] When considering data privacy, it is important to recognize that while it is typically thought of as an online issue, many offline businesses and industries have benefited from the use of data and would be affected by these laws. In fact, looking at Europe, everything from more commonly thought of services like retail loyalty programs to less likely considered entities like churches and cemeteries have been impacted by concerns about ensuring compliance with data privacy laws.[xiii]

Given the growing use of data in a wide array of industries, it is important to consider what harms a privacy law is trying to address. Penalizing certain types of data or creating mere statutory violations might prevent innovative beneficial applications in the future as well as impact those that already exist and do not cause harm.

(6) Are there any pending Congressional proposals regarding consumer data privacy of which the Maine Legislature should be aware?

The 117th Congress saw perhaps the most progress on a federal data privacy bill. The American Data Privacy Protection Act was a bipartisan bill that passed through committee in the House of Representatives, but failed to have further action that Congress. Congress continues to debate

possible data privacy; however, a similar bipartisan approach or comprehensive bill has not yet gained momentum in the 118th Congress.

Conclusion

Thank you for your time and consideration of this information. I welcome any questions related to my research on data privacy and my responses to these questions. This testimony should be considered for informational purposes and not in support of or opposition to any particular piece of legislation.

[i] Kaitlyn Harger, *Who Benefits from BIPA: An Analysis of Cases Brought Under Illinois' State Biometrics Law*. Chamber of Progress (2023). Accessible at https://progresschamber.org/wp-content/uploads/2023/03/Who-Benefits-from-BIPA-Analysis-of-Cases-Under-IL-Biometrics-Law.pdf.

[ii] *Rosenbach v. Six Flags Entertainment Corp*. (Illinois 2019).

[iii] *Illinois Biometric Privacy Cases Jump 65% After Seminal Ruling*. Bloomberg Law (2023). Accessible at https://news.bloomberglaw.com/privacy-and-data-security/illinois-biometric-privacy-cases-jump-65-after-seminal-ruling.

[iv] Victoria Cavaliere, *Judge approves $650 million settlement of Facebook privacy lawsuit linked to facial photo tagging.* Business Insider (2021). Accessible at https://www.businessinsider.com/facebook-settlement-pay-650-million-privacy-lawsuit-biometrics-face-tagging-2021-2?utm_source=copy-link&utm_medium=referral&utm_content=topbar.

[v] Robert D. Boley, Paula M. Ketcham, and Adam L. Littman, *First BIPA Trial Results in $228M Judgment for Plaintiffs.* National Law Review (2022). Accessible at https://www.natlawreview.com/article/first-bipa-trial-results-228m-judgment-plaintiffs.

[vi] Barry P. Kaltenbach and Robert T. Zielinski, *The $17 Billion Slider? Illinois Supreme Court Decides White Castle BIPA Case.* National Law Review (2023). Accessible at https://www.natlawreview.com/article/17-billion-slider-illinois-supreme-court-decides-white-castle-bipa-case.

[vii] *Google's art selfies aren't available in Illinois: Here's why*. Chicago Tribune (2023). Accessible at https://www.chicagotribune.com/business/ct-biz-google-art-selfies-20180116-story.html.

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

[ix] Tennessee Information Protection Act (2023), accessible at https://www.capitol.tn.gov//Bills/113/Amend/HA0348.pdf.

[x] *State Data Breach Notification Chart*. International Association of Privacy Professionals (2021). Accessible at https://iapp.org/resources/article/state-data-breach-notification-chart/.

[xi] 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/.

[xii] Alan McQuinn, *Understanding Data Privacy*. Real Clear Policy (2018). Accessible at https://www.realclearpolicy.com/articles/2018/10/25/understanding_data_privacy_110877.html.

[xiii] *If You Run a US Cemetery Here's Why GDP's Your New Best Friend.* Plot Box (2019). https://www.plotbox.io/blog/gdpr-in-us-cemeteries; *Data Protection: Parishes and GDPR*. Accessible at https://www.parishresources.org.uk/gdpr/.