HOUSE OF REPRESENTATIVES
2 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0002
(207) 287-1400
TTY: MAINE RELAY 711

Amy Kuhn
P.O. Box 66831
Falmouth, ME 04105
(207) 939-6903
Amy.Kuhn@legislature.maine.gov

May 5, 2025

Testimony of Representative Amy D. Kuhn introducing

LD 1822, An Act to Enact the Maine Online Data Privacy Act

Before the Joint Standing Committee on Judiciary

Senator Carney and distinguished members of the Judiciary Committee, my name is Amy Kuhn, and I proudly represent most of Falmouth in House District 111. It is a pleasure to be with you today to introduce **LD 1822, An Act to Enact the Maine Online Data Privacy Act.**

Life in America today is inextricably intertwined with the devices we use, the browsers we access and the apps we open. From shopping to dating, health care to banking, entertainment to travel, every swipe, scroll and click we make generates a trail of data that can be deeply revealing.

No doubt these linkings can produce convenient results. However, left unchecked, this vast trove of data makes us vulnerable to a myriad of risks, including civil rights violations, identity theft, financial exploitation and unlawful discrimination. The right to control our personal information is essential in the digital era.

Let's get specific. Why should we care about data privacy? Here are some examples:

1. Civil rights –

    - Policing – Police departments can now circumvent warrant requirements by buying sensitive data directly in the marketplace. The Brennan Center reports: "The government's ability to buy sensitive location information without judicial or legislative oversight upends the time-honored balance of power between the people and the government established by the Fourth Amendment."[1]

    - Discrimination – The use of data about race and gender in Artificial Intelligence (AI) decision making algorithms has resulted in different housing and employment opportunities being presented to people based on their personal profiles. For example, a University of Chicago study found that: "Facebook's ad algorithm used personal data to deploy targeted housing advertisements that discriminated against Black, Hispanic, and Asian users." These practices included

[1] Federal Agencies Are Secretly Buying Consumer Data, https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data

assigning lower priority to certain applications or offering higher interest rates to others.[2] Similarly, data about gender has been used to filter job postings, often "based on historical gender stereotypes," showing, for example, ads for mechanics more often to men and ads for preschool teachers more often to women.[3]

2. Risk of Breach – Cyber attacks and subsequent data breaches are ubiquitous and pose significant threats to consumers' personal and financial security.[4] Limiting collection on the amount and sensitivity of personal data on the internet helps reduce the risk of sensitive information from falling into the wrong hands.

3. Loss of Unbiased Viewpoint – When we open our phones, we do not see an objective portrayal of the world for us to consider and evaluate. Instead, the data that is collected about us facilitates the creation of a customized reality based on how an algorithm assesses our interests. The long term implications and consequences of this are unknown.

Since 2018, many states have adopted comprehensive data privacy laws. The first wave of these laws have been consent based laws, or what has been referred to here as the Connecticut Model. This model does offer new consumer rights such as the right to request, correct and delete data that has been collected about them. However, in terms of these companies' foundational business models, these laws essentially enshrine the status quo. In short, a company can collect, process and sell any data at all, so long as their practices are disclosed in their terms and conditions page and the consumer consents. There's only one problem – who reads the terms and conditions page? Almost no one. Most people click "accept" or "allow" or whatever the prompt may be so that we can get on with whatever we want to be doing, resulting in practice in no informed consent at all.

The second wave of laws prioritize real data minimization. This sets actual limits on what data can be collected and what companies can do with it. In order to be collected, personal data must be "reasonably necessary and proportionate" to the product or service the consumer requests. Sensitive data can only be collected if it is "strictly necessary" to the product or service requested. And, sensitive data cannot be sold. This means that any sensitive data that a consumer chooses to share will stay where the consumer left it, not travel around the internet without their knowledge.

This focus on data minimization brings us real benefits – it deters the possibility of civil rights violations, it protects us in the event of breach and it creates stronger data sets for AI.

[2] AI is Making Housing Discrimination Easier Than Ever Before, https://kreismaninitiative.uchicago.edu/2024/02/12/ai-is-making-housing-discrimination-easier-than-ever-before/recruitment practices

[3] People are missing out on job opportunities on Facebook because of gender, research suggests: https://www.cnn.com/2023/06/12/tech/facebook-job-ads-gender-discrimination-asequals-intl-cmd/index.html

[4] The Biggest Data Breaches in 2024: 1 Billion Stolen Records and Rising, https://techcrunch.com/2024/10/14/2024-in-data-breaches-1-billion-stolen-records-and-rising/

This data minimization approach was signed into law earlier this year in Maryland. Data minimization is also central to bills pending now in Massachusetts and Vermont, and in amendments pending in Connecticut.

I would like to walk you through the bill and describe some highlights so that you have landmarks in the bill for further review, including:

- P. 4 Definitions
- P. 6 Applicability
- P. 6 Exceptions
- P. 9 Consumer rights
- P. 12 Actions of controllers
- P. 13-14 Opt out of targeted advertising
- P. 17 Data protection Assessments
- P.21 Enforcement
- P.22 AG Reports

In summary, through this bill, I have sought to respect and carry over the tremendous progress that the Legislature and the business community made in the 131st while addressing the business concerns that remained at the end of session. In the 132nd, Maine has an opportunity to enact a truly robust privacy law, where we strike a balance between innovation and accountability, and foster a safer, more equitable digital ecosystem for generations to come.

I thank you for the opportunity to present this bill. I would be happy to answer any questions.