AMERICAN CIVIL LIBERTIES UNION
Maine

PO Box 7860
Portland, ME 04112

(207) 774-5444
ACLUMaine.org
@ACLUMaine

TESTIMONY OF MICHAEL KEBEDE, ESQ.

LD 1822 – Ought to Pass
An Act to Enact the Maine Online Data Privacy Act

LDs 1224, 1088, 1284 – Ought Not to Pass
An Act to Comprehensively Protect Consumer Privacy
An Act to Enact the Maine Consumer Data Privacy Act
An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information

Joint Standing Committee on Judiciary
May 5, 2025

Senator Carney, Representative Kuhn and distinguished members of the Joint Standing Committee on Judiciary, greetings. My name is Michael Kebede and I am policy director at the ACLU of Maine, a statewide organization committed to advancing and preserving civil liberties guaranteed by the Maine and U.S. Constitutions. On behalf of our members, I urge you to support LD 1822 and oppose LDs 1224, 1088, and 1284.

The ACLU has a long history of protecting the right to privacy, both as it pertains to governmental and to business intrusions into that right. The ACLU of Maine was instrumental in the drafting and passage of several of our state's seminal privacy laws, including our internet service provider privacy law, which is the strongest in the nation,[1] the law restricting the government's ability to use facial recognition technology, also the nation's strongest,[2] and the law requiring a warrant in order for law enforcement to access portable electronic information or cell phone location information.[3] Two of the bills before you today – LDs 1088 and 1284 – would repeal our internet privacy law. LD 1088 goes further, as does LD 1224, to propose industry-written rules that would not provide Maine people with enough protections. Only LD 1822 would meaningfully expand privacy rights.

The Need for Meaningful Privacy Legislation

Large technology companies have built a surveillance economy that seeks to collect and monetize as much information about us as possible. These companies harvest data about what we do at home, what we do at work, what we buy, where we go, what doctors we see,

[1] *See* 35-A M.R.S. §9301.
[2] *See* 25 M.R.S. §6001.
[3] *See* 16 M.R.S. §641 et seq., §647 *et seq.*

our contacts with the criminal and civil legal systems, and virtually any other measurable dimension of our behavior. In the United States, these companies face almost no real restrictions on the amount of personal information they can amass about us or the ways that they can exploit it. In the absence of meaningful protections, companies have compiled staggering amounts of information about each of us. This information can identify us across our interactions with the world both online and off, in public and in private, enabling an unprecedented power to predict and modify our behavior.

These unprecedented powers to predict and modify our behavior can be and are being sold to data brokers or used to manipulate public opinion, power surveillance-based advertising, and shape our decisions in any way intended by those able to pay. Many of these uses have discriminatory impacts, such as when companies exclude people from seeing advertisements for employment, housing, or credit on the basis of their gender, race, nationality, or membership in another protected class. Other uses undermine the very foundations of our constitutional democracy, fueling polarization or feeding skepticism about the integrity of our elections. Each of these harms can be traced back to the tech industry's unregulated amassment and analysis of intimate details of our lives.

To stop these harms, consumer privacy legislation must, at a minimum, contain these features:

- **Data minimization.** It is not enough that consumers receive notice of what personal data is collected and shared or that they are able to consent – especially when "notice" and "consent" are functionally legal fictions. "Notice" is commonly provided through privacy policies, and those policies are so dense and lengthy that they fail to provide any real "notice" at all. Similarly, "consent" is often inferred from use of the site or service or by clicking on a banner that provides no information on the service's data practices. Notice and consent cannot be the only protections that consumers are afforded. Instead, laws must minimize data collection and the ways that data can be used – meaning that services and sites should only be allowed to collect, use, and disclose data as is necessary to provide what the consumer requested. Collecting and storing more data than what is needed to provide a good or service increases the harms of data breaches, since malicious actors can obtain more data than if companies collected only what was necessary.

- **Requiring opt-in consent before companies collect and use our personal information.** Maine's internet service provider privacy law requires opt-in consent before internet service providers can sell our information, and that is a crucial protection for internet users. The so-called consumer privacy laws in Connecticut, Utah, Colorado, and eleven or so other states often apply "opt-in" only to a limited set of data, which is problematic because data mining and machine learning can use information that is not particularly sensitive to obtain a very specific picture of sensitive information.

- **Civil rights protections.** Our personal data is increasingly used in ways that affect our opportunities in traditionally protected areas of life such as housing, education, employment, and credit. There is ample evidence of the discriminatory harm that artificial

intelligence (AI) and algorithmic systems can cause to already marginalized groups.[4] Bias is often baked into the outcomes the AI is asked to predict and the data used to train the AI, which can manifest throughout the AI's design, development, implementation, and use. The impact on the daily lives of Americans is unprecedented. Banks and other lenders use AI systems to determine who is eligible for a mortgage or student loan. Housing providers use AI to screen potential tenants. AI now often decides who's helped and who's harmed with influential predictions about who should be jailed pretrial, admitted to college, or hired. A comprehensive privacy law must ensure that the use of our data in AI adheres to our foundational values of equality and nondiscrimination.

- **Private right of action.** A private right of action, especially in a state as small as Maine, is crucial to ensuring that companies are held accountable for breaking the law. The experiences of other states is illustrative: Illinois has a private right of action to enforce violations of its Biometric Information Privacy Act, while Washington and Texas do not. Washington and Texas, though their offices of the Attorney General are much bigger than Maine's, have not meaningfully enforced their biometric privacy laws. The private right of action in Illinois has been enforced by individual litigants. You may hear much about the sky falling in Illinois, but we can learn lessons from that state to ensure that a private right of action serves its intended purpose, rather than jettisoning it altogether.

Of the bills before you today, LD 1822 includes most of these features. It does, however, lack two important features: a private right of action and a data minimization framework that restricts not just collection, but also sale and disclosure of non-sensitive information.[5] In contrast, not only do LDs 1224 and 1088 also lack a private right of action, but they also lack an adequate data-minimization provision.

Why LDs 1224, 1088, and 1284 Ought Not to Pass

LDs 1088 and 1284 would both repeal our existing internet service provider privacy law, which prohibits internet companies from using or selling your data without your consent.[6] These bills represent the latest attempt in a long series of the tech industry's attempts to have the legislature repeal or a judge invalidate Maine's internet privacy law. Each of these attempts has failed.[7] But the tech industry is, apparently, undaunted. That is because repealing our internet privacy law will make it easier for tech companies to collect and monetize information about Mainers, with dire

[4] Kaveh Waddell, *How Tenant Screening Reports Make It Hard for People to Bounce Back From Tough Times*, Consumer Reports, March 11, 2021, *available at* https://www.consumerreports.org/electronics/algorithmic-bias/tenant-screening-reports-make-it-hard-to-bounce-back-from-tough-times-a2331058426/ (showing how tenant-screening algorithms are prone to errors and incorrectly include criminal or eviction records tied to people with similar names); Jeffrey Dastin, *Insight - Amazon scraps secret AI recruiting tool that showed bias against women*, Reuters, Oct. 10, 2018, *available at* https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G/ (reporting about how algorithmic resume scanners preference male candidates, are inaccessible to applicants with disabilities, and may de-preference first-generation college graduates.)

[5] *See* LD 1822, p. 12, lines 36-38.

[6] *See* 35-A M.R.S. §9301.

[7] *See, e.g., Internet service providers drop their challenge to Maine privacy law*, BDN, Sept. 6, 2022, *available at* https://www.bangordailynews.com/2022/09/06/politics/maine-privacy-law-challenge/.

consequences for Mainers' privacy, physical safety, and legal jeopardy. We strongly urge this committee to reject these bills and preserve Maine's pathbreaking internet privacy law.

We also urge you to oppose LDs 1088 and 1224. Although the ACLU shares the concerns that prompted the sponsors to propose these bills, we believe that the bills will not have the intended protective effect. LD 1224 would allow any sale or transfer of your data as long as the use is disclosed in a privacy policy.[8] LD 1088 would similarly allow any sale or transfer of your data as long as it is disclosed in a Terms and Conditions page or you click "I agree".[9] As you know, nobody really reads Terms and Conditions pages, and most of us click "I agree" without thinking twice. According to one peer-reviewed study, "98% of the participants did not read any agreement" for their cellphone applications.[10] Neither bill would even require tech companies to seek your opt-in permission for the sale of your data, but would instead require you to ask them to stop.[11] Similarly, neither LDs 1088 nor 1224 provide meaningful protections against use of our data in invidious discrimination — a crucial supplement to existing civil rights laws as AI increasingly makes decisions about who has access to housing, employment, education, credit, and more.

Conclusion

Thank you for the opportunity to present our testimony on the privacy legislation pending before you. The surveillance economy poses grave threats to democracy and personal autonomy. After carefully analyzing all four bills before you, we have concluded that only LD 1822 would provide meaningful protections.

To be sure, LD 1822 is not perfect: It would not apply to companies that process the data of fewer than 35,000 Maine residents. It exempts nonprofits and other entities. It does not include a private right of action, meaning that Mainers must rely on the Attorney General to enforce their data privacy rights. Its data minimization rule applies to collection but not to disclosure of personal data. These compromises represent a middle-ground between no data privacy protections and the strongest possible protections, and Maryland enacted a very similar compromise last year. Despite its limitations, LD 1822 is a better starting point than any other bill before the legislature. We urge you to support it and oppose LDs 1224, 1088, and 1284.

[8] *See* LD 1224 at p. 9, lines 24-32.
[9] *See* LD 1088 at p. 10, lines 12-15.
[10] Saadia Nemmaoui et al., *Privacy conditions changes' effects on users' choices and service providers' incomes*, International Journal of Information Management Data Insights, Vol. 3, Issue 1, Apr. 2023, *available at* https://www.sciencedirect.com/science/article/pii/S2667096823000204.
[11] LD 1224 at p. 7, line 39; LD 1088 at p. 8, line 30.