AMERICAN CIVIL LIBERTIES UNION
Maine

PO Box 7860
Portland, ME 04112
(207) 774-5444
www.aclumaine.org

TESTIMONY OF MEAGAN SWAY, ESQ.

LD 1977 – Ought To Pass

An Act to Create the Data Privacy and Protection Act

Joint Standing Committee on Judiciary

October 17, 2023

Senator Carney, Representative Moonen, and distinguished members of the Joint Standing Committee on Judiciary, good morning. My name is Meagan Sway, and I am Policy Director for the ACLU of Maine, here to speak in support of LD 1977, *An Act to Create the Data Privacy and Protection Act.* The ACLU of Maine defends and promotes the fundamental principles and values embodied in the Bill of Rights, the U.S. Constitution, and the Maine Constitution. As part of a nationwide network of ACLU affiliates, we offer not only our own experience working at the intersection of privacy and technology, but also the lessons learned by our sister affiliates in states that have been on the cutting edge of legislating to protect privacy in the digital age.

Corporations have built a surveillance economy that seeks to collect as much information about a person as possible to turn a profit, and it threatens our democracy. It is no longer possible to participate in society without providing personal information to private companies and other third parties that may, in and of itself, reveal details of one's life, or that, when combined with other data and analyzed, may expose such information. The consequences can be profound. For example, personal information has been leveraged so that only younger men see certain job postings and to exclude Black people from viewing certain housing advertisements.[1] Often, that data is readily available to governmental entities outside of the normal procedures for obtaining a warrant and outside judicial oversight.

In addition, as entities increasingly turn to sophisticated algorithms and automated decision-making to place ads, screen resumes, or in government hands, to make bail decisions, decide where to deploy police, or to make child custody decisions, the

---

[1] *See* Galen Sherwin & Esha Bhandari, *Facebook Settles Civil Rights Cases by Making Sweeping Changes to Its Online Ad Platform*, ACLU Speak Freely, Mar. 19, 2019, https://www.aclu.org/blog/womens-rights/womens-rights-workplace/facebook-settles-civil-rights-cases-making-sweeping.

training data used to develop the algorithms can have outsized impacts on individuals' opportunities and outcomes. In the political realm, companies have used our personal information shared on social media to manipulate us into voting for a certain candidate, abstaining from voting altogether, or joining movements that undermine democracy itself.[2]

Although there are portions of LD 1977 that we propose amending, in general, we support this legislation's approach to privacy regulation and urge the committee to pass it in an amended form. Below, I lay out the portions of the bill that we particularly support and think are important to maintain, as well as suggested amendments.

First and foremost, in order to reign in the harms of the surveillance economy, consumer privacy legislation must contain strong provisions designed to minimize the amount of personal information that can be collected and the ways it can be used. Legislation that protects consumers must establish data-minimization limitations that prevent companies from collecting and retaining more data than they need to provide the services we ask for. LD 1977 does just that. It states that entities covered by the bill "may not collect, process, or transfer covered data unless the collection, processing or transfer is limited to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the individual to whom the data pertains."

Second, for personal information that corporations are allowed to collect, there must be a requirement that consumers opt in, as opposed to requiring them to opt out, of the collection and use of their information. LD 1977 requires consumers to affirmatively opt in to the transfer of sensitive data (as defined by the bill) to third parties, §9605(3), transfer of video content or services on broadcast TV, cable, or streaming service, §9605(4), processing or transferring data for a purpose other than that which a consumer originally gave their affirmative consent, §9609(3), targeted advertising, §9610(1), transfer data related to minors, §9611(8), or retain data longer than necessary, §9616(2)(D).

Third, we appreciate the civil rights protections in LD 1977. 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

---

[2] Examples of this include the infamous Cambridge Analytica, which used over 50 million Facebook users' personal information to engage in "psychographics" that manipulated voters, *see* Timothy B. Lee, *Facebook's Cambridge Analytica scandal, explained [Updated]*, Ars Technica, Mar. 20, 2018, https://arstechnica.com/tech-policy/2018/03/facebooks-cambridge-analytica-scandal-explained/, or advertisers targeting Black voters in an effort to convince them to abstain from voting, *see* Natasha Singer, *'Weaponized Ad Technology': Facebook's Moneymaker Gets a Critical Eye*, Aug. 18, 2018, https://www.nytimes.com/2018/08/16/technology/facebook-microtargeting-advertising.html.

systems can cause to already marginalized groups. 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 our daily lives is unprecedented. Banks and other lenders use AI systems to determine who is eligible for a mortgage or student loan. Landlords use AI to screen potential tenants. AI decides who is helped and who is harmed with influential predictions about who should be jailed pretrial, admitted to college, or hired. Section 9614 specifically prohibits discrimination in data collection, processing or transfer, and in using data to make unavailable the equal enjoyment of goods or services on the basis of a user's membership in certain protected classes.[3] Section 9615 requires companies to do impact assessments of the algorithms used in their AI. Both of these will help ensure that Maine's laws adhere to our constitutional values of equality and nondiscrimination.

Finally, we are in strong support of making sure that any privacy legislation that goes forward has a private right of action. Without a private right of action, companies will have little incentive to comply with the law, and Mainers will have little practical way to seek relief when their personal information is unscrupulously collected or misused.

The experience in other states underscores that a lack of a private right of action effectively means an utter lack of enforcement. States with laws protecting against the misuse of biometric information (finger prints, voice prints, face prints, DNA, etc.) allow us to see clearly the dangers of denying consumers the right to sue companies that violate their rights . In 2008, Illinois passed the Biometric Information Privacy Act. In 2009, Texas passed a similar law, and in 2017 Washington passed its own version. The major differences between Illinois' law on the one hand, and Texas and Washington's laws on the other, is that Illinois' law has a private right of action but Texas and Washington's allow only the Attorney General to sue for enforcement. Despite being on the books for more than a decade, I have only been able to find two cases brought by the Texas Attorney General to enforce the state's biometric privacy laws, both initiated in 2022. I was unable to find evidence of the Washington Attorney General enforcing its biometric privacy law at all. (In 2023, Washington passed a health data privacy law that now allows a private right of action for misuse of health and biometric information.) In contrast to Texas and Washington, residents of Illinois have had their rights zealously protected in court since the law's inception.

LD 1977 contains limitations on the private right of action that Illinois' law does not have, such that industry's opposition to the private right of action should be treated with skepticism. Under LD 1977, private rights of action may only be brought against companies whose gross annual revenues totaled $41 million or more, who

[3] A final version of LD 1977 should include all protected classes under the Maine Human Rights Act, not just those currently listed in the bill.

did not annually collect or processed the data of more than 200,000 individuals, and who are not data brokers. The ACLU of Maine believes these limits are high, but we do believe that some lower limitation would be acceptable.

The ACLU of Maine does propose some changes to the legislation:

- Incorporate the ban on the sale or leasing of biometric identifiers contained in LD 1705, *An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data.* Because our biometric identifiers include our most personal, intimate and unchangeable data, the legislature should provide the utmost protection for this data.
- Ensure that all protected classes under the Maine Human Rights Act are incorporated into the prohibitions on discrimination in §9614.
- Add definitions for the terms transfer, collect, process, and publicly available information to ensure that companies have clear guidance on what is allowed and what is prohibited.
- Ensure that the protections in Maine's internet service provider privacy law, 35-A M.R.S. §9301, are not reduced. Internet service providers are in a unique position to gather information about our every move on the internet, and it is appropriate that they continue to be constrained by the current law.
- Clear up language in §9607 to make sure that the legislation does not contain a pay-for-privacy provision. Subsection one of this provision states that entities may not charge a different price for people who refuse to allow their personal data to be collected, but subsection three potentially allows companies to do just that.
- Change language in the bill so that customers are not required to opt-out of targeted advertising, but instead require companies to obtain opt-in permission.