ACLU
AMERICAN CIVIL LIBERTIES UNION
Maine

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

TESTIMONY OF MEAGAN SWAY, ESQ.

Ought Not To Pass – LD 1973

An Act to Enact the Maine Consumer Privacy Act

Joint Standing Committee on Judiciary

May 22, 2023

Senator Carney, Representative Moonen, and members of the Joint Standing Committee on Judiciary, good morning. My name is Meagan Sway and I am Policy Director for the American Civil Liberties Union of Maine, a statewide organization committed to advancing and preserving civil liberties guaranteed by the Maine and U.S. Constitutions through advocacy, education, and litigation. On behalf of our members, I urge you to reject LD 1973.

The ACLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovations. The ACLU of Maine has been a partner in some of the Maine Legislature's best privacy work: we helped write and pass legislation requiring warrants for cell phone location tracking, the strongest-in-the-nation internet service provider privacy laws, and strict limitations on government officials' ability to use facial recognition data, among other laws. Unfortunately, LD 1973 would not protect peoples' privacy, but instead make Mainers' private information less secure.

LD 1973 appears to be largely based on legislation passed in other states such as Virginia, Colorado and Utah. This legislation was written by corporations who make tremendous amounts of money off of a surveillance economy that seeks to collect as much information as possible to turn a profit. They harvest data about what we do at home, what we do at work, what we buy, where we go, what doctors we see, our contacts with the criminal legal system, and more. 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 protections, companies have compiled massive dossiers on each one of us containing staggering amounts of information. This information can identify us across our interactions with the world both online and off, within our homes and outside of them, creating the potential for private surveillance on a massive scale. That information can then be sold to data brokers or used to power surveillance-based advertising.

In order to stop these harms, consumer privacy legislation must, at a minimum, contain strong restrictions on the amount of personal information that can be collected and the ways in which it can be used, including: requiring opt-in consent before companies collect and use our personal information; providing users with the tools to access and control their personal information; creating strong new civil rights protections; prohibiting companies from discriminating against people who exercise their privacy rights under the law; enabling people to sue privacy-violating companies to obtain meaningful monetary relief; and preserving the ability of local activists to seek—and local governments to enact—stronger protections. LD 1973 lacks all of these protections.

LD 1973 fails to protect the privacy of Maine residents in the following ways:

- **Repeal of Maine's strongest-in-the-nation, first-of-its kind internet service provider privacy law from 2019.**[1] LD 1973 would replace our current internet service provider privacy law ("ISP law") with much weaker provisions that do not protect consumers. It is crucial to keep Maine's ISP law in place because internet service providers—Charter, Verizon, Comcast, Time Warner Cable, etc.—see every keystroke we make online. And, while we can choose whether to activate a Facebook page, or use a search engine other than Google, the vast majority of people today cannot opt out of using the internet. A 2021 Federal Trade Commission report describes the wide-ranging and disturbing ways in which internet service providers collect data on internet users.[2] Because ISPs have vertically integrated with services like home security, video streaming, email, connected cars, etc., they collect an enormous amount of data about consumers at a granular level, including information typed into emails and into web searches that reveal very detailed information about each of us. In Maine, unlike the rest of the country, our ISP law: (1) protects "[i]nformation from a customer's use of broadband Internet access service, including" the customer's web browsing history, application usage history, health information, information pertaining to a customer's children, the contents of a customer's communications, among other things from invasion of privacy and (2) requires internet service providers to obtain "express, affirmative consent" before it can use, disclose, sell or permit access to" a customer's information; and prohibits internet service providers from engaging in pay-for-privacy schemes that allow people

[1] 35-A MRS §9301.

[2] *See* Federal Trade Commission, *A Look At What ISPs Know About You: Examining the Privacy Practices of Six Major Internet Service Providers: An FTC Report*, Oct. 21, 2021, available at https://www.ftc.gov/system/files/documents/reports/look-what-isps-know-about-you-examining-privacy-practices-six-major-internet-service-providers/p195402_isp_6b_staff_report.pdf.

with money to have privacy and those without to lose theirs.[3] LD 1973 would undo these protections and replace them with marginally useful protections. Any privacy law worth its title would take our ISP law's protections as the baseline and build from there, not reduce the protections we already have in place.

- **Limited opt-out, rather than strong opt-in consent requirement:** LD 1973 permits the collection, use, and sharing of personal information unless the consumer opts out, and only allows consumers to protect themselves by opting out of three categories of uses (targeted advertising, sale of certain data, or profiling for the purposes of automated decisions about a person). This framework places the burden entirely on the consumer to wade through reams of legalese with multiple service providers in order to exercise their privacy rights. Additionally, the ability to opt out only from sale of personal information, but not use of that information, means that the data practices of the largest surveillance companies like Facebook and Google will remain mostly untouched. That is because Facebook and Google claim not to sell our personal information; rather, they amass information about their own users, buy people's information from other companies, and then sell access to tools that make invasive use of that information. Only a strong and broad opt-in consent requirement can adequately protect people's privacy.
- **Provides illusory protection for "sensitive information."** LD 1973 distinguishes between "personal data" and "sensitive data," and provides an additional right to consent to the processing of "sensitive data." Sensitive data is defined as data that reveals race or ethnic origins, religious beliefs, sexual orientation, citizenship and immigration status, and mental or physical health conditions or diagnoses. Although motivated by important concerns, this provision will leave people exposed to the very kinds of privacy violations that it seeks to avoid. Personal data that doesn't *expressly* reveal "sensitive" facts can also be highly sensitive, and when aggregated can reveal these sensitive characteristics even if individual data points do not. Indeed, the entire point of compiling massive stores of personal information by companies is to infer detailed information about people that any one piece of data does not reveal by itself. Additionally, the way LD 1973 defines consent is very broad, and allows for businesses to use a pop up window allowing people to click "I consent" or burying the consent in a privacy statement that most consumers never read.
- **Allows discrimination against people who exercise their right to opt-out.** Section 9605(3) allows companies to discriminate against users who exercise their right to opt-out of targeted advertising by charging the consumer higher prices or offering inferior service, disguised as allowing people to participate in "loyalty and rewards programs." This pay-for-privacy provision risks making privacy a luxury good, available only to those who can

[3] 35-A MRS §9301

afford to pay for it, further marginalizing the most marginalized, and exacerbating the existing digital divide.

- **Lacks meaningful civil rights protections.** LD 1973 fails to meaningfully restrict uses of personal information that harm civil rights. There should, at a minimum, be a requirement for companies to test their automated systems for bias. A strong bill would also include restrictions on the use of personal information in a manner that excludes people from opportunities on the basis of their membership in a protected class.
- **Weak enforcement provisions.** The enforcement provided in this bill is especially weak and means that it is exceedingly unlikely that any company will be held accountable for violations of the privacy protections that do exist in the bill. As written, the Attorney General would need to issue a notice of violation and right to cure letter to an entity violating the law. Even then a data collector could avoid any accountability by simply telling the Attorney General within 30 days that the data collector has fixed the problem (without supplying proof), at which point there could be no further action against the data collector. Given the limited resources of our consumer protection division and the limitations on enforcement in the bill, it is highly unlikely this law would be meaningfully enforced in the future. Without a private right of action, people have little practical ability to seek relief when their personal information is unscrupulously collected or misused. This eliminates a powerful incentive for companies to comply with the law. When companies ignore the law, a private right of action allows affected individuals to obtain redress for the harm they have suffered. A private right of action is also vital because government agencies do not have the resources to investigate every case—or sometimes any case—where people's rights are violated. And when intrusive corporate privacy practices put people's information within the reach of the police, it's people—not another government entity—who need the ability to push back in court. A private right of action both conserves state resources and ensures that state residents can vindicate their own rights.

We urge you to protect Mainers' privacy by rejecting LD 1973.