

MAINE STATE LEGISLATURE

The following document is provided by the
LAW AND LEGISLATIVE DIGITAL LIBRARY
at the Maine State Law and Legislative Reference Library
<http://legislature.maine.gov/lawlib>



Reproduced from scanned originals with text recognition applied
(searchable text may contain some errors and/or omissions)

Bruce C. Gerrity
bgerrity@preti.com
207.623.5300

May 7, 2025

Senator Anne Carney
Representative Kuhn
Judiciary Committee
3 State House Station
State House, Room 438,
Augusta, Maine 04333

RE: LD 1088 An Act to Enact the Maine Consumer Data Privacy Act
LD 1224 An Act to Comprehensively Protect Consumer Privacy
LD 1284 An Act to Repeal Provisions of Law Governing the Privacy of
Broadband Internet Customer Personal Information
LD 1822 An Act to Enact the Maine Online Data Privacy Act

Dear: Senator Carney and Representative Kuhn,

These comments augment the testimony presented at the public hearing on the above bills. The Maine Automobile Dealers Association (MADA) is the Association of all new car and truck dealers in Maine. Maine dealers are required to comply with a number of different statutes which impose varying privacy obligations. As such, Maine dealers should be fully exempt from the various provisions of the proposed legislation.

Several of the proposed bills before the Committee do exempt data provisions, such as the Gramm-Leach-Bliley Act (GLBA). Dealers are regulated by GLBA. Dealers are also broadly regulated by the Federal Trade Commission (FTC) (15 USC, section 41 et seq.), and more specifically, by the Fair Credit Reporting Act, (15 USC, section 1681(FCRA)) and the Fair and Accurate Credit Transaction Act (FACT Act), (15 USC, section 1601). These two laws, along with the FTC Rules and regulations, protect consumer data in relation to credit transactions, and more broadly, information received from consumers by dealers. The Red Flags Rule is part of FTC regulation, also known as the FACT Act Identity Theft Rules. This rule requires dealers to implement a written identity theft prevention program designed to detect warning signs of identity theft. This involves protecting sensitive consumer information. The Red Flags Rule was issued in 2007 under section 114 of the FACT Act, which in turn amended the FCRA. The Rule is published at 16 CFR 681.1.

In addition, even though dealers have obligations to keep data and consumer information private, they are also required to report to the Internal Revenue Service (IRS) the receipt of cash or cash equivalents of more than \$10,000 in a single transaction or two or more related transactions. IRS form 8300: BSA E-FILING System. This requires reporting "identifying documents" in some detail.

May 7, 2025

Page 2

In addition, MADA runs a Multiple Employer Welfare Arrangement (MEWA). This is a self-insured health plan offering coverage to dealers and their employees and families. It is regulated by the Bureau of Insurance. 24-A MRS ch.81. This regulatory authority extends to the privacy chapter of Title 24-A (24-A MRSA ch.24). This means dealers' privacy requirements are also regulated by the Bureau.

Also, telematics is now a critical component of owning and operating a motor vehicle. As such, Maine dealers are privy to significant consumer information stored in a vehicle's electronic components. The Maine right to repair statute, 29-A MRS §1801 et seq., does regulate access to telematics for repairs. The Housing and Economic Development Committee (HED) has received a report authorized pursuant to resolve 2023, ch.171 to advise it about various aspects of Right to Repair.

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwis77Wd1JGNAXW5GkFHflgH-0QFnoECBcQAQ&url=https%3A%2F%2Fwww.legislature.maine.gov%2Fdoc%2F11596&usg=AOvVaw29lSId8edWeD7ochlOBV7a&opi=89978449>

Central among those issues are consumer privacy protections, safety protections, and cyber security. The HED Committee is reviewing several bills, which include LDs 292, An Act to Implement the Automotive Right to Repair Working Group Recommendations, 442, An Act to Amend the Automotive Repair Statute, 1227, An Act to Repeal the Requirements That Motor Vehicle Manufacturers Equip Vehicles with a Standardized Data Access Platform, 1228, An Act to Clarify Certain Terms in the Automotive Right to Repair Laws, 1394, An Act to Support Maine's Electric Vehicle Adoption Goals by Providing an Exclusion for Electric Vehicles from Certain Requirements of the Right to Repair Law, 1467, An Act to Ensure Accountability for Repairs Conducted by Independent Repair Facilities on Motor Vehicles Under Warranty, and 1468, An Act to Establish Standards for Independent Motor Vehicle Repair Facilities in Maine. In short, the HED Committee is working on its own set of privacy and cyber security rules and obligations, which will apply to dealers, to protect consumers in the context of the repair of motor vehicles and access to privacy protected information which are part of a telematic system.

Given the broad nature of auto dealer obligations arising out of disclosures, consumer privacy, protected consumer and cyber security data under several federal and Maine laws, it is appropriate to exempt the Maine automobile dealers from the provisions of the bills under consideration by the Committee. Adding additional obligations can only create confusion, notification requirements and obligations that may be inconsistent and will not further the goals of the various bills before the Committee.

Respectfully submitted,

Bruce C. Gerrity

PRETI FLAHERTY

May 7, 2025
Page 3

BCG:mlb



May 2, 2025

Chairs Anne Carney, Amy D. Kuhn, and Members of the Committee
Joint Committee on Judiciary
Maine Legislature

RE: Bill Nos. LD 1088 | LD 1224 | LD 1822

Dear Chairs Carney, Kuhn, and Members of the Committee:

Headquartered in Oak Brook, Illinois, and with a 113-year history, the National Insurance Crime Bureau (NICB) is the nation's premier not-for-profit organization exclusively dedicated to leading a united effort to prevent insurance crime and fraud through intelligence-driven operations. NICB's 400-plus employees sit at the intersection between the insurance industry and law enforcement. NICB maintains operations in every state around the country, including in Maine where NICB is a longstanding, trusted partner in the fight against insurance fraud. NICB analysts and agents work daily with federal, state and local Maine law enforcement and regulatory agencies to provide assistance in all manner of cases, including the Maine State Police and Maine Bureau of Motor Vehicles.

Maine's Insurance Crime Reporting Requirements

Recognizing the adverse impact of insurance crime on the citizens of Maine, the legislature enacted laws requiring Maine insurers to report suspected insurance fraud to the Bureau of Insurance.ⁱ In the vast majority of cases, insurers submit suspected fraud referrals to the BOI through NICB's Fraud Bureau Reporting Program (FBRP). The FBRP connects through the National Association of Insurance Commissioners' Online Fraud Reporting System to deliver fraud reporting information to regulators. In addition to mandating that information be provided to the State, the Maine State Legislature also recognized the importance of reporting insurance crime and fraud information to law enforcement by enacting a statute providing civil immunity to any person and insurance professionals delivering such information to law enforcement and regulatory agencies in Maine.ⁱⁱ

Maine's Insurance Information and Privacy Protection Act

The Insurance Information and Privacy Protection Act was enacted to provide rules and regulatory oversight for insurance companies, agents, and insurance-support organizations, such as NICB, with regard to handling the personal information of policyholders. That law also provided a specific carve-out for certain disclosures, including those made for purposes of detecting or preventing criminal activity or fraud, reporting to a regulatory agency, or reporting to law enforcement.ⁱⁱⁱ By enacting this statute, Maine has addressed and preserved privacy interests for consumers in the insurance realm; and recognized the need for the free flow of information relating to fraud.

Impact of the Various Consumer Data Privacy Bills on NICB

NICB's anti-fraud efforts currently benefit from exemptions from the 16 enacted comprehensive consumer data privacy laws across the country, ensuring that NICB's limited resources as a non-profit remain directed at our fraud-fighting mission—a public benefit we provide to Maine residents at no cost. Limited exceptions for preventing, detecting, and protecting against fraud and illegal activity would not provide a wholesale exemption for such activities. Such limited exceptions would subject NICB to complex compliance obligations that would interfere with our vital information-sharing role and fraud-fighting mission. The policy reasons for excluding NICB from these burdens are several-fold. First, NICB provides a significant public benefit to the government and the millions of consumers who are victims of insurance fraud. Second, as a non-profit organization that serves a public interest, NICB is not equally situated with private entities that typically establish more complex compliance infrastructure for private-sector-related obligations. Third, NICB would become subject to consumer requests to, for example, confirm the existence of (or to delete) data. Even for non-viable requests, NICB would nevertheless bear the burden of proving to each consumer directly, or in litigation, that NICB's activities fall within the limitation. The obligation to do so would strain our organization's resources to such a degree that our operations, and ability to protect Maine consumers, would be significantly encumbered. Lastly, NICB's required responses to individual consumer requests would likely expose otherwise covert criminal investigations. For example, a fraudster could demand that NICB confirm we are processing that individual's data. A mere response from NICB tying that information to a fraud-related purpose would provide a clear signal to that individual, thereby exposing an investigation.

NICB's Request and Policy Rationale

Imposing what is essentially a “compliance, response, reporting and litigation” obligation – without any benefit to consumers – is inconsistent with Maine's insurance fraud reporting requirements and civil immunity provisions. These were enacted to facilitate, not impede, the mandatory flow of insurance fraud information to state authorities. Consistent with longstanding public policy determinations providing for the protection and flow of insurance fraud reporting information already considered and enacted in Maine law, NICB respectfully requests an entity-level exemption from the various bills.

Thank you for considering our views. As always, please consider NICB a resource and partner in the fight against insurance crime. If you have any questions or need additional information, please contact me at hhandler@nicb.org or 312-771-3974.

Sincerely,



Howard Handler, Senior Director
Strategy, Policy and Government Affairs

ⁱ 24-A M.R.S. § 2186

ⁱⁱ 24-A M.R.S. § 2187

ⁱⁱⁱ 24-A M.R.S. § 2215



Post Office Box 587
Augusta, ME 04332-0587

t: 207.622.7524

f: 207.622.0836

Testimony in support:

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

Testimony in opposition:

LD 1088, "An Act to Enact the Maine Consumer Data Privacy Act"

LD 1224, "An Act to Comprehensively Protect Consumer Privacy" and

LD 1284, "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 members of the Joint Standing Committee on Judiciary, my name is Laura Harper. I'm a senior associate at Moose Ridge Associates and I live in Hallowell. I am here today on behalf of my client, Maine Family Planning (MFP) to speak in support of LD 1822, "An Act to Enact the Maine Online Data Privacy Act" and against LD 1088, "An Act to Enact the Maine Consumer Data Privacy Act," LD 1224, "An Act to Comprehensively Protect Consumer Privacy" and LD 1284, "An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information."

MFP provides comprehensive sexual and reproductive health care to teens and adults at 19 locations statewide. Our mission is to ensure that all people have access to high-quality, culturally relevant and affordable sexual and reproductive health care services, comprehensive sexual health education, and the right to control their sexual and reproductive lives. One of the cornerstones to maintaining this access is protecting our patients' privacy, including their electronic data.

One doesn't need to look far to discover the latest attack on people's reproductive privacy. Most recently, our health centers have been under the threat of a Federal investigation for supposed civil rights violations inextricably connected to our mission to provide unbiased, evidence-based care to every patient who seeks our services, regardless of their immigration status, gender identity, race, or sexual orientation. This unproven Federal allegation has served as a groundless pretext for the Federal authorities to freeze our Title X funding, a long-standing investment in public health and family planning services by the U.S. government. Now more than ever, we need Maine law to provide the most comprehensive protection for our providers and patients. LD 1822 provides important tools so that our doors remain open and patients can access the life saving healthcare we've provided for over 50 years, free of government intrusions and/or corporate surveillance.

For example, some of our patients find menstrual cycle apps helpful to monitor their menstruation. These apps collect deeply personal, sensitive data on when a person has their period, when they are ovulating, if and when they may experience pre-menstrual syndrome and other information. Most consumers assume that this data is kept private and covered under HIPPA protections; instead they are at the whim of the privacy policies set by the app vendors. Without the protections in LD 1822, our patients fear their menstrual data and information regarding pregnancy and abortion care could be sold. We hear from our patients that many are already afraid to use these apps for fear of legal action in states where abortion and other sexual and reproductive health care is banned. LD 1822 will help to strengthen Maine's Shield Law, ensuring that all people can safely access abortion care here in Maine without fear. This bill would also help to eliminate fears of being geolocated while accessing lifesaving healthcare. In short, more data privacy equals better access to healthcare.¹

Of the four bills before you, LD 1822 is the only one that categorically prohibits collection of personal data. In contrast, LDs 1088 and 1224 would allow collection of sensitive data as long as the consumer clicks "I agree."² Most of us click "I agree" without a second thought, so these bills would not provide any meaningful protections for a majority of Maine people.

For these reasons and more, we oppose LDs 1088, 1224, and 1284; these bills lack the consumer protections our patients and providers need to safely access sexual and reproductive health services while keeping their personal data private.

In closing, we ask you to please vote LD 1822, "ought to pass" and to oppose LDs 1088, 1224 and 1284. Thank you for your attention and I'm happy to try to answer any questions you may have.

¹ LD 1088 also contains an anti-geofencing provision, but its data minimization provision would allow any collection or use of data as long as it is disclosed in a privacy policy. See LD 1088, p. 10, lines 7-20.

² See LD 1088, p. 10-11; LD 1224, p. 10.



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.

May 5, 2025



**Testimony of J.R. Kenny, Maine Alliance of Boys & Girls Clubs
In regard to LD 1088, An Act to Enact the Maine Consumer Data Privacy Act,
LD 1224, An Act to Comprehensively Protect Consumer Privacy and,
LD 1822, An Act to Enact the Maine Online Data Privacy Act**

On behalf of the **Maine Alliance of Boys & Girls Clubs** and the more than **8,000 youth we serve annually at 18 Club sites across Maine**, we appreciate the intent behind **LD 1088, LD 1224, and LD 1822** to enhance consumer data privacy protections in our state. However, we respectfully request that the committee carefully consider the impact these bills may have on nonprofit organizations, including Maine's Boys & Girls Clubs, and provide tailored provisions or exemptions to address our unique operational model and mission.

Boys & Girls Clubs operate within a federated model. Each Club is an independent 501(c)(3) organization, governed by its own board of directors, responsible for its own fundraising, and utilizing resources provided by **Boys & Girls Clubs of America (BGCA)** — including staff training, program curricula, strategic planning support, and data analysis tools. Like other nonprofit service providers, Boys & Girls Clubs collect limited personal information about youth members, families, staff, volunteers, and donors, and always with consent, solely for program delivery, safety, and reporting requirements to funders or for internal evaluation to improve services.

We have several concerns regarding the proposed legislation as currently drafted — specifically around compliance costs, data-sharing provisions, and applicability thresholds for nonprofit organizations. Every dollar that a youth-serving nonprofit like ours must devote to regulatory compliance is a dollar that cannot go toward feeding a child after school, providing academic support, or creating safe spaces for Maine kids during critical out-of-school hours. In other states where similar laws have passed, Boys & Girls Clubs have spent as much as **\$40,000 on legal and consultant fees** to navigate new requirements — a significant strain on already limited nonprofit resources.

Further, because of our **federated structure**, our local Clubs and BGCA would likely be classified as “third parties” under these bills, which could place burdensome restrictions on essential, mission-driven data sharing within our network. This limited, safeguarded sharing of de-identified or aggregated data between local Clubs and our national organization is critical for identifying statewide and national trends, securing grant funding, and continuously improving outcomes for the youth we serve.

Lastly, we note that **nonprofit organizations have historically been excluded from FTC consumer protection enforcement and exempt from most state consumer privacy laws**, given that nonprofits typically do not engage in commercial activity or data monetization. Nonprofits like ours collect only the data necessary to serve our mission and already adhere to strong ethical standards for safeguarding sensitive information.

In closing, the Maine Alliance of Boys & Girls Clubs respectfully requests that the committee:

1. **Increase the applicability threshold for nonprofits** to align with other state laws and recognize operational scale — for example, raising the threshold to **100,000 consumers annually**.
2. **Push back enactment dates** for nonprofit organizations to allow time for compliance planning and cost management.
3. **Provide clear guidance and exemptions for nonprofit organizations**, especially those that operate under federated models like ours, to avoid unintended limitations on internal, mission-critical data sharing.

We strongly support efforts to protect the privacy of Maine families — including the thousands of youth and families we serve each year — and believe that thoughtful adjustments to these bills can achieve that goal while safeguarding the ability of nonprofit organizations to continue serving their communities effectively.

Thank you for your time and consideration.

J.R. Kenny
Lead Director, Government Relations
Maine Alliance of Boys & Girls Clubs
Boys & Girls Clubs of America
770-596-1183
jrkenny@bgca.org



Senator Carney, Representative Kuhn, and esteemed members of the Joint Standing Committee on the Judiciary, my name is Lisa Margulies, I serve as Vice President of Public Affairs, Maine, for Planned Parenthood of Northern New England, and I am here today to submit testimony in support of LD 1822 and in opposition to LDs 1088, 1224, and 1284.

Planned Parenthood of Northern New England provides comprehensive reproductive and sexual health care in approximately 10,000 visits per year in Maine at four health centers located in Biddeford, Portland, Sanford, and Topsham, as well as online via telehealth. People turn to us for affordable, high-quality care including wellness exams, birth control, disease testing and treatment, cancer screenings, behavioral health care, abortion care, gender-affirming care, in addition to a variety of primary care services.

As a mission driven health care provider, we fundamentally believe everyone should be able to access affordable, high quality sexual and reproductive health care in their communities, no matter where they live or how much money they make, and we advocate for policies that help make this vision a reality. All people deserve to access comprehensive reproductive health care, including abortion and gender-affirming care, free from shame, stigma, and intimidation. We see everyone who comes to us regardless of ability to pay, and in a typical year, we provide more than \$1.2 million in free and discounted care to our communities in Maine. For many, we are their only access to the health care system.

Sensitive personal information, including reproductive health data, must be private. Ensuring privacy protections for and personal control over the collection and use of our own data is even more important as the breadth of information collected and inferred from our personal data grows. No one should fear that their sensitive data will be compromised or used against them.

Sadly, this information is already being weaponized to surveil and prosecute pregnant people, including those seeking abortions, and there are similar threats to trans and non-binary people seeking care along with their providers. In all these cases, people of color and people with low incomes are disproportionately impacted. Examples pre-date the repeal of Roe and include:

- Use of geolocation data to identify visitors to 140 abortion clinics in order to send those individuals ads for anti-abortion pregnancy counseling;ⁱ
- The sale of aggregated location data of people who visited abortion clinics, including more than 600 Planned Parenthoods over a one-week period for just \$160;ⁱⁱ
- The prosecution of a woman who experienced a pregnancy loss based on cell phone information after she searched online for medication abortion information;ⁱⁱⁱ
- Usage of geolocation data to charge a mother and son in Idaho with "abortion trafficking" for helping the son's girlfriend access abortion in Oregon;^{iv}



- Allegations that one of the most popular period tracking apps shared health information on its 100 million users with third-party data analytics firms, resulting in an FTC settlement.^v

Despite the widespread use of personal data, just 6% of adults report that they have a strong understanding of what companies do with the data they collect,^{vi} and the large majority of consumers (nearly 68%) are somewhat or very concerned about their online privacy.^{vii}

Planned Parenthood broadly supports policies that protect our individuals' right to privacy and control over their personal information. As states across the country ban access to abortion and gender-affirming care, Maine plays a critical role as a safe harbor for patients and their loved ones from throughout the country. Improving privacy protections for personal data is essential in safeguarding health care access.

LD 1284

Given our current national landscape, LD 1284 is, quite simply, a step in the wrong direction. By repealing Maine's current requirements that broadband Internet Service Providers protect customers' personal data and removing the prohibition on the sale of customer data without explicit consent, this bill actively worsens Maine's current data privacy protections at a time when they are increasingly needed.

LDs 1088, 1224, and 1822

Planned Parenthood of Northern New England supports the legislature's interest in increasing data protections in the state. While LDs 1088 and 1224 are laudable attempts to protect the data of Maine's citizens, we feel that the protections offered by these bills fall short of the demands of the present moment.

By contrast, LD 1822 by represents a broader and more robust approach to consumer protection, with specific protections for our patients, staff, and volunteers, by:

- Prohibiting sale of sensitive data, which is defined more broadly than in either LDs 1088 or 1224 and includes consumer health data (not included in LD 1224) and gender identity (not included in LDs 1088 or 1224);
- Requiring specific protections for "consumer health data" (not included in LD 1224), defined as personal data used to identify a consumer's physical or mental health status, and explicitly naming and including data related to gender-affirming health care services and reproductive health care services (not included in either LDs 1088 or 1224);
- Prohibiting geofencing a clinic offering in-person health services for purposes of identifying or collecting data or to send a notification to a consumer regarding consumer health data (not included in 1224);

- Allowing consumers to obtain a list of any third-party sales of their data (not included in LDs 1088 or 1224);
- Applying to a broader range of entities than LD 1088 or 1224, with both containing the same higher threshold for applicability (on the order of thousands of users);
- Authorizing enforcement action by the Attorney General, allowing the notice and the right to cure the violation if it is possible to cure, versus less discretion for enforcement under LD 1224, which requires notice and right to cure, and LD 1088, which requires notice and an opportunity to confer unless there is a showing of irreparable harm to consumers.

We believe that LD 1822's comprehensive approach is the right one, with such protections necessary given the extraordinary level of hostility facing reproductive and gender-affirming health care patients and providers.

Data has been referred to as the oil of the digital era^{viii} and as with oil in past centuries this modern commodity is ripe for exploitation, with extraordinary potential for misuse and harm. Following the example of other states such as Oregon and Maryland, we urge the legislature to pass a comprehensive data protection law that will safeguard the rights of all Mainers, enabling them to determine how their own personal information will be utilized by those who may exploit it.

We ask that the committee vote Ought to Pass on LD 1822 and Ought not to Pass on LDs 1088, 1224 and 1284. Thank you for your efforts to protect Mainers' privacy and ensure that no one fears harassment, investigation, or prosecution for seeking, providing, or assisting another in accessing health care.

ⁱ Coutts, Sharona; "Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits"; *Rewire News Group*; May 25, 2016; <https://rewirenewsgroup.com/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/>

ⁱⁱ Cox, Joseph; "Data Broker is Selling Location Data of People Who Visit Abortion Clinics"; *Vice News*; May 3, 2022; <https://www.vice.com/en/article/location-data-abortion-clinics-safegraph-planned-parenthood/>

ⁱⁱⁱ Rankin, Lauren; "How an online search for abortion pills landed this woman in jail"; *Fast Company*; February 26, 2020; <https://www.fastcompany.com/90468030/how-an-online-search-for-abortion-pills-landed-this-woman-in-jail>

^{iv} Frye, Jocelyn, Reeve Givens, Alexandra; "Digital Surveillance Supercharges Abortion Criminalization. Closing the Data Broker Loophole Is Urgent"; *National Partnership for Women & Families*; September 9, 2024; <https://nationalpartnership.org/digital-surveillance-supercharges-abortion-criminalization-closing-data-broker-loophole-urgent/>

^v "FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google and Others"; *Federal Trade Commission: Press Releases*; June 22, 2021; <https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google>

^{vi} Auxner, Brooke, Rainie, Lee, Anderson, Monica, Perrin, Andrew, Kumar, Madhu, Turner, Erica; "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information"; *Pew Research Center*; November 15, 2019; <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>

^{vii} Fazlioglu, Müge; "Privacy and Consumer Trust"; *International Association of Privacy Professionals*; March 2023; https://iapp.org/media/pdf/resource_center/privacy_and_consumer_trust_report_summary.pdf

^{viii} "The world's most valuable resource is no longer oil, but data"; *The Economist*; May 6, 2017; <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>



Testimony in Support of
LD 1822, An Act to Enact the Maine Online Data Privacy Act, and

in Opposition to
LD 1224, An Act to Comprehensively Protect Consumer Privacy,
LD 1088, An Act to Enact the Maine Consumer Data Privacy Act, and
LD 1284, An Act to Repeal Provisions of Law Governing the Privacy of
Broadband Internet Customer Personal Information.

Eric Null, Co-Director, Privacy & Data Program
Center for Democracy & Technology
Washington, DC

Before the Maine State Legislature
Hearing of the Judiciary Committee
Monday, May 5, 2025

Members of the committee, thank you for allowing me to provide feedback in support of LD 1822, An Act to Enact the Maine Online Data Privacy Act, and in opposition to three other privacy bills: LD 1224, LD 1088, and LD 1284.

My name is Eric Nul, I am the co-director of the privacy & data program at the Center for Democracy & Technology, a thirty-year-old nonpartisan, nonprofit organization focusing on protecting individual rights, civil rights, and civil liberties in the digital age.

In this testimony, I will first focus on why CDT supports LD 1822, specifically because it moves us beyond the notice-and-consent regime to a true data minimization regime. Then, I will discuss a few ways it could still be improved. Last, I will discuss why Maine should not pass the three other privacy bills you are considering today, including repeal of its broadband privacy law.

One of the primary goals of privacy legislation should be to move beyond the failed notice-and-consent regime, which has been dominant since the 1990s, has allowed a free-for-all on data collection and processing, and ultimately places the burden of reviewing privacy policies and protecting privacy on already-overburdened individuals. We know people do not view privacy policies as effective or useful.¹ We know people do not read privacy policies.² And we know that reading privacy policies, even if people wanted to, would require hundreds of hours per year.³ As a result, people have a sense of futility in privacy and feel a lack of control over privacy risks, and they often underestimate the risks of disclosing data.⁴

Data minimization, on the other hand, shifts the primary privacy burden to the companies who benefit most from the collection and exploitation of data by requiring them to justify their data practices as necessary to provide their products or services, or

¹ Sixty-one percent of adults consider privacy policies to be an ineffective way for companies to explain data practices, and almost seventy percent consider privacy policies to be just something to “get past.” Colleen McClain *et al*, *How Americans View Data Privacy*, Pew Research Center (2023), <https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy>.

² Fifty-six percent of American adults say they agree to privacy policies without reading them, compared to only eighteen percent who say they rarely or never agree without reading. *Id.*

³ A 2008 study estimated that people would spend 244 hours per year, or forty minutes a day, reading privacy policies if they read all policies that apply to them. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, *I/S: A Journal of Law and Policy for the Information Society* 540, 560 (2008), https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Final1.pdf. Privacy policies have only gotten longer since. Ryan Amos *et al*, *Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset*, In *Proceedings of the Web Conference* (2021), <https://arxiv.org/pdf/2008.09159>.

⁴ Wenjun Wang *et al.*, *An Exploration of the Influencing Factors of Privacy Fatigue Among Mobile Social Media Users From the Configuration Perspective*, *Scientific Reports* (2025), <https://www.nature.com/articles/s41598-024-84646-z>.

as fitting into another permissible purpose.⁵ It also helps prevent privacy harms at the outset because data a company does not have cannot lead to downstream harm through misuse, unauthorized access, disclosure to third parties including law enforcement, or some other harmful action. Data minimization has bipartisan support: a recent Consumer Reports survey found that seventy-two percent of Republicans and seventy-nine percent of Democrats “support a law that limits companies to using only the data they need to provide their service.”⁶

LD 1822 includes strong data minimization provisions by limiting collection of non-sensitive data to that which is reasonably necessary to provide a product or service,⁷ and by limiting collection, processing, and sharing of sensitive data to that which is strictly necessary to provide a product or service.⁸ These requirements help prevent boundless data collection practices, and they help avoid further saddling consumers with the burden of consenting to every data practice engaged in by every company they interact with. Similar requirements have already passed in Maryland, where they will come into effect in October 2025.

Two other Maine bills, LD 1224 and LD 1088, would change very little about privacy practices. The requirement in those bills for “data minimization,” if you can call it that, is weak. For non-sensitive data, companies can collect data reasonably necessary to any disclosed purpose—in other words, anything in the lengthy privacy policies that people don’t read. That is already a restatement of deceptive trade practices law,⁹ and is actually weaker, because the latter’s limits apply to all data practices (use, disclosure) as well as collection. For sensitive data, the only limits are on processing: companies can process sensitive data only with opt-in consent. While opt-in consent for processing sensitive data may be better than nothing, it is not better than the minimization provisions in LD 1822. Overall, these requirements are not privacy *protections* as much as privacy *burdens*, shouldered again by the consumer.

There is, of course, room for improvement in LD 1822. First, the minimization protections for non-sensitive data apply only to collection, but they should also apply to processing and sharing. If the limits do not apply to those practices, a company may be

⁵ Eric Null, *States Are Letting Us Down on Privacy*, Center for Democracy & Tech. (Jan. 28, 2024), <https://cdt.org/insights/states-are-letting-us-down-on-privacy>.

⁶ Scott Medintz, *Americans Want Much More Online Privacy Protection Than They’re Getting*, Consumer Reports (Nov. 20, 2024), <https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306>.

⁷ §9608(2)(A).

⁸ §9608(1)(A).

⁹ *See generally*, FTC Statement on Deception, FTC (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

limited in its initial collection of data, but it would generally be free to process or share non-sensitive data for any purpose unrelated to the product or service.

Second, the knowledge standard is not properly calibrated. CDT has historically been concerned with language surrounding “knowing” the age of internet users because of the potential for that language to incentivize or even force companies to institute privacy-invasive age-assurance and age-verification techniques.¹⁰ LD 1822 applies additional protections to users a company knows or “reasonably should know” a user is a minor. That standard is likely to *reduce* privacy and anonymity online, because companies may feel compelled to comply with those provisions by requiring all users to upload identifying documentation showing their age when normally that information would be kept private. We urge that the bill be amended to rely on a “knowledge fairly implied under objective circumstances” standard, as that standard is less likely to incentivize companies to adopt across-the-board age verification techniques.

Third, privacy laws are only as strong as their enforcement, and they should be enforced through multiple channels. LD 1822 includes Attorney General enforcement, but explicitly disallows the private right of action that already exists in Maine’s Unfair Trade Practices law, which is itself limited to actual damages and equitable relief. Without that private right of action, the bill would lead to perverse results: a Maine resident who finds themselves subject to identity theft, physical danger, harassment, or some other harm because of the data practices of a company may not be able to hold that company accountable under the privacy law. Attorney General enforcement is not sufficient to make that Maine resident whole.

If Maine insists on placing the entire enforcement burden on the Attorney General’s office, it should at least ensure the office is appropriated enough funds to build a dedicated team, like in Texas.¹¹

Finally, CDT opposes LD 1284, the bill to repeal Maine’s broadband privacy law, particularly given LD 1822 includes a carve-out for broadband providers. Back in 2016, the Federal Communications Commission passed a nationwide rule protecting the

¹⁰ See Letter from CDT et al. to Majority Leader Schumer et al., Opposition to S. 3663’s Threats to Minors’ Privacy and Safety Online, Nov. 28, 2022, at 2 <https://cdt.org/wp-content/uploads/2022/11/Coalition-letter-opposing-Kids-Online-Safety-Act-28-Nov-PM.pdf> (“Service providers will thus face strong incentives to employ age verification techniques to distinguish adult from minor users, in order to apply these strict limits only to young people’s accounts. Age verification may require users to provide platforms with personally identifiable information such as date of birth and government-issued identification documents, which can threaten users’ privacy, including through the risk of data breaches, and chill their willingness to access sensitive information online because they cannot do so anonymously.”).

¹¹ Texas built a \$5 million privacy-specific enforcement team and they have been out ahead on enforcement efforts. Cobun Zweifel-Keegan, *A View from DC: the Price of Privacy Enforcement*, IAPP (Feb. 28, 2025), <https://iapp.org/news/a/a-view-from-dc-the-price-of-privacy-enforcement>.

privacy of broadband subscribers, a significant win for consumers. The rule was simple: broadband providers could use and disclose data for service-related purposes (or pursuant to other narrow exceptions), but other, non-service-related uses required consent from the subscriber.¹² That rule, despite its sensible and beneficial privacy protections, was unfortunately overturned in 2017 by Congress under the Congressional Review Act, which also prevents the agency from adopting “substantially similar” rules without Congressional approval.¹³ In the aftermath, Maine was the only state courageous enough to adopt a similar law (with a unanimous vote in the Senate and bipartisan support overall¹⁴) to protect Maine residents against the exploitation of data collected by broadband providers and used for marketing and other unrelated purposes. Those protections are purpose-built for broadband providers and make sense in that context. Maine should not repeal those protections.

¹² In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Dkt. No. 16-106, Report and Order, Oct. 27, 2016, <https://docs.fcc.gov/public/attachments/FCC-16-148A1.pdf> (App’x A).

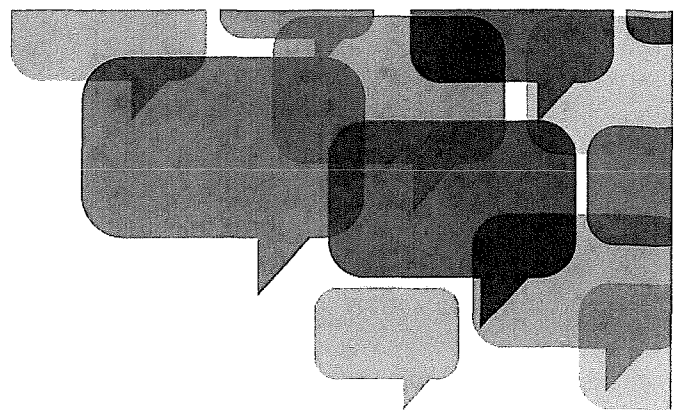
¹³ *Congress Has Repealed the FCC’s Privacy Rules – Now What?*, Cooley (Mar. 29, 2017), <https://www.cooley.com/news/insight/2017/2017-03-29-congress-repeals-fccs-privacy-rules>.

¹⁴ *Governor Mills Signs Internet Privacy Legislation*, State of Maine (June 6, 2019), <https://www.maine.gov/governor/mills/news/governor-mills-signs-internet-privacy-legislation-2019-06-06>



**RETAIL
ASSOCIATION OF
MAINE**
Voice of Maine Retail

45 Melville Street, Suite 1
Augusta, ME 04330
Phone: 207.623.1149
www.retailmaine.org



May 5, 2025

Senator Anne Carney, Chair
Representative Amy Kuhn, Chair
Members of the Judiciary Committee

RE: Testimony Regarding:

- **LD 1822 An Act to Enact the Maine Online Data Privacy Act**
- **LD 1224 An Act to Comprehensively Protect Consumer Privacy**
- **LD 1088 An Act to Enact the Maine Consumer Data Privacy Act**
- **LD 1284, An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information**

Dear Senator Carney, Representative Kuhn and members of the Judiciary Committee:

My name is Curtis Picard, and I serve as the President and CEO of the Retail Association of Maine. Our association represents retailers of all sizes from small, independent retailers, to a number of well-known Maine retail brands, and including a number of larger, multi-state retailers. Maine's retailers employ more than 80,000 Mainers, and our industry is one of the largest private sector employers in Maine.

Thank you for the opportunity to provide testimony regarding these comprehensive privacy proposals before you. We appreciate the Committee's attention to this important and complex issue, and we commend Representative Kuhn, Representative Roberts, Representative Henderson, and Senator Stewart for their commitment to protecting Maine consumers.

For the record, we are not taking a position on LD 1284. That is a narrowly focused bill related to the existing Maine ISP law.

Instead, we are focusing our testimony on LD 1224, LD 1088, and LD 1822. As veteran members of this committee know, the Retail Association of Maine, and our members, were actively involved during last year's discussion of comprehensive data privacy. I will say again what I said then – we support Maine passing comprehensive data privacy legislation. We are hopeful that this year we can reach consensus on legislation that does not put Maine businesses at a competitive disadvantage nor require a different level of compliance than other states. We are willing to work with the committee to hopefully find a path forward this year.

Moreover, this approach paradoxically removes consumer control. Instead of asking for the consumer's consent to collect sensitive data (as in LD 1224), the "strictly necessary" standard makes the judgment for them. It limits businesses from providing services that consumers may very much want—such as follow-up promotions or tailored product recommendations—even when the consumer is open to it.

Finally, enforcement under this standard becomes speculative. Regulators would be required to assess whether a business's judgment about what is "strictly necessary" is valid—a subjective and unprecise task—rather than simply reviewing a privacy notice for compliance, as they would under LD 1224.

Additionally, in the definition of Sensitive Data (Section 9602[34]): The inclusion of "billing, financial or payment method information" is vague and could be misinterpreted to include innocuous data such as purchase price or sales trends—key components of business analytics. We recommend Maine adopt the clearer definitions used in New Jersey and California. These definitions focus on financial information that, if disclosed, could grant access to a consumer's financial accounts, thereby safeguarding sensitive data without impeding standard business analytics practices.

Section 9608(2)(A): Limiting the Collection of Personal Data

This provision states that a business may only collect personal data if it is "reasonably necessary and proportionate" to provide or maintain a specific product or service requested by the consumer. As stated above, this is also language from the Maryland law which is not yet effective and therefore not yet tested.

This narrow requirement effectively bans personalized and targeted advertising, which is a vital tool for small businesses, nonprofits, and even political campaigns. These organizations rely on personalized outreach to find and serve the right audiences—without it, marketing efficiency drops and costs rise.

We appreciate that LD 1822 allows businesses to continue offering loyalty, rewards, and discount programs — a key benefit for Maine consumers, especially in the grocery and retail sectors. Consumers love loyalty and rewards programs. The average consumer is enrolled in nearly 17 different loyalty programs, and actively engages with 9 of them.

However, we are concerned that the current provision in Section 9608, Subsection 3(B), which prohibits the "sale of personal data as a condition of participation" in a loyalty program, may unintentionally restrict standard industry practices that are pro-consumer and privacy-protective.

Specifically, grocery stores and other retailers often partner with manufacturers or service providers to administer rewards. In many cases, limited customer data is shared with a supplier or processor **solely to fulfill the benefits of the loyalty program** — for example, applying a

collection, processing, and sale of data related to such individuals. While we strongly support efforts to protect younger users online—particularly young children—we are concerned that these provisions may unintentionally impair legitimate and responsible marketing practices directed at older teenagers, including those who are already participants in the economy as both consumers and workers.

Teenagers aged 15 to 17 are not only an important consumer demographic—they are also a meaningful part of the retail workforce. These young individuals make independent purchasing decisions, often with their own income, and engage with brands in the same way adults do. Applying restrictions to this entire group as if they are incapable of consumer autonomy overlooks their real-world behavior and may limit their access to relevant information about products, job opportunities, and services specifically intended for their age group. Retailers could find it legally risky or operationally unclear whether they can advertise back-to-school promotions, athletic gear, or teen-oriented brands to an audience that clearly wants and expects to receive them.

Furthermore, LD 1822 includes a provision that prohibits certain data practices when a controller *"knew or should have known"* that the consumer is a minor. This *"should have known"* standard is troubling. It imposes an ambiguous and highly subjective duty on businesses to assess a consumer's age, even when no age or birthdate has been collected. In many cases, especially in contexts where no account is created, it is neither practical nor possible to know—or infer—with certainty that a user is under 18. This could force businesses to take overly conservative approaches or to avoid certain kinds of content and interactions altogether, ultimately limiting access to lawful, age-appropriate services for older teens.

We recommend narrowing the application of these provisions to known children under 13, consistent with federal COPPA standards and other state frameworks, or at the very least clarifying that heightened obligations only apply when a business affirmatively knows the consumer is a minor. This would better balance the privacy rights of youth with their evolving roles as independent consumers and workers.

We also wish to express our general support for LD 1088, the Maine Consumer Data Privacy Act. This bill aligns closely with LD 1224 in its core structure and consumer protections, offering a familiar and workable framework for businesses. Notably, LD 1088 includes additional provisions that enhance consumer privacy, such as prohibiting geofencing near healthcare facilities and requiring data protection assessments for high-risk processing activities. These measures demonstrate a thoughtful approach to emerging privacy concerns and reinforce Maine's commitment to safeguarding personal data.

We appreciate the introduction of LD 1088 as part of the broader dialogue on data privacy. Its provisions contribute valuable perspectives to the conversation, and we encourage consideration of its elements in shaping comprehensive and balanced privacy legislation for Maine.

New Hampshire Data Privacy Act

On January 1, 2025, the New Hampshire Data Privacy Act (“NHDPA”), RSA 507-H, came into effect. This statute is the result of two bills, SB 255-FN and HB 1220-FN. Former Governor Chris Sununu signed SB 255-FN into law on March 6, 2024, and HB 1220-FN into law on July 19, 2024.

The following contains a summary of rights for New Hampshire consumers and a list of frequently asked questions for businesses. The information contained herein is not legal advice or an opinion from the Attorney General and should not be considered comprehensive. If consumers or businesses have questions regarding the requirements of RSA 507-H, they are encouraged to review [the statute](#) or speak with a private attorney.

If you would like to report a violation of the NHDPA, please fill out a Consumer Protection complaint form at [this link](#) or email CPB-DOJ@doj.nh.gov.

A business must provide a mechanism for you to revoke consent “that is at least as easy” as the mechanism by which you provided consent. Once the business receives your request to revoke consent, it must stop processing your data within 15 days.

How can New Hampshire consumers exercise their data privacy rights?

- You may exercise your rights by any secure and reliable means described to you in the business’ privacy notice. This notice must be clear, meaningful, and reasonably accessible.
- Businesses that control data must “clearly and conspicuously” disclose how to opt out of data sales and targeted advertising. Such businesses must also provide a “clear and conspicuous” link on their website to a webpage that enables you or your agent to opt out of targeted advertising and sales of your personal data.
- You may designate an agent to exercise your opt-out rights for you. You may also opt out of targeted advertising and data sales through an opt-out preference signal or global device setting.
- A parent or legal guardian may exercise consumer rights on their child’s behalf. For consumers subject to a guardianship, conservatorship, or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer’s behalf.

The attorney general has exclusive authority to enforce NHDPA violations. **If you believe the NHDPA has been violated, please submit a complaint to the New Hampshire Attorney General.** Fill out a Consumer Protection complaint form at [this link](#) or email CPB-DOJ@doj.nh.gov.

What are some issues that New Hampshire consumers might encounter while trying to exercise their rights?

- Certain businesses and types of information are exempted from the NHDPA (See Below FAQs for a list of exempt businesses).
- A business which controls data can deny your rights request if it is unable to authenticate a rights request. If this happens, the business must provide you notice that it is unable to authenticate the request until you provide additional information reasonably necessary to authenticate the request. A business cannot require you to create a new account to exercise your rights.
- A business which controls data may deny an opt-out request if it has a good faith, reasonable and documented belief that your request is fraudulent. If this occurs after you try to exercise your opt-out rights, the business must send you a notice explaining that it

Frequently Asked Questions for Businesses

When did the NHDPA take effect?

RSA 507-H took effect on **January 1, 2025**.

What does the NHDPA do?

The NHDPA gives New Hampshire residents certain rights over their personal data and establishes responsibilities and privacy protection standards for entities which handle personal data (data controllers and processors).

What is “Personal Data?”

“Personal Data” is any information that is linked or reasonably linkable to an identified or identifiable individual. “Personal data” does not include de-identified data or publicly available information. RSA 507-H:1, XIX.

What rights can New Hampshire residents exercise under the NHDPA?

New Hampshire consumers have the following rights:

- **Confirm** whether or not a controller is **processing** the consumer’s personal data;
- **Access** the consumer’s personal data;
- **Correct inaccuracies** in the consumer’s personal data;
- **Delete** personal data provided by, or obtained about, the consumer;
- **Obtain a copy** of the consumer’s personal data processed by the controller; and
- **Opt-out of the processing of the personal data for purposes of targeted advertising, the sale of personal data, except as provided in RSA 507-H:6, or profiling** in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

RSA 507-H:4, I.

- Mental or physical health condition or diagnosis;
- Sex life or sexual orientation;
- Citizenship or immigration status;
- The processing of genetic or biometric data for the purpose of uniquely identifying an individual;
- Personal data collected from a known child; or
- Precise geolocation data.

RSA 507-H:1, XXVIII.

What are the NHDPA requirements for processing “Sensitive Data”?

“Sensitive Data” is subject to additional restrictions under RSA 507-H. For example,

- Controllers may not process sensitive data concerning a consumer without obtaining the consumer’s consent,
- Controllers may not process sensitive data concerning a known child without processing such data in accordance with COPPA, and
- Controllers must conduct and document a data protection assessment for each of the controller’s processing activities that include processing sensitive data.

RSA 507-H:6, I (d), RSA 507-H:8, I.

Who is exempt from complying with the NHDPA?

The following entities are exempt from the NHDPA:

- Any State of New Hampshire body, authority, board, bureau, commission, district or agency or any political subdivision thereof;
- Any nonprofit organization;
- Any institution of higher education;
- Any national securities association that is registered under 15 U.S.C. section 78o-3 of the Securities Exchange Act of 1934;

- The protection of human subjects under 21 C.F.R. Parts 6, 50, and 56, or personal data used or shared in research, as defined in 45 C.F.R. 164.501, that is conducted in accordance with the standards set forth in this chapter, or other research conducted in accordance with applicable law; RSA 507-H:3, II (e);

Certain Information and Data Regarding Professional Review Activities

- Information and documents created for purposes of the Health Care Quality Improvement Act of 1986, 42 U.S.C. 11101 et seq.; RSA 507-H:3, II (f);
- Patient safety work product for purposes of the Patient Safety and Quality Improvement Act, 42 U.S.C. 299b-21 et seq., as amended; RSA 507-H:3, II (g);

Certain Information about Applicants, Employees, Agents, or Independent Contractors

- Data processed or maintained in the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or third party, to the extent that the data is collected and used within the context of that role; as the emergency contact information of an individual under this chapter used for emergency contact purposes; or, that is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under HIPPA and used for the purposes of administering such benefits; RSA 507-H:3, II (o);

Certain Information and Data Subject to Other Federal Laws

- The collection, maintenance, disclosure, sale, communication or use of any personal information bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.; RSA 507-H:3, II (k);
- Personal data collected, processed, sold or disclosed in compliance with the Driver's Privacy Protection Act of 1994, 18 U.S.C. 2721 et seq., as amended; RSA 507-H:3, II (l);
- Personal data regulated by the Family Educational Rights and Privacy Act, 20 U.S.C. 1232g et seq., as amended; RSA 507-H:3, II (m);
- Personal data collected, processed, sold or disclosed in compliance with the Farm Credit Act, 12 U.S.C. 2001 et seq., as amended; RSA 507-H:3, II (n);
- Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the Airline Deregulation Act, 49 U.S.C. 40101 et seq., as amended, by an air carrier subject to the act, to the extent this chapter is preempted by the Airline Deregulation Act, 49 U.S.C. 41713, as amended; RSA 507-H:3, II (p);

Can a consumer opt-out of the sale of personal data to third parties?

Yes, a consumer can opt-out of the sale of personal data to third parties. The controller must provide a process for submitting an opt-out request. A consumer can also designate a third party to opt-out on his or her behalf and can use an opt-out preference signal.

Can a controller deny a consumer rights request?

Yes, under certain circumstances.

If a controller is unable to authenticate a request to exercise any of the rights afforded under RSA 507-H:4, I(a)-(d) using commercially reasonable efforts, the controller shall not be required to comply with a request to initiate the requested action. The controller must provide notice to the consumer that the controller is unable to authenticate the request until the consumer provides additional information reasonably necessary to authenticate the request. RSA 507-H:4, III (d).

A controller may deny an opt-out request if the controller has a good faith, reasonable and documented belief that the request is fraudulent. If a controller denies an opt-out request because the controller believes it is fraudulent, the controller must send a notice to the person who made the request explaining that the controller believes the request is fraudulent, why the controller believes it is fraudulent and that the controller will not comply with a fraudulent request. RSA 507-H:4, III (d).

If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than 45 days after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision. RSA 507-H:4, III (b).

Does a consumer have a right to appeal a denial?

Yes.

A controller shall establish a process for a consumer to appeal the controller's refusal to take action on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process shall be conspicuously available and similar to the process for submitting requests. A controller has 60 days after receiving the appeal to inform the consumer in writing of any action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the attorney general to submit a complaint.

RSA 507-H:4, IV.

- The date the privacy notice was last updated. RSA 507-H:6, III (g).

Controllers must also clearly and conspicuously disclose the following:

- All personal data sales and targeted advertising. RSA 507-H:6, IV.
- How a consumer may opt out of data sales and targeted advertising. RSA 507-H:6, IV.
- A link on the controller's website to a targeted advertising and data sales opt-out webpage. RSA 507-H:6, V (a)(1)(A).

When must a controller seek consent before processing data?

- A controller must only process a consumer's data outside of the controller's disclosed purposes of collection if the consumer consents. RSA 507-H:6, I (b).
- A controller must only process sensitive data of a consumer if the consumer consents. RSA 507-H:6, I (d).
- A controller must allow consumer to revoke consent easily and stop processing within 15 days of consumer's revocation. RSA 507-H:6, I (f).

When must a controller conduct a data protection assessment?

If a controller processes data or causes data to be processed after July 1, 2024, that controller must conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer.

Processing that presents a heightened risk of harm to a consumer includes:

- The processing of personal data for the purposes of **targeted advertising**, RSA 507-H:8, I (a);
- The **sale** of personal data, RSA 507-H:8, I (b);
- The processing of personal data for the purposes of certain types of **profiling**, RSA 507-H:8, I (c); and
- The processing of **sensitive data**. RSA 507-H:8, I (d).

- Instructions for processing data,
- The nature and purpose of processing,
- The type of data subject to processing,
- The duration of processing, and
- The rights and obligations of both parties. RSA 507-H:7, II.

The controller-processor contract must also require that the processor:

- Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data, RSA 507-H:7, II(a);
- At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law, RSA 507-H:7, II(b);
- Upon the reasonable request of the controller, make available to the controller all information in its possession necessary to demonstrate the processor's compliance with the obligations in this chapter, RSA 507-H:7, II(c);
- After providing the controller an opportunity to object, engage any subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data, RSA 507-H:7, II(d); and
- Allow, and cooperate with, reasonable assessments by the controller or the controller's designated assessor, or the processor may arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations under this law, using an appropriate and accepted control standard or framework and assessment procedure for such assessments. The processor shall provide a report of such assessment to the controller upon request. RSA 507-H:7, II(e).

Who can enforce the NHDPA?

The attorney general has exclusive authority to enforce NHDPA violations. RSA 507-H:11, I. The NHDPA does not provide for a private right of action. RSA 507-H:11, IV.

Is there a cure period?

Between January 1, 2025 and December 31, 2025

Prior to initiating an action for a violation of RSA 507-H, if the attorney general determines that a cure is possible, the attorney general will issue a notice of violation to a controller. If the



PO Box 7860
Portland, ME 04112

(207) 774-5444
ACLUMaine.org
@ACLUMaine

TESTIMONY OF ALICIA REA, 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 Alicia Rea and I am a policy fellow 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.

Privacy and Bodily Autonomy

The rights to privacy and bodily autonomy are at the core of access to abortion and gender affirming health care. Throughout the country, our bodies have become battlegrounds on these fronts. Privacy and bodily autonomy connect several issues, from abortion and contraception to gender-affirming care and marriage equality. These are all linked by our foundational right to life, liberty and the pursuit of happiness. These rights and freedoms allow us to write our own stories, determine our own paths, and thrive on our terms.

Following the United States Supreme Court's opinion overturning *Roe v. Wade*, questions and fears about our digital privacy and the criminalization of healthcare have proliferated.¹ The criminalization of people seeking reproductive health care, and of doctors and nurses who seek to provide it, has expanded since this decision, with out-of-state actors seeking information about Maine patients and providers who engage in healthcare that is legal in this state. In the face of these attacks on reproductive healthcare and other care that is legal in Maine, our digital privacy matters even more today than it has in the past.

¹ *Dobbs v. Jackson Women's Health Organization*, 597 U.S. 215 (2022).

The lack of strong digital privacy protections has profound implications in the face of expanded criminalization of reproductive and gender affirming health care. The recent breathtaking and authoritarian attacks on bodily autonomy mean that we must fight with new urgency to ensure that people maintain control over their personal information. If we fail, the repressive surveillance techniques and powers that police and prosecutors have used to wage the ineffectual and damaging wars on drugs and terror will be marshaled to track, catalogue, and criminalize patients and those seeking basic information about health issues.

Laws that criminalize reproductive health and gender affirming care are already being used disproportionately by government actors to surveil, penalize, and control people, especially people of color. According to Pregnancy Justice, the past 15 years have seen a shocking spike in arrests and prosecutions for crimes related to stillbirths, miscarriages, and alleged drug and alcohol use during pregnancy.² Of the 1,792 people prosecuted for these offenses since 1980, 1,379 were charged after 2006, and those targeted were disproportionately Black and Indigenous women.³ And, just last year, U.S. Senator Ron Wyden, revealed that an anti-abortion political group used mobile phone location data to send targeted misinformation to people who visited any of 600 reproductive health clinics in 48 states.⁴

Prior to the *Dobbs* decision, a Texas district attorney and sheriff worked to indict and arrest a 26-year-old woman and charge her with murder, after the woman self-managed her abortion.⁵ In 2017, an online search for the abortion medication misoprostol was used to charge one woman with second-degree murder.⁶ In 2015, a series of text messages with a friend about getting an abortion helped convict another woman of feticide and child neglect.⁷

Expanded criminalization of healthcare has become increasingly common, which is why we must be prepared to digitally defend ourselves against

² Pregnancy Justice, *The Rise of Pregnancy Criminalization*, Sep. 2023, available at <https://www.pregnancyjusticeus.org/wp-content/uploads/2023/09/9-2023-Criminalization-report.pdf>.

³ *Id.*

⁴ Letter from U.S. Senator Ron Wyden to FTC Chair Lina Khan and SEC Chair Gary Gensler (Feb. 13, 2024), available at https://www.wyden.senate.gov/imo/media/doc/signed_near_letter_to_ftc_and_sec.pdf.

⁵ Nicole Narea, *Why was a Texas woman charged with murder over an abortion?*, Vox, available at <https://www.vox.com/policy-and-politics/23021104/texas-abortion-murder-charge-starr-county>.

⁶ Cat Zakrzewski et al., *Texts, Web Searches About Abortion Have Been Used to Prosecute Women*, The Washington Post (July 2022), available at <https://www.washingtonpost.com/technology/2022/07/03/abortion-data-privacy-prosecution/>.

⁷ Emily Bazelon, *Purvi Patel Could Be Just the Beginning*, New York Times (Apr. 2015), available at <https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html>.

corporate and government surveillance. We must take real action to protect our digital privacy, in the face of attempts to invade Maine's current legal protections.

Over the past 20 years, digital technologies have rapidly advanced, changing the way we communicate, seek and share information, travel, work, play, document and track our own health metrics, find love, and more. Billion-dollar industries have taken shape that work behind the scenes and without consent to create, share, trade, and sell extremely sensitive data about hundreds of millions of people, buoyed by leaps in computing power and the declining cost of data storage.

The Government can gain access to this corporate surveillance in what some have called a "public-private surveillance partnership." In many cases, government actors can obtain extremely detailed information from corporations about people's finances, internet use, and communications without ever going to a judge, and without a shred of evidence that someone is involved in criminal activity. When cops are armed with court orders, virtually none of the information collected and processed in what has been called the "surveillance capitalist" marketplace is off limits to the government. And even for types of personal information that courts have said police can only force companies to turn over with a warrant—like cell phone location data—government agencies are sidestepping the warrant requirement by paying to access sensitive information instead of going to a judge. The Fourth Amendment should not be for sale, yet our inadvertent transfer of our sensitive data to private companies means there can be no expectation of privacy in the data collected, stored, and sold.

A lack of local-related data privacy can also have serious implications for one's livelihood. In 2001, "[t]he top administrator of the U.S. Conference of Catholic Bishops resigned after a Catholic media site told the conference it had access to cellphone data that appeared to show he was a regular user of Grindr, the queer dating app, and frequented gay bars."⁸

In response to these profound transformations, civil rights advocates have championed consumer privacy protections to give people control over their personal information. In Illinois, such protections limit what kinds of information companies can collect and the ways they can share and use these

⁸ Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021), <https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-bumill/>.

data.⁹ In Virginia, the state legislature passed a law that prohibits the collection, use, or sharing of reproductive or sexual health information without consent and provides Virginians with a private right of action for at least \$500 per violation..¹⁰

Legislatures must impose strict limitations on the use of invasive technologies and techniques, restricting surveillance warrants to only the most serious kinds of criminal investigations and excluding investigations related to sexual health and gender affirming care. Maine should seek to preserve access to healthcare for all Mainers by taking extreme care to protect information created or maintained in our jurisdiction from being disclosed to out-of-state officials investigating sexual health related matters. Technology companies should be required to change their internal policies and procedures to ensure that they collect and disclose minimal information from consumers and adopt notification procedures for when data could be sold, giving people a chance to fight back against surveillance aimed at their personal health information.

Of the bills before you today, only LD 1822 contains provisions that would end the needless collection of sensitive information like location and biometric data and outlaw the use of search word and geofencing warrants, which allow police to conduct dragnet-like surveillance.¹¹

The recent rollbacks of the right to privacy should serve as a reminder to us all that we should never accept living in a surveillance society, no matter what technology is used to carry it out. The right to privacy sits at the heart of democracy, and we must fight to ensure its relevance now and in the decades to come.

To facilitate strong consumer privacy protections, please vote ought to pass on LD 1822 and ought not to pass on LDs 1088, 1224, and 1284.

⁹ Biometric Information Privacy Act, 740 ILCS 14/1 et seq. (2008).

¹⁰ Ashton Harris et al., *Analyzing Virginia's New PRA for Protecting Consumer Reproductive and Sexual Health Information*, ByteBack, Apr. 24, 2025, available at <https://www.bytebacklaw.com/2025/04/analyzing-virginias-new-pra-for-protecting-consumer-reproductive-and-sexual-health-information/>.

¹¹ LD 1088 also contains an anti-geofencing provision, but its data minimization provision would allow any collection or use of data as long as it is disclosed in a privacy policy. *See* LD 1088, p. 10, lines 7-20.



May 5, 2025

Senator Anne Carney
3 State House Station
Augusta, Maine 04333
Anne.Carney@legislature.maine.gov

Representative Amy D. Kuhn
2 State House Station
Augusta, ME 04330
Amy.Kuhn@legislature.maine.gov

Representative Jennifer L. Poirier
2 State House Station
Augusta, ME 04330
Jennifer.Poirier@legislature.maine.gov

Re: Maine Consumer Data Privacy Act: H.P. 710, L.D. 1088, "An Act to Enact the Maine Consumer Data Privacy Act"; H.P. 799, L.D. 1224, "An Act to Comprehensively Protect Consumer Privacy"; H.P. 1220, L.D. 1822, "An Act to Enact the Maine Consumer Data Privacy Act."

Dear Chairpersons Carney and Kuhn, Ranking Member Poirier, and the other distinguished members of the Judiciary Committee:

National Futures Association (NFA) appreciates the opportunity to provide written testimony on the Maine Legislature's proposed data privacy bills, Bill H.P. 710, "An Act to Enact the Maine Consumer Data Privacy Act"; Bill H.P. 799, "An Act to Comprehensively Protect Consumer Privacy"; and Bill H.P. 1220, "An Act to Enact the Maine Consumer Data Privacy Act."

NFA generally supports increased privacy protections, but for the reasons discussed below, seeks a narrowly tailored exemption to enable it to continue performing its critical role in regulating derivatives markets and protecting investors.

NFA is a not-for-profit, registered futures association (RFA) under the Commodity Exchange Act.¹ NFA is the industrywide self-regulatory organization (SRO) for the derivatives industry, including futures, swaps, and retail off-exchange foreign currency (or forex). Every aspect of NFA's regulatory authority is overseen and monitored by the Commodity Futures Trading Commission (CFTC), the Congressionally authorized commodity derivatives regulator. NFA's responsibilities include registering firms and industry professionals on behalf of the CFTC,² passing rules to ensure fair dealing with customers, examining and investigating Members for compliance with those rules,

¹ See 7 U.S.C. § 21; 17 C.F.R. §§ 170.1 et seq.

² 17 CFR § 3.2(a) (stating that the registration functions of the CFTC shall be performed by NFA).

taking enforcement actions against those Members that violate NFA Rules, administering proficiency examinations for individuals engaged in derivatives activities, and providing a low-cost arbitration forum for members of the investing public to resolve their disputes with NFA Members.

In order for NFA to successfully carry out these regulatory functions, NFA must collect and process data. Importantly, NFA only uses the data it collects for regulatory purposes—data is not collected, shared, or sold for any commercial purpose.

NFA is concerned that the proposed legislation may interfere with NFA's efforts to safeguard financial markets and protect investors in Maine and throughout the nation. For example, the data NFA collects often includes financial account numbers, which H.P. 710 and H.P. 1220 would include in the definition of "sensitive data." However, because NFA regulates thousands of financial firms with millions of financial accounts, NFA cannot possibly obtain separate individual consents from accountholders before commencing a regulatory exam or investigation. Additionally, NFA must maintain the integrity of its investigative files and exam papers. Thus, NFA cannot typically disclose, modify or delete data upon the request of consumers.

Notably, the proposed bills already include exemptions for a closely analogous self-regulatory organization. All three proposed comprehensive data privacy bills under consideration by the Judiciary Committee today would provide a full exemption to the Financial Industry Regulatory Association (FINRA), which is a national securities association and the nationwide SRO for the securities markets. FINRA performs largely identical functions to NFA and is subject to similar federal supervision. While FINRA is the SRO for the nation's securities brokerage industry and operates under the comprehensive oversight of the SEC, NFA is the SRO for the nation's derivatives industry and operates under the comprehensive oversight of the CFTC.

Recognizing NFA and FINRA's analogous roles in safeguarding the financial markets, other states' comprehensive data privacy laws, such as the Delaware Personal Data Privacy Act and the Maryland Online Data Privacy Act of 2024, include entity-level exemptions both for registered futures associations and national securities associations, and do so in the same section.³

For these reasons, we respectfully request that the underlined language below be added to § 9603(3)(B) of the proposed Maine Consumer Data Privacy Act under H.P. 710 and 799, or to § 9604(1)(D) under H.P. 1220. Such language would not risk sweeping too broadly (as NFA is the nation's only RFA), would be consistent with other state comprehensive data privacy laws, and would ensure that NFA could continue to fulfill its role and responsibilities, which include protecting Maine investors.

³ See Del. Code Ann. tit. 6, § 12D-103(b)(4); Md. Code Ann., Com. Law § 14-4703(a)(2).

". . . Exempt entities . . .

A national securities association that is registered under the federal Securities Exchange Act of 1934, 15 United States Code, Section 78a et seq., or a registered futures association so designated pursuant to Section 17 of the Commodity Exchange Act, 17 United States Code, Section 21 et seq., as amended, or any regulations adopted thereunder;"

If you have any questions or there is any further information we may be able to provide, please reach out to Michael Schorsch at mschorsch@nfa.futures.org.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Lucy C. Hynes', written in a cursive style.

Lucy C. Hynes
Managing Director
Government & Regulatory Affairs
National Futures Association

MAINE BANKERS

Association

May 5, 2025

Testimony to the 132nd Maine Legislature Committee on Judiciary

Good afternoon, Senator Carney, Representative Kuhn, and honorable members of the Committee. My name is Josh Steirman and I am the Director of Government Relations for the Maine Bankers Association. We are testifying today regarding several data privacy bills. We support the approach taken in LD 1224 and LD 1088. We oppose certain provisions of LD 1822 and are opposed to the bill as currently drafted.

The Maine Bankers Association is the trade association representing 34 retail banks across Maine, with over 9,000 employees in virtually every community state-wide. Last year, our banks provided over \$2.5 billion in residential real estate loans, and over \$3.2 billion in small business loans. Banks are deeply embedded in their communities: last year, bankers volunteered over 145,000 hours, and donated over \$18 million to charitable causes. Maine bankers are your neighbors, working to provide a safe place for deposits, modern technology solutions, fraud protection, a home mortgage, or a small business loan.

Customer trust and security are at the core of our work as financial institutions. Protecting customer data and safeguarding deposits is essential for banks, and we take that trust very seriously. To protect vital information online, banks seek to use as many technological tools as possible: this includes biometric identifiers such as voice recognition, fingerprints, and facial recognition. Use of these identifiers is much safer than passwords alone, and helps create the robust cyber security that customers demand.

We are concerned that new legislation could restrict banks' ability to use these biometric identifiers to keep customer data safe. Banks are already one of the most heavily regulated industries in the nation, regularly subjected to financial examinations, consumer protection laws, and compliance audits continually from a wide variety of federal and state regulatory agencies. Additional state regulation could not only be duplicative, but also counterproductive: without a clearly drafted exemption, the wrong bill would almost certainly decrease use of biometric data by financial institutions, removing highly demanded features such as voice recognition and fingerprints, and ultimately leaving consumer data less secure.

Our priority is to maintain a full entity-level exemption for financial institutions already regulated under the Gramm-Leach-Bliley Act (GLBA). This clarity will allow banks to continue protecting customers with cutting-edge technology and security. An entity-level exemption for financial institutions which are already regulated under the Gramm-Leach Bliley Act (GLBA) is most appropriate and necessary in any new privacy legislation in Maine, and we emphasize the following reasons:

1.) Entity-level exemptions promote clarity and consistency: of the states which have already implemented similar data privacy laws, 12 out of 13 states have laws with an entity-level exemption for financial institutions already subject to GLBA. We hope to avoid confusing and unnecessary conflict between the laws of Maine and other states. If Maine is outside national standards, Maine people will have reduced access to financial services which are essential to buy

homes, save for retirement, and build businesses. A data-level exemption would exacerbate an inconsistent patchwork approach with differences between states.

2.) Definitions based on state statutes create confusion and encourage costly litigation: if Maine law utilized a data-level exemption, the need to delineate applicability would almost certainly force state government to engage in costly and time-consuming lawsuits at taxpayer expense. We are concerned about limited state resources diverted to this type of unnecessary legal challenge.

3.) Data-level exemptions would put cyber security at risk for consumers: definitional uncertainty of a data-level exemption would dampen the responsible use of technologies that improve cyber security for Maine consumers. Maine people consistently demand that banks employ the strongest cyber security frameworks available; this includes the use of biometric identifiers such as face-ID to access mobile phone applications, or voice recognition over the phone. Customers choose to opt into them at overwhelming rates, and are much more secure than passwords alone. Banks need regulatory certainty to continue providing customers with the most advanced levels of technology for customer safety and data security.

4.) Existing regulation is stringent: banks are already subject to extensive regulation (including GLBA) which mandate high standards of data security and notice of data practices to consumers. GLBA continues to be updated by rulemaking and legislation, such as recent passage in the US House of the Data Privacy Act of 2023. Notably, these laws are enforced through ongoing supervision by agencies including the FDIC, Federal Reserve, US Treasury, and Maine Bureau of Financial Institutions. This robust oversight is in contrast to many other unregulated industries where laws are only enforced by the threat of prosecution or litigation.

We respectfully urge the Legislature to include an entity-level GLBA exemption in any new data privacy legislation. This approach is utilized in LD 1224 and LD 1088, and we encourage any version which advances to utilize these definitions. Banks treat customer data as sacrosanct: they don't sell it, are prohibited from selling it, and guard it as the foundation of trust with customers. An entity-level GLBA exemption provides the clarity needed for banks to continue providing the high standard of cyber security that consumers demand and deserve.

In conclusion, we urge caution, deliberation, and moderation when considering new privacy regulations. This is a complex policy matter deserving extensive public discussion. Piecemeal state regulation would threaten the availability of necessary security features. Data security and trust are imperative to the viability of our business, and we ask for regulatory clarity to meet those customer demands for security. We applaud a coordinated and balanced approach.

Thank you for your consideration, I am happy to answer any questions.

Respectfully Submitted,

Joshua Steirman
Director of Government Relations



Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

May 1, 2025

P 202 371 0910

CDIAONLINE.ORG

Senator Anne Carney
Chair
Joint Committee on Judiciary
Room 438
Maine Senate
100 State House Station
Augusta, ME 04333

Representative Amy Kuhn
Chair
Joint Committee on Judiciary
Room 438
Maine House of Representatives
100 State House Station
Augusta, ME 04333

Chair Carney, Chair Kuhn and Members of the Committee:

On behalf of the Consumer Data Industry Association (CDIA), I write to share our perspective on LDs 1088, 1224, and 1822, the three comprehensive data privacy proposals under consideration by the committee. While CDIA would prefer a single, national standard, if Maine intends to adopt its own version, we respectfully request it align to the greatest extent possible with the models already adopted across the country. With that in mind, we are concerned by the definition of “publicly available information” incorporated into LD 1088 (§9602 24., on pg. 3, line 40 through pg. 4, line 26) and LD 1822 (§9602 31., on pg. 4, line 27) and instead encourage the committee to include the definition from LD 1224 (§9602 23., on pg. 3, line 36) in any final comprehensive data privacy proposal.

CDIA is the trade association representing consumer reporting agencies (“CRAs”), including the nationwide credit bureaus, regional and specialized credit bureaus, and background check and residential screening companies. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, thereby helping ensure fair and safe transactions for consumers and facilitating consumer’s access to financial products and other services suited to their unique needs.

In evaluating comprehensive data privacy proposals, CDIA focuses intently on a handful of critical provisions that align state privacy statutes with various federal laws governing different types of consumer data flows that our members must adhere to and the United States Constitution. This includes the Fair Credit Reporting Act (FCRA), which is regarded as one of the nation’s first privacy laws, the Gramm-Leach-Bliley Act (GLBA), the national financial privacy statute, and the Driver’s Privacy Protection Act (DPPA), which governs the sharing and use of motor vehicle records. Beyond specific statutes, CDIA also focuses on provisions related to the use of personal data to combat fraud, for employment purposes and how privacy statutes treat information contained in public records.

While CDIA is pleased that all of the proposals before the committee include provisions that contemplate the FCRA, data governed by GLBA, the DPPA, fraud and employment uses, we are concerned by the proposed definition of “publicly available information” in LD 1088 and LD 1822 that depart from the standard format utilized across the country, specifically LD1088’s §9602 24. B. (4) and LD 1822’s §9602 31. B. (4), excluding inferences derived from publicly available information from being exempt from the law. However, LD 1224 incorporates a definition of “publicly available information” that more closely aligns with the standard approach taken by other states and we encourage the committee to ensure any approved bill uses LD 1224’s definition (§9602 23., on pg. 3, line 36-40).

Our member companies rely on access to public records to ensure completeness and accuracy in relation to consumer reports, credit reports, background checks, and tenant screening products. Information from public records also helps support our members' identity verification, fraud detection, product recall, and benefits administration work. Some of CDIA's members collect, maintain, and share information with government and law enforcement agencies to assist with fraud prevention, including unemployment fraud, workers' compensation fraud and tax fraud.

Information from public records feeds into these critical processes and functions alongside other data streams that may be subject to federal laws like the FCRA, GLBA, or DPPA and exempt from all of the data privacy proposals before the committee. Invariably, combining this information, contrasting it against other sources, or comparing it necessitates making inferences, like whether the data is being placed in the right report, whether or not the data provided matches the expected data to verify an identity or detect fraud, to determine whether a consumer is the current owner of a vehicle requiring safety recall services, among others.

This is why we are concerned by the inclusion of clause B. (4) in the definition of "publicly available information" in both LD 1088 and LD 1822. By subjecting certain uses of public record information to the provisions of these proposed data privacy statutes, it seems to swallow other critical exemptions for certain federal statutes or other well-recognized and understood applications like fraud detection or employment uses.

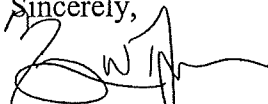
Further, this limitation fails to contemplate when one item of data may be provided from multiple sources. Consider a consumer's address derived from a public record included in a consumer report. CDIA members would have challenges understanding whether, when combined with other information, if it is covered under the "publicly available information" provisions or excluded based on the FCRA exemption.

If the limitation at B. (4) from LD 1088 and LD 1822 is not removed, Maine's prospective comprehensive data privacy statute not only risks unintentionally complicating consumers' lives but also could empower fraudsters by giving them a pathway to cover their tracks at the same time they are victimizing Mainers. Surely this is not the legislature's intent.

CDIA members take concerns regarding privacy, data security, and appropriate uses of data seriously. We appreciate the recognition in all three of these proposals that the data and activities of our member companies are already tightly regulated by various federal laws and our industry serves a critical purpose for consumers, businesses, volunteer organizations, communities and the larger economy.

With that in mind, we respectfully request that the committee adopt the "publicly available information" definition from LD 1224 (§9602 23., on pg. 3, line 36-40) and preserve the exemptions for the FCRA, the DPPA, data regulated by GLBA, fraud detection, and employment purposes already in each of the proposals to ensure Maine's privacy statute aligns as closely as possible to the laws already adopted by other states. Thank you for your time and consideration.

Sincerely,



Zachary W. Taylor
Director, Government Relations
Consumer Data Industry Association



May 5, 2025

The Honorable Anne Carney
Senate Chair, Committee on Judiciary

The Honorable Amy Kuhn
House Chair, Committee on Judiciary

Submitted Electronically

Re: LD 1284 and LD 1088 – OPPOSE

Dear Chairs Carney and Kuhn:

I write today on behalf of the Electronic Frontier Foundation, a San Francisco-based, non-profit organization that works to protect civil liberties in the digital age. EFF represents more than 30,000 active donors and members, including in Maine. We write to respectfully oppose LD 1284 and LD 1088, which would repeal this state's landmark broadband privacy law.

EFF supported these broadband privacy provisions, both in the legislature and in court with an amicus brief supporting the law before broadband companies dropped their challenge to it in 2022.¹

Repealing this law would be a devastating step back for privacy in Maine. With this law in place, broadband internet access services (BIAS) have to ask people for their consent to use and disclose "customer personal information." That includes billing information and social security number. It also includes information derived from a customer's use of broadband service. Such information includes browsing history, application use, precise geolocation, financial and health information, device identifiers, and contents of communications.

That is highly sensitive information. Broadband internet service providers, left unchecked, are in a unique position to mine and profit from this data in ways that individual customers would never expect. A customer must entrust a BIAS provider to carry their online communications—much like UPS or FedEx carry physical packages or letters. This gives BIAS providers the opportunity to rifle through customers' online lives.

We would find it unacceptable if FedEx or UPS logged such information. And, unlike package carriers, when it comes to broadband providers, customers are also often not given a choice of provider in their area. That leaves them uniquely at the whim of an individual company's policies.

¹ Schwartz, Adam, et al. "EFF to Court: Broadband Privacy Law Passes First Amendment Muster." *Electronic Frontier Foundation*, 28 May 2020, www.eff.org/deeplinks/2020/05/eff-court-broadband-privacy-law-passes-first-amendment-muster.

EFF letter in opposition to LD1284 and LD1088

Page 2 of 2

Maine's broadband privacy law is one of the best such laws in the country. That is why we oppose LD 1284 and LD 1088 and urge you not to take away these crucial protections by repealing the law. We respectfully urge your "no" vote. Thank you.

Sincerely,

A handwritten signature in dark ink, appearing to read 'Hayley Tsukayama', with a long horizontal flourish extending to the right.

Hayley Tsukayama
Associate Director of Legislative Activism
Electronic Frontier Foundation
(415) 436-9333 x 161

cc: Honorable members of the Joint Standing Committee on Judiciary



Testimony Neither For Nor Against LD 1088, “An Act to Enact the Maine Consumer Data Privacy Act” and in Opposition to 1822, “An Act to Enact the Maine Online Data Privacy Act”

Senator Carney, Representative Kuhn, and the distinguished members of the Committee on Judiciary, my name is Harris Van Pate and I serve as policy analyst for Maine Policy Institute. Maine Policy is a free-market think tank, a nonpartisan, non-profit organization that advocates for individual liberty and economic freedom in Maine. Thank you for the opportunity to provide testimony on LDs 1088 and 1822.

Position on LD 1088: Neither For Nor Against

While Maine Policy Institute prefers LD 1088 to 1822, both bills have weaknesses in several categories and need significant changes to properly balance privacy rights with free enterprise and speech principles.

Notably, LD 1088 establishes clear consumer rights and consent standards, particularly for teens aged 13 to 15, and recognizes key business exemptions, including employment data and contextual advertising. However, it still establishes a fair “willful disregard” standard for those collecting these Mainers’ data.

The bill’s thresholds—applying only to companies with 100,000+ consumers or those deriving 25% or more of revenue from data sales—are still stricter than many other privacy laws, but are at least less far-reaching than 1822. However, concerningly, the phase-in process of applying to smaller companies in 2028 undermines this bill’s attempt at a light-handed privacy protection approach.

This bill could be altered to better balance consumers’ privacy rights with Maine companies’ speech rights and business needs. The third section of this testimony, “Concerns and Recommendations for Amendments,” suggests changes to both bills before you today.

We commend this bill’s inclusion of cure periods and flexible opt-in standards, which align with MPI’s limited government and free enterprise principles. The bill attempts to account for individual liberties and privacy rights in its structure, though it still needs significant changes to do so thoroughly.

Position on LD 1822: Against

While LD 1822 shares the goal of strengthening data privacy protections, it represents a more aggressive regulatory model that may unintentionally stifle economic opportunity



and constitutional freedoms. We appreciate the bill's intention but urge caution and refinement.

Unlike LD 1088, LD 1822 flatly bans the sale and processing of sensitive data in certain circumstances and imposes requirements that exceed the norms of many state privacy laws. These provisions raise legitimate concerns about overreach, enforceability, and adverse impacts on speech, public engagement, and innovation.

Further, unlike LD 1088, LD 1822 prohibits data controllers from selling sensitive data, processing personal data of minors for targeted advertising or sale (even if the controller is unaware). Additionally, both bills largely stop companies from altering services provided based on whether a consumer agrees to information disclosure, a burdensome rule to apply to companies.

We do not oppose LD 1822's underlying objectives. However, this legislation should be significantly amended to preserve free expression and reduce unnecessary regulatory strain.

Concerns and Recommendations for Amendments

1. Preserving Free Expression and Consumer Choice

- **Amend the bills to further protect First Amendment activities**, including political speech and canvassing. The current geofencing restrictions could unintentionally limit advocacy or public health alerts.
- **Clarify that targeted advertising is allowed with affirmative consumer consent**, including for minors aged 13–15 with parental approval, rather than banning it outright. This balances family autonomy and free commercial speech.
- **Broaden the exemption for publicly available information** to include public records, journalistic activities, and widely disseminated content, preventing unintended restrictions on news, transparency, or public databases.
- **Consider the requirement to disclose third-party access** in limiting the bills' application, as many smaller controllers will have difficulty accessing, categorizing, and reporting data sales compared to better-resourced large organizations.

2. Reducing Regulatory Burdens on Small Businesses

- **Raise the bills' applicability thresholds** to mirror those in other states. For example, one such state only applies to companies that produce products or services targeted at in-state residents, generate \$25 million in revenue annually,



and either control or process the personal data of at least 100,000 consumers annually, or derive over 50% of gross revenue from personal data sale and control the personal data of at least 25,00 people.¹ This would focus compliance on large-scale data operators, not local Maine businesses.

- **Expand nonprofit exemptions** to include all 501(c) tax-exempt organizations, ensuring that all nonprofits, trade associations, clubs, and unions are not inadvertently subjected to onerous requirements.
- **Maintain a permanent cure period or introduce a safe harbor** for companies that demonstrate good-faith compliance or use frameworks such as NIST or AICPA privacy standards. The bills provide shorter cure periods, and LD 1288 only creates a temporary one, but many other states have established permanent cure periods instead. This incentivizes strong privacy practices without imposing punitive burdens.

3. Supporting Common Business Practices

- **Amend LD 1822 to explicitly allow loyalty programs and discounts tied to voluntary data collection.** This will ensure that consumers can choose value-added services and businesses can continue innovative customer engagement models. This bill currently only allows loyalty programs that are not directly connected with data sales. If a loyalty program allows a company to pass on some of the profit of data sales to the consumer, it seems unfair to ban such a mutually beneficial agreement.
- **Clarify that “necessary” processing of sensitive data includes common operational needs,** such as service personalization, and internal analytics, provided consumers are informed and have opt-out options.
- **Moving away from necessity requirements and relying more on consumer opt-ins** will also allow greater flexibility in relationships between companies and their customers. While LD 1088’s “reasonably necessary” language is a bit more vague, it matches the language of more pro-business laws. It allows greater discretion on the end of companies regarding what data to collect and what purposes justify its use.

4. Limiting Government Overreach

- **Restrict the Attorney General’s enforcement authority** to actions consistent with published guidance and allow businesses a clear pathway to compliance. Agencies should not have unchecked discretion to demand internal documents or impose penalties for minor missteps.

¹ <https://www.akingump.com/en/insights/alerts/utah-consumer-privacy-act-what-businesses-need-to-know>



- **Add a statutory review clause or sunset provision** that mandates reevaluation of the law's impact within two years of enactment. This ensures the law adapts to technology and focuses on real-world privacy risks, not theoretical harms.

Conclusion

These bills present broad regulatory schemes that warrant caution and refinement. We encourage the committee to amend LD 1088 to balance consumer privacy with economic liberty and constitutional values. Meanwhile, we believe that LD 1822 in its current form is too burdensome on Maine businesses and does not adequately balance speech and business interests with the right to privacy. Thank you for your time and consideration.

DISABILITY RIGHTS MAINE

May 5, 2025

Senator Anne Carney, Chair
Representative Amy Kuhn, Chair
Joint Standing Committee on Judiciary
State House, Room 438
Augusta, Maine 04333

Re: Testimony in Support of LD 1822, An Act to Enact the Maine Online Data Privacy Act and Against LDs 1088, 1224, and 1284

Dear Senator Carney, Representative Kuhn, and Members of the Joint Standing Committee on Judiciary:

My name is Lauren Wille and I am the Legal Director at Disability Rights Maine. DRM is Maine's designated Protection and Advocacy agency, and our mission is to advance justice and equality by enforcing rights and expanding opportunities for people with disabilities in Maine. Thank you for the opportunity to provide testimony in support of LD 1822, and against LDs 1088, 1224, and 1284.

LD 1822 is an important policy that will allow Maine to protect its citizens in the face of rapidly evolving technology. This bill prohibits entities, including for-profit companies, from collecting digital consumer data except where necessary to provide the product or service requested by the consumer. And, crucially, it prohibits such entities from processing consumer data in a way that discriminates or makes unavailable the enjoyment of goods and services on the basis of enumerated statuses, including disability. In contrast to LD 1822, LDs 1088 and 1224 would allow companies to collect personal information as long as the consumer clicks "I agree," or the collection is disclosed in a privacy policy. Very few people read privacy policies, and those of us who do, will be forced to choose between our privacy and accessing a service.

Assistive technology has been tremendously beneficial in helping people with disabilities become more independent, but, as technology expands, so do the privacy concerns. There are apps that help people track chronic pain, transcribe speech for people who are Deaf or hard of hearing, provide wheelchair accessibility information, read aloud written

160 Capitol Street, Suite 4, Augusta, ME 04330
207.626.2774 • 1.800.452.1948 • Fax: 207.621.1419 • drme.org

MAINE'S PROTECTION AND ADVOCACY AGENCY FOR PEOPLE WITH DISABILITIES

information on devices, and provide daily task reminders, to name just a few. These apps are not “health care providers” that are subject to confidentiality under HIPAA. Instead, users might agree to give up privacy protections in order to access the technology. Users may not be aware of the implications of this data being collected, processed, and sold to third-parties. But they may notice that suddenly they are receiving very targeted ads for equipment, certain medications, and other products. The ordinary consumer may not be aware of the exchange of personal data that has occurred to enable this.¹

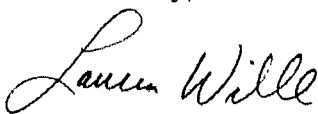
The recipients of our sensitive data include entities are not subject to confidentiality laws under HIPAA, which only governs health records connected to health care providers. With the proliferation of apps, a great many consumers do not understand that, and how, their personal data is being collected, processed, and sold to other entities. LD 1822 provides protection for all consumers, including consumers with disabilities. In our work at DRM, we see daily how the lack of privacy, through the lens of ableism, leads to rampant discrimination and exploitation of individuals with disabilities. This bill is one step toward safeguarding that usage and allowing people to have control over their personal data and how it is used.

In addition, LD 1822 enables consumers to, among other things, confirm whether their data is being collected, access that data, correct inaccuracies, and opt out of processing and sale of personal data for targeting marketing.

LD 1822 provides comprehensive protections for Mainers, including Mainers with disabilities, and DRM urges this esteemed Committee to vote Ought to Pass. We also urge you to oppose LDs 1088 and 1224, which do not go far enough, and LD 1284, which would repeal our internet privacy law.

Thank you for your time and consideration.

Sincerely,

A handwritten signature in cursive script that reads "Lauren Wille".

Lauren Wille, Esq.
Legal Director
Disability Rights Maine

¹ For a comprehensive analysis of the benefits and risks of data collection as it relates to health equity, see Silvia Yee & Mary Lou Breslin, *This Data, Not That Data: Big Data, Privacy, and the Impact on People with Disabilities*, Disability Rights Education and Defense Fund, https://healthlaw.org/wp-content/uploads/2023/03/This-Data-Not-That-Data_Disability-Rights-Education-and-Defense-Fund_FINAL.pdf (last accessed May 5, 2025).